The Algebra of Topological Quantum Computing

by

Julia Evans

School of Computer Science
McGill University, Montréal

August 2011

A thesis submitted to McGill University
in partial fulfillment of the requirements of the degree of
Master of Science

Abstract

Topological quantum computing is an approach to the problem of implementing quantum gates accurately and robustly. The idea is to exploit topological properties of certain quasiparticles called anyons to obtain a proposed implementation of quantum computing which is inherently fault-tolerant. The mathematical structure that describes anyons is that of modular tensor categories. These modular tensor categories can be constructed from the representations of certain algebraic objects called quantum groups. In this thesis we give an explanation of modular tensor categories and quantum groups as they relate to topological quantum computing. It is intended that it can be read with some basic knowledge of algebra and category theory. The hope is to give a concrete account accessible to computer scientists of the theory of modular tensor categories obtained from quantum groups. The emphasis is on the category theoretic and algebraic point of view rather than on the physical point of view.

Résumé

Le calcul quantique topologique est une approche au problème d'implementation de circuits quantique d'une façon robuste et precisé. L'idée s'agit d'exploiter certaines propriétés de quasiparticules, dites "anyons", pour obtenir une implémentation du calcul quantique qui est intrinsequement tolerante aux pannes. La structure mathématique qui décrit ces anyons est celle des catégories modulaires. Ces objets peuvent être construites à partir de représentations de certaines algèbres, appelées groupes quantiques. Dans ce mémoire, nous donnerons une exposition des catégories modulaires, des groupes quantiques et du lien qu'ils partagent avec le calcul quantique. Le mémoire ne devrait requérir qu'une connaissance de base en algèbre et en théorie des categories. L'espoir étant de donner un model concret pour les informaticiens de la théorie de catégories obtenus à partir de groupes quantiques. L'emphase sera sur le point de vu algèbrique et catégorique plutôt que celui physique.

Acknowledgments

Firstly, I thank my awesome advisor Prakash Panangaden for introducing me to topological quantum computing, telling me when I'm not making sense, and for cooking some excellent meals.

I thank all of my amazing professors at McGill, in particular Patrick Hayden for first getting me excited about quantum computing.

Thanks to the Quantum Group at Oxford University for their hospitality during my visit to Oxford and many useful discussions.

I thank all of my friends for their support and company. In particular I'd like to thank Rebecca and Kamal. I also thank Alex Lang and Svetla Vassileva for reading this thesis and offering many useful comments and corrections, and Andrew Stacey, for writing and providing some much-needed help with the braids package I used to draw braid diagrams. Finally, I thank my parents, for always encouraging me in my studies.

Pursuing this degree was possible thanks to scholarships from NSERC and FQRNT.

Contents

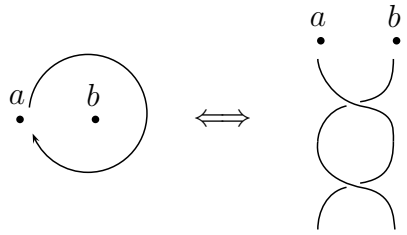
Chapter 1
Introduction

One of the major challenges in implementations of quantum computing is that of implementing quantum gates accurately and robustly. Topological computing, first proposed by Kitaev in 1997 [22], exploits topological properties of certain quasiparticles called *anyons* to obtain a proposed implementation of quantum computing which is inherently fault-tolerant.

What are anyons? When 2 identical particles are interchanged in 3 dimensions, there are exactly 2 possibilities: either the wave function is symmetric (in the case of bosons) or it is antisymmetric (in the case of fermions). Intuitively one can view this as arising from the following argument. In 3 dimensions, 2 identical particles being interchanged twice is topologically equivalent to one particle being transported around the other, which is in turn topologically equivalent to neither particle moving at all.

In 2 dimensions the situation is completely different: moving one particle around another is topologically nontrivial, and the system may not end up in the same state. We refer to particles in 2 dimensions which are neither bosons nor fermions as *anyons*.

Suppose we have a system of n anyons, and rearrange them in some way. Each topological class of such trajectories in 2+1 dimensions corresponds to an element of the braid group B_n:



and the state Ψ of the anyons transforms depending only on the braid σ corresponding to the trajectory of the anyons:

$$\Psi \mapsto \rho(\sigma)\Psi \tag{1.0.1}$$

The state of the anyons therefore transforms via representations of the braid group B_n. In the simplest case, the state transforms via a one-dimensional representation of B_n:

$$\Psi \mapsto e^{i\theta}\Psi \tag{1.0.2}$$

Anyons which transform in this way are called *abelian anyons*. The other possibility is that the state transforms according to some higher-dimensional representation of B_n. In this case nontrivial operations can be performed simply by rearranging the anyons in some suitable way. Anyons which transform according to higher-dimensional representations are called *nonabelian anyons*, and it is possible to do quantum computation with certain species of nonabelian anyons.

The key point here is that in this model the change in state of the anyons depends *only* on the topological class of the braid, so minor perturbations of a particle's path won't affect the result of the computation at all. The process is thus inherently resistant to errors.

Do anyons actually exist? As we said earlier, all particles in 3 dimensions are bosons or fermions. However, in 2 dimensions many other types are possible. These are of course not fundamental particles but merely excitations of the 2D electron gas that behave like particles: they are called quasiparticles.

In general a system with anyons will have several different types of anyons. Any two anyons can be brought together to form a new anyon. This process is called *fusion*. In general if two anyons fuse, then there might be several possible results.

The mathematical structure that describes anyons is that of modular tensor categories: the tensor structure models the process of fusion. The goal of this thesis is to give an explanation of modular tensor categories as they relate to topological quantum computing. It is intended that this thesis can be read with some basic knowledge of algebra and category theory. The modular tensor categories that describe anyons' behavior are constructed from the representations of certain algebraic objects called *quantum groups*.

In Chapter 2 we give the algebraic background of braid groups, Lie algebras, and Hopf algebras necessary to construct quantum groups. In Chapter 3 we describe the correspondence between the features of anyonic systems and those of modular tensor categories and define modular tensor categories. In Chapter 4 we introduce the quantum group $U_q(\mathfrak{sl}(2))$ and discuss its representation theory. In Chapter 5 we explain how to construct a modular tensor category from the quantum group $U_q(\mathfrak{sl}(2))$.

In Chapter 6 we finally get to the business of discussing topological quantum computing. We review the work that has been done on the subject, in particular that on the computational business of constructing braids that correspond to particular unitaries.

The hope is to give a concrete account accessible to computer scientists of the theory of modular tensor categories obtained from quantum groups. The emphasis is on the category theoretic and algebraic point of view rather than on the physical point of view.

Chapter 2
Algebraic Background

Anyons are modelled by representations of certain algebras called quantum groups, which arise as deformations of Lie algebras. Their trajectories correspond to braids. In this chapter we define and discuss some relevant results about the required algebraic structures: Lie algebras, braid groups, and Hopf algebras. This sets the stage for the definition of the quantum group $U_q(\mathfrak{sl}(2))$ in Chapter 4, which is a Hopf algebra and a deformation of the Lie algebra $\mathfrak{sl}(2)$. Everything in this section takes place over a field k of characteristic 0.

2.1 Algebras and their representations

We give a few key definitions about algebras and their representations here.

An associative algebra A over a field k is a k-vector space which also has the structure of a ring. Some important examples of k-algebras are:

1. k itself
2. The $n \times n$ matrices over k, $M_n(k)$

3. The group algebra of a finite group (defined in 2.4.5)

4. The algebra $k[x]$ of polynomials in x over k

5. The universal enveloping algebra of a Lie algebra (defined in 2.4.6)

A module for an algebra A is the same as a representation of the algebra, and we will use the terms interchangeably.

Definition 2.1.1. *An* A-module *for an algebra* A *is a vector space* M *with a binary operation* $A \times M \to M$ *written* $r \cdot n$ *or* rn *such that for* $r, s \in A$ *and* $m, n \in M$*:*

1. $r(n+m) = rn + rm$
2. $(rs)n = r(sn)$
3. $1n = n$
4. $(r+s)n = rn + sn$

Definition 2.1.2. *A subspace* $N \subset M$ *of a module* M *is a* submodule *of* M *if* $an \in N$ *for every* $a \in A, n \in N$*.*

Definition 2.1.3. *A submodule* N *of a module* M *is called* maximal *if there is no submodule* N' *of* M *such that* $N \subsetneq N' \subsetneq M$*.*

Definition 2.1.4. *We say that a module is* simple *or* irreducible *if it has no non-trivial submodules.*

Anyon types will correspond to irreducible representations of quantum groups.

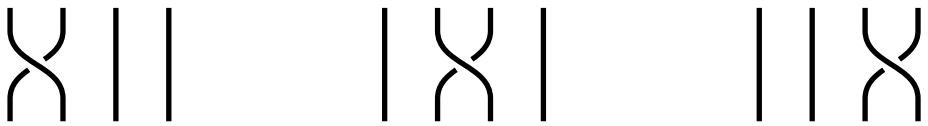
2.2 Braid groups

Topological quantum computing is performed by braiding the worldlines of anyons, and the states of anyons transform via representations of the braid group. The study of braid groups is a rich and fascinating subject, and we will only give some basic definitions here. For more, see *Braid Groups* by Kassel [20].

The braid group B_n on n strands is generated by $\sigma_1, \sigma_2, \ldots, \sigma_n$ with relations

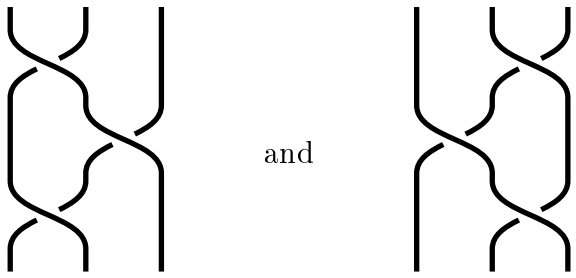
$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}\sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2 \tag{2.2.1}$$

Note that this is the same as the presentation of the symmetric group S_n, without the additional relations $\sigma_i^2 = 1$. Any element of B_n can be depicted as a braid diagram. For example, B_4 is generated by



σ_1 σ_2 σ_3

The relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ (also known as the Yang-Baxter equation) corresponds to the topological equivalence between the two braids



and

2.3 Lie algebras

Anyons are modelled by representations of quantum groups, which are deformations of semisimple Lie algebras. We will give some basic definitions of Lie algebras, ideals, simplicity, and semisimplicity, and discuss briefly the classification of semisimple Lie algebras. For more information about Lie algebras, [12] is an excellent reference for complex Lie algebras, and [14] for the more general case of Lie algebras over a field of arbitrary characteristic. Here we will work over $\mathbb{C}$.

Throughout this section $\mathfrak{g}$ will denote a Lie algebra.

A *Lie algebra* is a vector space $\mathfrak{g}$ with a bilinear operation $[\cdot,\cdot]\ \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$ called the *bracket* such that for any $x,y,z\in\mathfrak{g}$,

- $[x,y]=-[y,x]$
- $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$ (the Jacobi identity)

A basic example of a Lie algebra is $\mathfrak{sl}(2)$: the algebra of 2×2 matrices with trace zero. $\mathfrak{sl}(2)$ is spanned by the matrices

$$X^+=\begin{pmatrix}0&1\\0&0\end{pmatrix},X^-=\begin{pmatrix}0&0\\1&0\end{pmatrix},H=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \tag{2.3.1}$$

In general Ado's theorem says that any finite dimensional Lie algebra over a field of characteristic zero can be realized as a vector space of matrices such that

$$\left[X^+,X^-\right]=X^+X^--X^-X^+$$

for any X^+,X^-. The bracket $[X^+,X^-]$ can therefore safely be thought of as the commutator $X^+X^--X^-X^+$.

We will only be interested in semisimple Lie algebras, which are a well-characterized class of Lie algebras. They are defined as follows.

Definition 2.3.1. *A subspace $\mathfrak{h} \subset \mathfrak{g}$ of a Lie algebra is a* Lie subalgebra *if $\mathfrak{h}$ is closed under the Lie bracket.*

An ideal *I of $\mathfrak{g}$ is a subalgebra such that $[\mathfrak{g}, I] \subset I$*

Definition 2.3.2. *A Lie algebra is* simple *if it has no proper ideals and is not commutative.*

$\mathfrak{sl}(2)$ is the lowest-dimensional simple Lie algebra. In fact, it is the basic example of a simple Lie algebra: its representation theory is used in a crucial way in the study of the representation theory of all semisimple Lie algebras.

Definition 2.3.3. *A Lie algebra is* semisimple *if it is the direct sum of simple Lie algebras.*

2.3.1 Representations of $\mathfrak{sl}(2)$

We will model anyons by representations of a deformation of $\mathfrak{sl}(2)$, and understanding the representations of $\mathfrak{sl}(2)$ is an important first step. We present the basic facts about the representation theory of $\mathfrak{sl}(2)$ here without proof.

A *representation* of a Lie algebra $\mathfrak{g}$ is a vector space V together with an action of $\mathfrak{g}$ on V such that

$$[x, y]\, v = x(yv) - y(xv)$$

$$(x + y)v = xv + yv$$

$$(ax)v = a(xv)$$

for all $x, y \in \mathfrak{g}, v \in V, a \in \mathbb{C}$

A representation is called *irreducible* if it has no nontrivial subspaces invariant under the action of $\mathfrak{g}$.

In $\mathfrak{sl}(2)$,

1. Every finite dimensional representation decomposes as a direct sum of irreducible representations (in other words, is completely reducible).

2. The eigenvectors of H form a basis for every irreducible representation. Their eigenvalues are called *weights* and are all integers [1]. The eigenspaces of H are called *weight spaces*.

3. Each irreducible representation is generated by an eigenvector v_0 of H such that $X^+ v_0 = 0$. This eigenvector has the largest weight among all the eigenvectors of H and is called a "highest weight vector".

1. Physicists use a different convention so that the highest weights are half-integers

4. The irreducible representations are classified by their highest weights $n \geq 0$: the representation $V(n)$ with highest weight n has basis $\{v_0, \ldots, v_n\}$ such that

$$Hv_i = (n-2i)v_i$$

$$X^- v_i = \begin{cases} (i+1)v_{i+1} & \text{for } i < n \\ 0 & \text{for } i = n \end{cases}$$

$$X^+ v_i = \begin{cases} (n-i+1)v_{i-1} & \text{for } i > 0 \\ 0 & \text{for } i = 0 \end{cases}$$

Because X^+ and X^- take eigenvectors v_i of H to eigenvectors with respectively higher and lower weights, they are termed raising and lowering operators.

2.3.2 Representations of semisimple Lie algebras

Here we will describe some of the representation theory of semisimple Lie algebras. In particular we define roots and weights and inner products of roots. We will need this theory in Chapter 4 when discussing the representation theory of quantum groups constructed from semisimple Lie algebras.

In a general semisimple Lie algebra, the *Cartan subalgebra* $\mathfrak{h}$ will take the place of the matrix H. The basis vectors for irreducible representations of $\mathfrak{g}$ will be simultaneous eigenvectors of every element of $\mathfrak{h}$ instead of eigenvectors of H.

Definition 2.3.4. *If $\mathfrak{g}$ is a complex semisimple Lie algebra, then a* Cartan subalgebra *of $\mathfrak{g}$ is a complex subspace $\mathfrak{h}$ of $\mathfrak{g}$ such that:*

i) $[H_1, H_2] = 0$ *for all* $H_1, H_2 \in \mathfrak{h}$

ii) For any $X \in \mathfrak{g}$, $[H, X] = 0 \ \forall \ H \in \mathfrak{h} \implies X \in \mathfrak{h}$

iii) ad_H *is diagonalizable for all* $H \in \mathfrak{h}$

where $\mathrm{ad}_H : \mathfrak{g} \to \mathfrak{g}$ *is the map taking* $X \mapsto [H, X]$.

When $\mathfrak{g}$ is not a semisimple Lie algebra, the definition of a Cartan subalgebra is different.

Definition 2.3.5. *A* root *of* $\mathfrak{g}$ *is a nonzero linear functional* α *on* $\mathfrak{h}$ *such that there exists a nonzero element* $X \in \mathfrak{g}$ *with*

$$[H, X] = \alpha(H)X \tag{2.3.2}$$

for all $H \in \mathfrak{g}$

It is always possible to define an inner product $\langle \cdot, \cdot \rangle$ on $\mathfrak{g}$ which satisfies certain other properties that we will not go into here. For example, in $\mathfrak{sl}(2)$ an appropriate inner product is

$$\langle A, B \rangle = \mathrm{tr}(A^* B) \tag{2.3.3}$$

We can use this inner product to identify $\mathfrak{h}$ with $\mathfrak{h}^*$. In particular, this lets us identify roots with elements of $\mathfrak{h}$, giving us the new definition:

Definition 2.3.6. *A* root *of* $\mathfrak{g}$ *is an element* α *of* $\mathfrak{h}$ *such that there exists a nonzero element* $X \in \mathfrak{g}$ *with*

$$[H, X] = \langle \alpha, H \rangle \, X \tag{2.3.4}$$

for all $H \in \mathfrak{h}$

From now on we will consider roots to be elements of $\mathfrak{h}$. This means in particular that there is an inner product on roots.

The *root system* $R \subset \mathfrak{g}$ of $\mathfrak{g}$ is the set of its roots.

Definition 2.3.7. *A* base *for a root system R is a subset $\{\alpha_1, \ldots, \alpha_r\} \subseteq R$ which is a basis for $\mathfrak{g}$, and further if*

$$\alpha = n_1\alpha_1 + \ldots + n_r\alpha_r \tag{2.3.5}$$

then either all the n_i are greater than or equal to zero or all the n_i are less than or equal to zero. A root α with all the $n_i \geq 0$ is called a positive root. *A root α with all the $n_i \leq 0$ is called a* negative root. *The elements $\{\alpha_1, \ldots, \alpha_r\}$ are called the* positive simple roots.

Suppose ρ is a finite dimension representation of $\mathfrak{g}$ on V. $\mu \in \mathfrak{h}$ is called a *weight* for ρ if there exists a nonzero vector $v \in V$ such that

$$\rho(H)v = \langle \mu, H \rangle \, v \tag{2.3.6}$$

for all $H \in \mathfrak{h}$. v is simultaneously an eigenvalue of every $\rho(H)$, and μ gives its eigenvalues.

We define a partial order on the weights as follows:

Definition 2.3.8. *Let $\mu_1, \mu_2 \in \mathfrak{h}$. Then $\mu_1 \geq \mu_2$ if there are $n_1, \ldots, n_r \geq 0$ such that*

$$\mu_1 - \mu_2 = n_1\alpha_1 + \ldots + n_r\alpha_r \tag{2.3.7}$$

A weight μ_0 is a highest weight *if $\mu_0 \geq \mu$ for all weights μ.*

We need to make one last definition before stating the theorem classifying the representations of semisimple Lie algebras.

Definition 2.3.9. *A* dominant integral element *of* $\mathfrak{g}$ *is an element* $\mu \in \mathfrak{h}$ *such that*

$$2\frac{\langle \mu, \alpha \rangle}{\langle \alpha, \alpha \rangle} \tag{2.3.8}$$

is a nonnegative integral for all positive simple roots α*.*

Theorem 2.3.10. *1. Every finite dimensional representation of* $\mathfrak{g}$ *has a highest weight.*

2. Representations with the same highest weight are isomorphic.

3. Every highest weight is a dominant integral element.

4. Every dominant integral element occurs as the highest weight of some representation.

2.4 Hopf algebras

Models of topological quantum computation come from certain algebras called quantum groups. These quantum groups are somewhat deceptively named in that they are not groups. However, they are Hopf algebras, which are a generalization of the group algebra of a group: they have a map called the antipode which generalizes the group inverse. Basically a Hopf algebra is an algebra which has a compatible coalgebra structure and an antipode map which "behaves like" an inverse in a suitable

way. If an algebra is a Hopf algebra, then its category of representations has additional structure, which will be crucial for us in our discussion of topological quantum computing. This is explained in 3.7.

In this section, we define algebras and coalgebras, then bialgebras which are simultaneously algebras and coalgebras, then Hopf algebras which are bialgebras with an antipode map.

2.4.1 Algebras and coalgebras

We said earlier that for a field k, a *k-algebra* A is a k-vector space with an associative bilinear mapping $A \times A \to A$ which has an identity element $1 \in A$ such that $1 \cdot x = x \cdot 1 = x$ for any $x \in A$.

Restated in categorical terms, a k-algebra is given by a triple (A, μ, η), where A is a vector space, and the multiplication map $\mu : A \otimes A \to A$ and the unit map $\eta : k \to A$ are linear maps. For A to be an algebra, the following two diagrams need to commute:

Associativity axiom:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes \mathrm{id}} & A \otimes A \\ \downarrow{\scriptstyle \mathrm{id} \otimes \mu} & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow{\mu} & A \end{array} \tag{2.4.1}$$

Unit axiom:

$$\begin{array}{ccccc} k \otimes A & \xrightarrow{\eta \otimes \mathrm{id}} & A \otimes A & \xleftarrow{\mathrm{id} \otimes \eta} & A \otimes k \\ & {\scriptstyle \simeq} \searrow & \downarrow{\scriptstyle \mu} & \swarrow {\scriptstyle \simeq} & \\ & & A & & \end{array} \tag{2.4.2}$$

An algebra is called *commutative* if $x \cdot y = y \cdot x$ for any $x, y \in A$. In categorical terms, it needs to satisfy the commutativity axiom:

The triangle

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\tau_{A,A}} & A \otimes A \\ & {\scriptstyle \mu} \searrow \quad \swarrow {\scriptstyle \mu} & \\ & A & \end{array} \tag{2.4.3}$$

commutes, where $\tau(a \otimes b) = b \otimes a$.

Given two algebras (A_1, μ_1, η_1) and (A_2, μ_2, η_2), a linear map $f : A_1 \to A_2$ is called a *morphism of algebras* or an *algebra homomorphism* if $f(\mu_1(a, b)) = \mu_2(f(a), f(b))$ for any $a, b \in A_1$ and $f(\eta_1(1)) = \eta_2(1)$. In other words, the following two diagrams need to commute:

$$\begin{array}{ccc} 1 & \xrightarrow{\eta_1} & A_1 \\ & {\scriptstyle \eta_2} \searrow & \downarrow {\scriptstyle f} \\ & & A_2 \end{array} \tag{2.4.4}$$

$$\begin{array}{ccc} A_1 & \xrightarrow{f} & A_2 \\ {\scriptstyle \mu_1} \uparrow & & \uparrow {\scriptstyle \mu_2} \\ A_1 \otimes A_1 & \xrightarrow[f \otimes f]{} & A_2 \otimes A_2 \end{array} \tag{2.4.5}$$

We can obtain the definition of a coalgebra by reversing all the arrows in the diagrams above as follows:

Definition 2.4.1. *A* coalgebra *is a triple* (C, Δ, ε) *where* C *is a vector space, and* $\Delta : C \to C \otimes C$, $\varepsilon : C \to k$ *are linear maps such that the following two diagrams commute:*

Co-associativity axiom:

$$\begin{array}{ccccc} C\otimes C\otimes C & & \xleftarrow{\Delta\otimes\mathrm{id}} & & C\otimes C \\ {\scriptstyle \mathrm{id}\otimes\Delta}\uparrow & & & & \uparrow{\scriptstyle \Delta} \\ C\otimes C & & \xleftarrow{\Delta} & & C \end{array} \tag{2.4.6}$$

Counit axiom:

$$\begin{array}{ccccc} k\otimes C & \xleftarrow{\varepsilon\otimes\mathrm{id}} & C\otimes C & \xrightarrow{\mathrm{id}\otimes\varepsilon} & C\otimes k \\ & {\scriptstyle\simeq}\nwarrow & \uparrow{\scriptstyle\Delta} & \nearrow{\scriptstyle\simeq} & \\ & & C & & \end{array} \tag{2.4.7}$$

A coalgebra is called *cocommutative* if the following triangle commutes:

$$\begin{array}{ccc} A\otimes A & \xleftarrow{\tau_{A,A}} & A\otimes A \\ & {\scriptstyle\Delta}\nwarrow \quad \nearrow{\scriptstyle\Delta} & \\ & A & \end{array} \tag{2.4.8}$$

A linear map $f : C_1 \to C_2$ between two coalgebras $(C_1, \Delta_1, \varepsilon_1)$, $(C_2, \Delta_2, \varepsilon_2)$ is a coalgebra homomorphism if the following two diagrams commute:

$$\begin{array}{ccc} 1 & \xrightarrow{\eta_1} & A_1 \\ & {\scriptstyle\eta_2}\searrow & \downarrow{\scriptstyle f} \\ & & A_2 \end{array} \tag{2.4.9}$$

$$\begin{array}{ccc} A_1 & \xrightarrow{f} & A_2 \\ {\scriptstyle\mu_1}\uparrow & & \uparrow{\scriptstyle\mu_2} \\ A_1\otimes A_1 & \xrightarrow[f\otimes f]{} & A_2\otimes A_2 \end{array} \tag{2.4.10}$$

2.4.2 Bialgebras

Suppose H is a vector space which has both an algebra structure (H, μ, η) and a coalgebra structure (H, Δ, ε). We call this a *bialgebra* if the two structures are compatible in the following sense:

Definition 2.4.2. *A vector space with an algebra and coalgebra structure is called a* bialgebra *if one of the following two equivalent conditions holds:*

1. *The maps μ and η are morphisms of coalgebras*
2. *The maps Δ and ε are morphisms of algebras*

A morphism of bialgebras is a map which is both a morphism of algebras and a morphism of coalgebras.

2.4.3 Hopf algebras

As we said earlier, a Hopf algebra is a bialgebra with an antipode map:

Definition 2.4.3. *Let $(H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra. An endomorphism S of H is called a* antipode *for the bialgebra if the following two diagrams commute:*

$$\begin{array}{ccccccc} H & \xrightarrow{\Delta} & H \otimes H & \xrightarrow{S\otimes \mathrm{id}} & H \otimes H & \xrightarrow{\mu} & H \\ & \searrow^{\varepsilon} & & & & \nearrow_{\eta} & \\ & & & k & & & \end{array} \tag{2.4.11}$$

$$\begin{array}{ccccccc} H & \xrightarrow{\Delta} & H \otimes H & \xrightarrow{\mathrm{id}\otimes S} & H \otimes H & \xrightarrow{\mu} & H \\ & \searrow^{\varepsilon} & & & & \nearrow_{\eta} & \\ & & & k & & & \end{array} \tag{2.4.12}$$

Definition 2.4.4. *A* Hopf algebra *is a bialgebra with an antipode. A morphism of Hopf algebras is a morphism between the bialgebras which commutes with the antipode maps.*

Example 2.4.5. *As mentioned earlier, the group algebra $k[G]$ of any finite group is a Hopf algebra. $k[G]$ has basis $\{g : g \in G\}$ and multiplication given by the group multiplication. Define*

$$\Delta(g) = g \otimes g \tag{2.4.13}$$

$$\varepsilon(g) = 1 \tag{2.4.14}$$

$$S(g) = g^{-1} \tag{2.4.15}$$

It is easy but useful to check that this gives a Hopf algebra structure on $k[G]$.

Note that the group algebra is not commutative if the underlying group is not commutative, but is always cocommutative. The examples of Hopf algebras we will be interested in later (quantum groups) are neither commutative nor cocommutative.

In general the antipode map can be thought of as an analogue to the inverse map in a group. If a bialgebra has an antipode, it is unique, and $S^2 = \mathrm{id}$.

This next example will be quite important to us: the quantum groups we will study are deformations of universal enveloping algebras of semisimple Lie algebras.

Example 2.4.6. *Given a Lie algebra $\mathfrak{g}$, we can define an associative algebra called the* universal enveloping algebra *of $\mathfrak{g}$. The universal enveloping algebra of any Lie algebra is a Hopf algebra.*

They key property of the universal enveloping algebra is that the Lie algebra embeds in it in such a way that the bracket becomes the commutator. The universal enveloping algebra is constructed as follows.

The tensor algebra $T(V)$ *of any k-vector space V is an associative algebra defined by*

$$T(V) = k \oplus \bigoplus_{n=1}^{\infty} \underbrace{(V \otimes \cdots \otimes V)}_{n \text{ times}} \tag{2.4.16}$$

with multiplication $v \cdot w = v \otimes w$.

If we have a Lie algebra $\mathfrak{g}$, then we can define an ideal $I(\mathfrak{g})$ of the tensor algebra $T(\mathfrak{g})$ generated by all elements of the form $(xy - yx) - [x, y]$ for $x, y \in \mathfrak{g}$.

We define the universal enveloping algebra to be

$$U(\mathfrak{g}) = T(\mathfrak{g})/I(\mathfrak{g}). \tag{2.4.17}$$

We can put a Hopf algebra structure on the enveloping algebra $U(\mathfrak{g})$ for any Lie algebra $\mathfrak{g}$, with Δ, ε, S defined by:

$$\Delta(x) = x \otimes 1 + 1 \otimes x \tag{2.4.18}$$

$$\varepsilon(x) = 0 \tag{2.4.19}$$

$$S(x) = -x \tag{2.4.20}$$

for $x \in \mathfrak{g}$.

2.4.4 Braided Hopf algebras and the R-matrix

Both of the examples of Hopf algebras above are cocommutative. As mentioned earlier, quantum groups are not cocommutative. However, bialgebras that are not cocommutative can be *braided*. This additional structure on a bialgebra will allow us to make its category of representations braided.

Recall that a bialgebra is *cocommutative* if for any x

$$\tau_{H,H} \circ \Delta(x) = \Delta(x) \tag{2.4.21}$$

Definition 2.4.7. *A bialgebra $(H, \mu, \eta, \Delta, \varepsilon)$ is* quasi-cocommutative *if there exists an invertible element $R \in H \otimes H$ such that for any x,*

$$\tau_{H,H} \circ \Delta(x) = R\Delta(x)R^{-1} \tag{2.4.22}$$

Such an element R is called a *universal R-matrix* for the bialgebra.

Definition 2.4.8. *A quasi-cocommutative bialgebra $(H, \mu, \eta, \Delta, \varepsilon, R)$ is* braided *if R satisfies the conditions*

$$(\Delta \otimes \mathrm{id}_H)(R) = R_{13}R_{23} \tag{2.4.23}$$

$$(\mathrm{id}_H \otimes \Delta)(R) = R_{13}R_{12} \tag{2.4.24}$$

where $R_{ij} \in H \otimes H \otimes H$, $R_{ij} = \sum_i y_i^{(1)} \otimes y_i^{(2)} \otimes y_i^{(2)}$

$$y_i^{(k)} = \begin{cases} s_i & \text{if } k = i \\ t_i & \text{if } k = j \\ 1 & \text{else} \end{cases} \tag{2.4.25}$$

For example $R_{13} = \sum_i s_i \otimes 1 \otimes t_i$.

It can be shown that R satisfies the Yang-Baxter equation

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12} \tag{2.4.26}$$

We will see in 3.7.1 how this leads to a braiding on the category of representations.

Chapter 3
Categorical Background

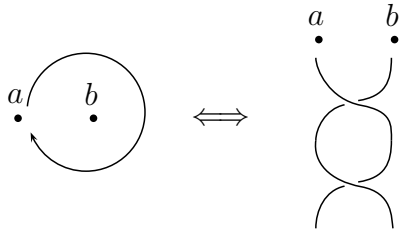
Any anyonic model corresponds to a modular tensor category. In this chapter we give a series of definitions leading up to the definition of a modular tensor category. Before delving into categorical definitions, however, we give a sketch of the correspondence between an anyonic model and a modular tensor category to motivate the upcoming definitions. The basic idea is that anyons correspond to objects and anyon types correspond to isomorphism classes of simple objects. So,

- Anyons correspond to objects.
- In any anyonic model, there are a finite number of *charges* or *types*. These correspond to isomorphism classes of simple objects.
- Anyons are the basic entities of the theory, and any object is constructed from them. In categorical terms, the category must be *semisimple*.
- Systems of several anyons correspond to tensor products of anyons: the category is *monoidal*. These tensor products decompose as direct sums of anyons, e.g.

$$a \otimes b \simeq 2a \oplus 3c \tag{3.0.1}$$

The physical interpretation of this is that if an anyon of type a fuses with an anyon with type b, the result is either an anyon of type a, in one of two possible ways, or an anyon of type b, in one of three possible ways. The trivial charge corresponds to the tensor unit.

– Exchanging anyons corresponds to braiding their worldlines, which in the category corresponds to applying an appropriate braiding isomorphism to the system of anyons. In other words, the category is *braided*.



– The conjugate of a charge corresponds to its *dual*: the category is *rigid*.

– Anyons are extended objects, so that their worldlines become twisted under rotation. The corresponding mathematical formalism is that of a braided *ribbon category*.

To summarize, the category must be semisimple, monoidal, braided, rigid, and ribbon. A category with all these properties that satisfies one additional condition is called a modular tensor category. We will explain this condition and discuss modular tensor categories in more detail in Section 3.6. In this chapter, we give abstract definitions for all the properties a MTC needs to satisfy. We also show that the category of representations of any Hopf algebra is a rigid monoidal category, since the modular tensor categories we will be interested in are constructed from categories of representations of Hopf algebras.

3.1 Monoidal categories

Definition 3.1.1. *A* monoidal category *is a category* $\mathcal{C}$ *with*

i) a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$

ii) a unit object $\mathbf{1}$ *and natural isomorphisms*

$$\lambda_V : \mathbf{1} \otimes V \xrightarrow{\sim} V \tag{3.1.1}$$

$$\rho_V : V \otimes \mathbf{1} \xrightarrow{\sim} V \tag{3.1.2}$$

iii) a natural isomorphism

$$\alpha_{UVW}(U \otimes V) \otimes W \xrightarrow{\sim} U \otimes (V \otimes W) \tag{3.1.3}$$

iv) if X_1, X_2 *are two objects obtained from* $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ *by inserting* $\mathbf{1}$*s and brackets, then all isomorphisms* $\varphi : X_1 \xrightarrow{\sim} X_2$ *composed of* α*s,* λ*s, and* ρ*s are equal.* [1]

v) $\mathbf{1}$ *is a simple object and* $\mathrm{End}_{\mathcal{C}} \mathbf{1} = k$

In the context of topological quantum computing, the unit object should be thought of as the trivial anyon. The fact that $\mathbf{1} \otimes V \xrightarrow{\sim} V$ in a natural way should be taken to mean that fusing a trivial anyon with any other anyon has no effect.

Example 3.1.2. *i) The category of* k*-vector spaces* $\mathrm{Vec}(k)$

ii) The category of finite dimensional representations of a group, algebra, or Lie algebra

1. This is usually presented as a theorem that follows from the fact that a particular diagram, the "pentagon", is required to commute

3.2 Rigid monoidal categories

A rigid monoidal category is a monoidal category where there is a notion of a dual. This corresponds to the notion of charge conjugation: every anyon type T has a unique conjugate type T^* which fuses with it to give the trivial charge.

Definition 3.2.1. *Let $\mathcal{C}$ be a monoidal category, V an object in $\mathcal{C}$. A* right dual *to V is an object V^* with two morphisms*

$$e_V : V^* \otimes V \to \mathbf{1} \tag{3.2.1}$$

$$i_V : \mathbf{1} \to V \otimes V^* \tag{3.2.2}$$

such that the composition

$$V \xrightarrow{i_V \otimes \mathrm{id}_V} V \otimes V^* \otimes V \xrightarrow{\mathrm{id}_V \otimes e_V} V \tag{3.2.3}$$

is equal to id_V, and similarly the composition

$$V^* \xrightarrow{\mathrm{id}_{V^*} \otimes i_V} V^* \otimes V \otimes V^* \xrightarrow{e_V \otimes \mathrm{id}_{V^*}} V^* \tag{3.2.4}$$

is equal to id_{V^*}

The morphisms i_V and e_V can be thought of as encoding the way in which V^* and V fuse to yield the trivial charge.

3.3 Braided monoidal categories

The central operation in topological quantum computing is that of exchanging two anyons. Mathematically, the structure we need to model this is that of a braided monoidal category: any trajectory where a set of anyons are rearranged corresponds to an element of the braid group. A braided monoidal category is a monoidal category $\mathcal{C}$ with a natural isomorphism

$$\sigma_{V,W} : V \otimes W \to W \otimes V \tag{3.3.1}$$

For $V_1, V_2, \ldots, V_n \in \mathcal{C}$, consider expressions of the form

$$((V_{i_1} \otimes V_{i_2}) \otimes (V_{i_3} \otimes 1)) \otimes \cdots \otimes V_{i_n} \tag{3.3.2}$$

obtained from $V_1, V_2, \ldots, V_n$ by adding brackets and $\mathbf{1}$s.

To any composition of αs, λs, and ρs, assign an element of the braid group B_n as follows:

$$\alpha, \lambda, \rho \mapsto \mathbf{1} \tag{3.3.3}$$

$$\sigma_{V_{i_k}, V_{i_{k+1}}} \mapsto b_k \tag{3.3.4}$$

Definition 3.3.1. *A* braided tensor category *is a monoidal category with natural isomorphisms $\sigma_{X,Y}$ as above such that any $\varphi : X_1 \to X_2$ obtained by composing αs, λs, ρs, and σs depends only on its image in B_n.*

Definition 3.3.2. *A braided tensor category is called* symmetric *if $\sigma_{X,Y} \circ \sigma_{Y,X} = \mathrm{id}_{X \otimes Y}$ for any objects X, Y.*

Some examples of symmetric tensor categories include:

– The category **Vect** of finite dimensional vector spaces over a field k.

3.4 Ribbon categories

Anyons can be rotated so that their worldlines become twisted. This requires more structure than in a braided monoidal category. In ribbon categories, it is possible to define a natural twisting isomorphism $\theta_V : V \to V$ for each V. It is also possible to define the notion of a *trace*, which will be important later on.

Definition 3.4.1. *A* ribbon category *is a rigid braided tensor category with a natural isomorphism*

$$\delta_V : V \to V^{**} \tag{3.4.1}$$

such that

i) $\delta_{V\otimes W} = \delta_V \otimes \delta_W$

ii) $\delta_{\mathbf{1}} = \mathrm{id}$

iii) $\delta_{V^*} = (\delta_V^*)^{-1}$

In any rigid braided tensor category, we can construct natural isomorphisms

$$\psi_V : V^{**} \to V \tag{3.4.2}$$

via the composition

$$V^{**} \xrightarrow{i\otimes \mathrm{id}} V \otimes V^* \otimes V^{**} \xrightarrow{id\otimes\sigma^{-1}} V \otimes V^{**} \otimes V^* \xrightarrow{id\otimes e} V \tag{3.4.3}$$

Define the twist maps θ_V by

$$\theta_V = \psi_V \delta_V \tag{3.4.4}$$

If V is an object in a ribbon category $\mathcal{C}$ and f an endomorphism of V, we can define the trace of f by the composition

$$\mathbf{1} \xrightarrow{i_V} V \otimes V^* \xrightarrow{f \otimes \mathrm{id}} V \otimes V^* \xrightarrow{\delta_V \otimes \mathrm{id}} V^{**} \otimes V^* \xrightarrow{e_{V^*}} \mathbf{1} \tag{3.4.5}$$

We define the dimension of an object V to be $\dim V = \operatorname{tr} \mathrm{id}_V$.

3.5 Semisimple categories

Any object in a modular tensor category is constructed from simple objects, which correspond to anyon types: MTCs are *semisimple*.

Definition 3.5.1. *A category $\mathcal{C}$ is called* abelian *if it satisfies the conditions:*

i) All the hom sets $\mathrm{Hom}(A, B)$ *are k-vector spaces, and the composition*

$$(\varphi, \psi) \mapsto \varphi \circ \psi \tag{3.5.1}$$

is k-bilinear.

ii) There is a zero object $\mathbf{0} \in \mathrm{Ob}\,\mathcal{C}$ *such that* $\mathrm{Hom}(\mathbf{0}, V) = \mathrm{Hom}(V, \mathbf{0}) = \mathbf{0}$ *for every object V*

iii) Finite direct sums exist in $\mathcal{C}$

iv) Every morphism φ has a kernel $\ker\varphi$ *and a cokernel* $\operatorname{coker}\varphi$*. Every morphism is a composition of an epimorphism followed by a monomorphism. If* $\ker\varphi = 0$*, then* $\varphi = \ker(\operatorname{coker}\varphi)$*. If* $\operatorname{coker}\varphi = 0$*, then* $\varphi = \operatorname{coker}(\ker\varphi)$*.*

Examples of abelian categories include the category of finite-dimensional k-vector spaces, the category of finite dimensional k-vector spaces, and the category of representations of a group G over k.

Definition 3.5.2. *An object U in an abelian category is called* simple *if any injection $V \hookrightarrow U$ is either 0 or an isomorphism.*

Definition 3.5.3. *An abelian category $\mathcal{C}$ is* semisimple *if any object V is isomorphic to a direct sum of simple objects*

$$V \simeq \bigoplus iN_iV_i \tag{3.5.2}$$

where the V_i are simple objects, $N_i \in \mathbf{N}$

Suppose that $\mathcal{C}$ is a semisimple ribbon category. Let I be the set of equivalence classes of nonzero simple objects in $\mathcal{C}$ and choose a representative V_i for each equivalence class $i \in I$.

We can define the *fusion coefficients* $N_{ij}^k \in \mathbf{N}$.

$$V_i \otimes V_j \simeq \bigoplus_k N_{ij}^k V_k \tag{3.5.3}$$

We call each equation of this type a *fusion rule*. These equations describe how anyons fuse to form new anyons.

3.6 Modular tensor categories

The mathematical structure that describes anyons is that of modular tensor categories. The definition of modular tensor categories first appeared in [24]. They arise in conformal field theory and also from quantum groups: we will explain how they arise from quantum groups in Chapter 5. They have applications to topological quantum field theory: Reshetikhin and Turaev associated a TQFT in 2+1 dimensions to every MTC. An exposition is in Bakalov & Kirillov [21].

Essentially modular tensor categories are a special type of braided tensor category. The *symmetric center* $\mathbf{Z}_2(\mathcal{C})$ of a braided category $\mathcal{C}$ is a full subcategory with

$$\mathrm{Ob}\,\mathbf{Z}_2(\mathcal{C}) = \{x \in \mathcal{C} : \sigma_{XY} \circ \sigma_{YX} = \mathrm{id}\ \ \forall\, Y \in \mathcal{C}\} \tag{3.6.1}$$

The symmetric center is a measure of "how commutative" $\mathcal{C}$ is. In a symmetric category, $\mathbb{Z}_2(\mathcal{C}) = \mathcal{C}$. A modular tensor category is in this sense the opposite of a symmetric category:

Definition 3.6.1. *A modular tensor category is a semisimple ribbon category such that* $\mathbf{Z}_2(\mathcal{C})$ *is trivial*

These categories are called modular because each one gives rise to a projective representation of the modular group $SL(2,\mathbb{Z})$.

In any semisimple rigid braided tensor category, define the *S-matrix*

$$s_{X,Y} = \mathrm{tr}_{X\otimes Y}(\sigma_{Y,X} \circ \sigma_{X,Y}) \tag{3.6.2}$$

for every simple object X, Y.

It is proved in [26] that

Theorem 3.6.2. $\mathbf{Z}_2(\mathcal{C})$ *is trivial if and only if the matrix* s *is invertible.*

This is the original definition of a modular tensor category.

3.7 The category of representations of a Hopf algebra

In this section we show that the category of representations of any Hopf algebra is a rigid monoidal category. Anyonic models are constructed from categories of representations of Hopf algebras.

Suppose $(H, \mu, \eta, \Delta, \varepsilon, S)$ is a Hopf algebra.

Let $\mathrm{Rep}_f H$ be the category of finite dimensional representations of H as a k-algebra.

If A is an algebra and U, V are A-modules, then $U \otimes V$ is a vector space. However, there is no natural way to impose an A-module structure on $U \otimes V$. The comultiplication Δ on H allows us to impose a H-module structure on the tensor product $U \otimes V$ of two H-modules U, V as follows.

Suppose $\Delta(h) = \sum_i h_i^{(1)} \otimes h_i^{(2)}$. Then we define

$$h(u \otimes v) = \sum_i h_i^{(1)} u \otimes h_i^{(2)} v \tag{3.7.1}$$

We define the tensor unit using the counit ε: $\mathbf{1}$ is the vector space k, with

$$h(1) = \varepsilon(h)\mathbf{1} \tag{3.7.2}$$

for any $h \in H$.

So we have that $\mathrm{Rep}_f(H)$ is a monoidal category, with this tensor product. Only the counit and the comultiplication are required for this definition, so in fact the category of representations of any bialgebra is a monoidal category.

We can use the antipode S to define duals as follows:

For any module U, let the dual U^* be the dual vector space of linear functionals on U, with action

$$(h \cdot \varphi)(u) = \varphi(S(h)u) \tag{3.7.3}$$

It follows that $\mathrm{Rep}_f(H)$ is a rigid monoidal category. This also serves as motivation for the definition of a Hopf algebra: it is an algebra with additional structures such that its category of representations is monoidal and rigid.

3.7.1 Braided structure

Recall Definition 2.4.8 where we defined what it means for a bialgebra to be braided. In this section we will sketch the proof of the following theorem, which justifies the terminology. The details of the proof can be found in [19].

Theorem 3.7.1. *Let $(H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra. The category $\mathrm{Rep}_f(H)$ is braided if and only if H is braided.*

Proof. Suppose $(H, \mu, \eta, \Delta, \varepsilon)$ has a universal R-matrix R. Let V, W be two H-modules, and $R = \sum_i s_i \otimes t_i$.

We can define a natural isomorphism $\sigma^R_{V,W}$ between $V \otimes W$ and $W \otimes V$ by

$$\sigma^R_{V,W} = \tau_{V,W}(R(v \otimes w)) = \sum_i t_i w \otimes s_i v \tag{3.7.4}$$

Conversely, let $(H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra, and suppose the category $\mathrm{Rep}_f(H)$ has a braiding σ. Define

$$R = \tau_{H,H}(\sigma_{H,H}(\mathbf{1} \otimes \mathbf{1})) \tag{3.7.5}$$

Then it turns out that R is a universal R-matrix for H and H is a braided bialgebra. □

Chapter 4
Quantum Groups at Roots of Unity

Models of anyons are usually presented as modular tensor categories for reasons explained in the introduction. One important source of modular tensor categories, and hence possible models of anyonic quantum computing, is the theory of quantum groups. The category of representations of a quantum group does not form a modular tensor category directly, however, after suitable constructions, a modular tensor category can be constructed from the category of representations of a quantum group. The main goal of this chapter is to introduce quantum groups.

There is no agreed upon definition of quantum group, rather, there are a number of examples that are called quantum groups. The concept arose in inverse scattering theory [8] and also in earlier work by Yang [36] on the factorizability of certain transfer matrices in statistical mechanics. This was later expanded by Baxter [3] and led to the Yang-Baxter equation. The abstract presentation of these ideas is due to M. Jimbo [16] and V. Drinfeld [7]. Essentially quantum groups are certain kinds of Hopf algebras and are, in general, neither commutative nor cocommutative. The ones of so-called Drinfeld-Jimbo type arise as deformations of the universal enveloping algebra of Lie algebras.

In this chapter we will define and describe in detail the representation theory of the quantum group $U_q(\mathfrak{sl}(2))$ at a root of unity, which arises as a deformation of the Lie algebra $\mathfrak{sl}(2)$. We will also give a braiding on the category of representations and discuss briefly the general case, of $U_q(\mathfrak{g})$ for any semisimple Lie algebra $\mathfrak{g}$, an exposition of which can be found in [30].

4.1 The quantum group $U_q(\mathfrak{sl}(2))$

The quantum group $U_q(\mathfrak{sl}(2))$ is a Hopf algebra which is a deformation of the universal enveloping algebra $U(\mathfrak{sl}(2))$ defined in Example 2.4.6. In this section we will define the algebra $U_q(\mathfrak{sl}(2))$, explain its relationship to $U(\mathfrak{sl}(2))$, and give the Hopf algebra structure on $U_q(\mathfrak{sl}(2))$.

Recall that the algebra $U(\mathfrak{sl}(2))$ is generated by X^+, X^-, H with relations

$$[X^+, X^-] = H \tag{4.1.1}$$

$$[H, X^+] = 2X^+ \tag{4.1.2}$$

$$[H, X^-] = -2X^- \tag{4.1.3}$$

where $[\cdot, \cdot]$ is the commutator.

X^+ and X^- act as raising and lowering operators on the representations of $U(\mathfrak{sl}(2))$. In the representation $V_n = \text{span}\{v_0, \ldots, v_n\}$:

$$Hv_i = (n-2i)v_i \tag{4.1.4}$$

$$X^+v_i = (n-i+1)v_{i-1} \qquad \text{for } i > 0 \tag{4.1.5}$$

$$X^-v_i = (i+1)v_{i+1} \qquad \text{for } i < n \tag{4.1.6}$$

Before giving the definitions of $U_q(\mathfrak{sl}(2))$, we introduce the concept of q-integers. These are combinatorial objects studied as far back as the early 19^{th} century. Interestingly, they have come to play an important role in the modern theory of quantum groups.

$$[n]_q = \frac{q^n - q^{-n}}{q - q^{-1}} = q^{n-1} + q^{n-3} + \cdots + q^{-n+3} + q^{-n+1} \tag{4.1.7}$$

The $[n]_q$ are called *q-integers*. Like quantum groups they may be viewed as deformations, in this case of ordinary integers. We also define the q-factorial and q-binomial coefficients as follows:

$$[n]!_q = [n]_q[n-1]_q \cdots [1]_q \tag{4.1.8}$$

$$\binom{n}{k}_q = \frac{[n]!_q}{[n-k]!_q[k]!_q} \tag{4.1.9}$$

$q^{2d} = 1$ if and only if $[d]_q = 0$, so $[n]_q \neq 0$ for every nonzero integer when q is not a root of unity. When q is an ℓ^{th} root of unity, $[n]_q = 0$ when ℓ divides n.

Definition 4.1.1. *Let q be an indeterminate. $U_q(\mathfrak{sl}(2))$ is the associative algebra over the field of fractions $\mathbb{C}(q)$ with generators X^+, X^-, K, K^{-1} and relations*

$$KK^{-1} = 1 = K^{-1}K \tag{4.1.10}$$

$$KX^{+}K^{-1} = q^2X^{+} \tag{4.1.11}$$

$$KX^{-}K^{-1} = q^{-2}X^{-} \tag{4.1.12}$$

$$[X^{+}, X^{-}] = \frac{K - K^{-1}}{q - q^{-1}} \tag{4.1.13}$$

X^+ and X^- should be thought of as the analogues of the eponymous raising and lowering operators in $U(\mathfrak{sl}(2))$. This last equation can be thought of as replacing

$$[X^{+}, X^{-}] = H \tag{4.1.14}$$

with the "quantum version"

$$[X^{+}, X^{-}] = [H]_q = \frac{q^H - q^{-H}}{q - q^{-1}} \tag{4.1.15}$$

Of course q^H does not make sense here, so we introduce a new element K to take the place of q^H and obtain Equation 4.1.13. X^+ and X^- act as raising and lowering operators in representations of $U_q(\mathfrak{sl}(2))$ the same way as in $U(\mathfrak{sl}(2))$. To see the relationship between $U_q(\mathfrak{sl}(2))$ and $U(\mathfrak{sl}(2))$, we will make use of an alternate presentation of $U_q(\mathfrak{sl}(2))$. Define $U_q'(\mathfrak{sl}(2))$ to be the associative algebra with generators X^+, X^-, L, K, K^{-1} and relations

$$KK^{-1} = 1 \qquad K^{-1}K = 1 \tag{4.1.16}$$

$$KX^+K^{-1} = q^2X^+ \qquad KX^-K^{-1} = q^{-2}X^- \tag{4.1.17}$$

$$[X^+, X^-] = L \qquad (q - q^{-1})L = K - K^{-1} \tag{4.1.18}$$

$$[L, X^+] = q(X^+K + K^{-1}X^+) \qquad [L, X^-] = -q^{-1}(X^-K + K^{-1}X^-) \tag{4.1.19}$$

A long but straightforward calculation shows that $U_q(\mathfrak{sl}(2)) \simeq U_q'(\mathfrak{sl}(2)$. Define the algebra $U_1'(\mathfrak{sl}(2))$ over $\mathbb{C}$ having the same generators and relations as $U_q'(\mathfrak{sl}(2))$ with q replaced by 1. It is easily seen that

$$U_1'(\mathfrak{sl}(2))/(K-1) \simeq U(\mathfrak{sl}(2)) \tag{4.1.20}$$

by sending $X^+ \mapsto X^+, X^- \mapsto X^-, L \mapsto H, K \mapsto 1$. This gives some justification for calling $U_q(\mathfrak{sl}(2))$ a deformation of $U(\mathfrak{sl}(2))$.

We can define a Hopf algebra structure on $U_q(\mathfrak{sl}(2))$ as follows:

The comultiplication and counit are given by

$$\Delta(X^+) = 1 \otimes X^+ + X^+ \otimes K \qquad \Delta(X^-) = K^{-1} \otimes X^- + X^- \otimes 1 \tag{4.1.21}$$

$$\Delta(K) = K \otimes K \qquad \Delta(K^{-1}) = K^{-1} \otimes K^{-1} \tag{4.1.22}$$

$$\varepsilon(X^+) = \varepsilon(X^-) = 0 \qquad \varepsilon(K) = \varepsilon(K^{-1}) = 1 \tag{4.1.23}$$

and the antipode by

$$S(X^+) = -X^+K^{-1} \qquad S(X^-) = -KX^- \tag{4.1.24}$$

$$S(K) = K^{-1} \qquad S(K^{-1}) = K \tag{4.1.25}$$

It is straightforward to check that this defines a Hopf algebra structure. This looks quite similar to the Hopf algebra structure on $U(\mathfrak{sl}(2))$ defined in Example 2.4.6, and in fact the isomorphism $U_1'(\mathfrak{sl}(2))/(K-1) \simeq U(\mathfrak{sl}(2))$ is an isomorphism of Hopf algebras.

4.2 Representations of $U_q(\mathfrak{sl}(2))$

The representation theory of $U_q(\mathfrak{sl}(2))$ bears a striking resemblance to that of $\mathfrak{sl}(2)$ discussed in 2.3.1. In particular, in $U_q(\mathfrak{sl}(2))$:

i) Every finite dimensional representation is completely reducible.

ii) The eigenvectors of K form a basis for any irreducible representation. Their eigenvalues are called *weights* and are all integer powers of q. The eigenspaces of each eigenvalue *weight spaces*.

iii) Each irreducible representation has a highest weight vector

iv) The irreducible representations are classified by highest weights much as in $\mathfrak{sl}(2)$.

The proofs of these facts are also more or less analogous to those in $U(\mathfrak{sl}(2))$, though not always in a straightforward way. For proofs of i), ii), see [19] or [15]. We will sketch the classification of the irreducible representations of $U_q(\mathfrak{sl}(2))$ here.

Claim 4.2.1. *Let M be a finite dimensional $U_q(\mathfrak{sl}(2))$-module. Then there is an eigenvector $v_0 \in M$ of K such that $X^+ v_0 = 0$. We call v_0 a* highest weight vector.

Proof. Suppose not. Let v be an eigenvector of K with eigenvalue λ. $KX^+ = q^2X^+K$, so it follows that $(X^+)^i v$ is an eigenvector of K with eigenvalue $q^{2i}\lambda$. Each value $q^{2i}\lambda$ is different, therefore K has infinitely many eigenvectors.

This is impossible, so some $(X^+)^i v$ must be zero. Let i be the smallest such, and choose $v_0 = (X^+)^{i-1}v$. □

We now have that any irreducible representation of U_q is generated by a highest weight vector. We can now show how to classify the irreducible representations.

For any $\lambda \in \mathbb{C}(q), \lambda \neq 0$ there is an infinite-dimensional $U_q(\mathfrak{sl}(2))$-module $M(\lambda)$ called a *Verma module* with basis $v_0, v_1, v_2, \ldots$ such that for any i,

$$Kv_i = \lambda q^{n-2i} v_i \tag{4.2.1}$$

$$X^- v_i = v_{i+1} \tag{4.2.2}$$

$$X^+ v_i = \begin{cases} 0 & \text{if } i = 0 \\ [i]_q \frac{\lambda q^{1-i} - \lambda^{-1} q^{i-1}}{q - q^{-1}} v_{i-1} & \text{else} \end{cases} \tag{4.2.3}$$

To see that this a $U_q(\mathfrak{sl}(2))$-module, we can note that $M(\lambda)$ is isomorphic to the quotient of $U_q(\mathfrak{sl}(2))$ by the left ideal generated by X^+ and $K - \lambda$,

$$M(\lambda) \simeq U_q(\mathfrak{sl}(2))/(U_q(\mathfrak{sl}(2))X^+ + U_q(\mathfrak{sl}(2))(K - \lambda)) \tag{4.2.4}$$

with v_i being the coset of $(X^-)^i$. It follows from this that if M is a $U_q(\mathfrak{sl}(2))$-module and $v \in M$ is such that $X^+ v = 0$ and $Kv = \lambda v$, there is a unique homomorphism $\varphi : M(\lambda) \to M$ where $\varphi(v_0) = v$. If M is simple, then this homomorphism must be surjective and it follows that M is a quotient of $M(\lambda)$.

We now have that

Claim 4.2.2. *Any finite dimensional simple $U_q(\mathfrak{sl}(2))$-module is a quotient of $M(\lambda)$.*

Claim 4.2.3. *$M(\lambda)$ is simple for $\lambda \neq \pm q^n$*

Proof. See [15]. □

For $\lambda = \pm q^n$, $M(\lambda)$ has one nontrivial submodule spanned by the v_i with $i \geq n+1$. This leads us to the following characterization (details can be found in [15]):

For each integer $n \geq 0$, there are two unique (up to isomorphism) representations of $U_q(\mathfrak{sl}(2))$ of dimension $n+1$. The representations are $V_q(n)$ with basis $\left\{v_0^+, \ldots, v_n^+\right\}$, and $V_q^-(n)$ with basis $\left\{v_0^-, \ldots, v_n^-\right\}$ with action defined by

$$Kv_i^+ = q^{n-2i}v_i^+ \qquad Kv_i^- = -q^{n-2i}v_i^-$$

$$X^-v_i^+ = \begin{cases} [i+1]_q v_{i+1} & \text{if } i < n \\ 0 & \text{if } i = n \end{cases} \qquad X^-v_i^- = \begin{cases} [i+1]_q v_{i+1}^- & \text{if } i < n \\ 0 & \text{if } i = n \end{cases}$$

$$X^+v_i^+ = \begin{cases} [n-i+1]_q v_{i-1} & \text{if } i > 0 \\ 0 & \text{if } i = 0 \end{cases} \qquad X^+v_i^- = \begin{cases} -[n-i+1]_q v_{i-1}^- & \text{if } i > 0 \\ 0 & \text{if } i = 0 \end{cases}$$

Note that these representations are much the same as the representations of $\mathfrak{sl}(2)$, with the integers in the action of X^+ and X^- replaced by q-integers. By the proof sketched above, these are the only representations of $U_q(\mathfrak{sl}(2))$. Note that the representations $V_q^-(n)$ can be obtained by $V_q(n)$ by tensoring with the one-dimensional representation $V_q^-(0)$: essentially the difference from $U(\mathfrak{sl}(2))$ here is

that there are 2 nonisomorphic 1-dimensional representations of $U_q(\mathfrak{sl}(2))$. We will therefore restrict our attention to the representations $V_q(n)$.

If we consider tensor products of these representations $V_q(n)$, we find another similarity with the representation theory of $\mathfrak{sl}(2)$. It is well known that the tensor product of two irreducible representations $V(n), V(m)$ of $\mathfrak{sl}(2)$ $(n \geq m)$ decomposes as follows:

$$V(n) \otimes V(m) \simeq V(n-m) \oplus V(n-m+2) \oplus \cdots \oplus V(n+m-2) \oplus V(n+m) \quad (4.2.5)$$

Exactly the same formula holds for the irreducible representations $V_q(n)$. See [19] for a proof.

$$V_q(n) \otimes V_q(m) \simeq V_q(n-m) \oplus V_q(n-m+2) \oplus \cdots \oplus V_q(n+m-2) \oplus V_q(n+m) \quad (4.2.6)$$

4.3 Setting q to be a root of unity

We are interested in constructing modular tensor categories from quantum groups at roots of unity. In this section, we explain how to set the indeterminate q to be a complex root of unity in $U_q(\mathfrak{sl}(2))$. There are several different ways to set q to be a complex number z, which result in different algebras when z is a root of unity. We give two such ways below. We will take z to be an ℓ^{th} root of unity, $\ell \geq 3$ odd.

The first and most obvious way is, for any $z \in \mathbb{C}$ such that $z^2 \neq 0, 1$, to set $q = z$ in the definition (4.1.1) of $U_q(\mathfrak{sl}(2)$. Denote the algebra obtained in this way

by $U_z(\mathfrak{sl}(2))$. This algebra is of interest in its own right when z is a root of unity ([15] discusses it in detail), but does not lead us to a modular tensor category.

The second way is to let $\mathcal{A} = \mathbb{Z}[q, q^{-1}]$ and define a 'restricted' $\mathcal{A}$-subalgebra $U_{\mathcal{A}}^{res}(\mathfrak{sl}(2))$ to be the $\mathcal{A}$-subalgebra of $U_q(\mathfrak{sl}(2))$ generated by X^+ ,X^-,K,K^{-1}, $(X^+)^{(n)}$, $(X^-)^{(n)}$, where

$$(X^+)^{(n)} = \frac{(X^+)^n}{[n]_q^!} \tag{4.3.1}$$

$$(X^-)^{(n)} = \frac{(X^-)^n}{[n]_q^!} \tag{4.3.2}$$

Define

$$U_z^{res}(\mathfrak{sl}(2)) = U_{\mathcal{A}}^{res}(\mathfrak{sl}(2)) \otimes_{\mathcal{A}} \mathbb{C} \tag{4.3.3}$$

The objects in the MTC we will construct will be representations of this algebra. If z is not a root of unity, then $U_z^{res}(\mathfrak{sl}(2))$ and $U_z(\mathfrak{sl}(2))$ are isomorphic. When z is an ℓ^{th} root of unity, $\ell \geq 3$, the following result is obtained.

Lemma 4.3.1. *In $U_z^{res}(\mathfrak{sl}(2))$, $(X^+)^\ell = (X^-)^\ell = 0$ for all i*

Proof. $(X^+)^\ell = [\ell]_q^!(X^+)^{(\ell)} = 0$ as $[\ell]_q^! = 0$. Similarly for $(X^-)^\ell$. □

$(X^+)^\ell \neq 0$ in $U_z(\mathfrak{sl}(2))$, so it is clear that these algebras are not isomorphic when q is a root of unity.

4.4 The representation theory of $U_z^{res}(\mathfrak{sl}(2))$

Throughout this section z will be assumed to be an ℓ^{th} root of unity, where $\ell \geq 3$ is odd.

The objects of the MTC we are interested in are irreducible representations of $U_z^{res}(\mathfrak{sl}(2))$. Unlike in the case of $U_q(\mathfrak{sl}(2))$, not every representation of $U_z^{res}(\mathfrak{sl}(2))$ is completely reducible, and in general the representation theory is quite complicated. To get an idea of why this is the case, note that the argument in Claim 4.2.1 for why every representation has a highest weight breaks down when $q = z$, a root of unity, so there may not be a highest weight vector in general.

However, the modular tensor category we wish to construct comes from a subcategory of the category of representations, so it will be enough to understand a limited subset of the representations. In particular the representations we will study will always have highest weight vectors and will in fact be constructed from the irreducible representations of $U_q(\mathfrak{sl}(2))$. These representations are called *Weyl modules*, and we will define them in this section. The simple objects of our MTC will be irreducible Weyl modules.

Define a representation of U_z^{res} to be of *type* **1** if $K^\ell = 1$. As in $U_q(\mathfrak{sl}(2))$, any representation of U_z^{res} is isomorphic to the tensor product of a representation of type **1** with a one-dimensional representation. We can therefore restrict our attention to representations of type **1**.

Recall that in $U_q(\mathfrak{sl}(2))$ the irreducible representations $V_q(n)$ are indexed by integers $n \geq 0$. We will use these representations to define representations of $U_z^{res}(\mathfrak{sl}(2))$ as follows.

Let $V_q(n)$ be the irreducible $U_q(\mathfrak{sl}(2))$-module defined in section 4.2. Let $V_{\mathcal{A}}^{res}(n)$ be the $U_{\mathcal{A}}^{res}$-submodule of $V_q(n)$ generated by v_0, and define the *Weyl module*

$$W_z^{res}(n) = V_{\mathcal{A}}^{res}(n) \otimes_{\mathcal{A}} \mathbb{C} \tag{4.4.1}$$

More concretely, the Weyl module $W_z^{res}(n)$ has basis $\{v_0, v_1, \ldots, v_n\}$, and

$$X^+ v_i = [n-i+1]_z v_{i-1} \tag{4.4.2}$$

$$(X^+)^{(\ell)} v_i = ((n-i)_1) + 1) v_{i-\ell} \tag{4.4.3}$$

$$(X^-)^{(\ell)} v_i = (i_1 + 1) v_{i+\ell} \tag{4.4.4}$$

$$X^- v_i = [i+1]_z v_{i+1} \tag{4.4.5}$$

$$K v_i = z^{n-2i} v_i \tag{4.4.6}$$

$$\tag{4.4.7}$$

where for any integer r, r_0, r_1 are defined such that $r = r_0 + \ell r_1$ and $0 \leq r_0 < \ell$.

Claim 4.4.1. *$W_z^{res}(n)$ is irreducible if and only if $n < \ell$ or $\ell \mid (n+1)$*

Proof. See [30] □

In the case that $W_z^{res}(n)$ is not irreducible, it is not too difficult to prove the following proposition about the structure of $W_z^{res}(n)$. This proposition lets us construct what turn out to be all the irreducible $U_z^{res}(\mathfrak{sl}(2))$-modules.

Proposition 4.4.2. *Let V' be the subspace of $W_z^{res}(n)$ spanned by the v_r such that $n_0 < r_0 < \ell$ and $r_1 < m_1$*

i) V' is the only proper U_z^{res}-submodule of $W_z^{res}(n)$

ii) $V' \simeq V_z^{res}(m)$, where $m = \ell - 2 - n_0 + \ell(n_1 - 1)$

iii) $W_z^{res}(n)/V'$ is irreducible

It follows that each $W_z^{res}(n)$ has a unique irreducible quotient module $V_z^{res}(n) = W_z^{res}(n)/V'$.

The proofs of the following two theorems about the structure of irreducible representations of $U_z^{res}(\mathfrak{sl}(2))$ can be found in [30]. We record these theorems here to give some more intuition about the structure of the category of representations of $U_z^{res}(\mathfrak{sl}(2))$.

Theorem 4.4.3. *Every finite-dimensional irreducible U_z^{res}-module of type* **1** *is isomorphic to some $V_z^{res}(n)$*

This tells us that even though the Weyl modules are not irreducible as with $\mathfrak{sl}(2)$, every irreducible module is the unique quotient of a Weyl module.

Theorem 4.4.4. $V_z^{res}(n) \simeq V_z^{res}(n_0) \otimes V_z^{res}(\ell n_1)$

where again $n = n_0 + \ell n_1$, $0 \leq n_0 < \ell$. We can see from this that in some sense understanding the modules $V_z^{res}(n) \simeq W_z^{res}(n)$ for $0 \leq n < \ell$ takes us a long way towards understanding all irreducible modules. Our anyon types will correspond to these irreducible Weyl modules.

4.5 A braiding for $U_z^{res}(\mathfrak{sl}(2))$

To construct a MTC from the representations of $U_z^{res}(\mathfrak{sl}(2))$, we need a braiding on the category of representations as defined in Section 3.3. In this section we will give a braiding $\sigma_{V,W} : V \otimes W \to W \otimes V$ for certain representations V, W of $U_z^{res}(\mathfrak{sl}(2))$. This braiding does not come from a universal R-matrix for $U_z^{res}(\mathfrak{sl}(2))$ as discussed in 2.4.4, but is derived from a universal R-matrix for a larger algebra. Throughout V and W will be assumed to be representations which are the direct sums of their weight spaces. We give an explicit form for all the elements in this braiding since being able

to compute the braiding morphisms is important when studying topological quantum computation.

Details of this construction, including much more motivation for the R-matrix $\tilde{R}_q$ below, can be found in [30].

Define

$$\tilde{R}_q = \sum_{t=0}^{\infty} q^{\frac{1}{2}t(t+1)} \frac{(1-q^{-2})^t}{[t]_q^!} ((X^+)^t \otimes (X^-)^t) \tag{4.5.1}$$

This will be our "universal R-matrix". Of course, this is not an element of $U_z^{res}(\mathfrak{sl}(2)) \otimes U_z^{res}(\mathfrak{sl}(2))$ as the sum is infinite; it lies in a completion of $U_z^{res}(\mathfrak{sl}(2)) \otimes U_z^{res}(\mathfrak{sl}(2))$. However, each of the terms in the sum is an element of $U_z^{res}(\mathfrak{sl}(2)) \otimes U_z^{res}(\mathfrak{sl}(2))$. For any two irreducible finite dimensional representations $\rho_V : U_z^{res}(\mathfrak{sl}(2)) \to \mathrm{End}(V)$, $\rho_W : U_z^{res}(\mathfrak{sl}(2)) \to \mathrm{End}(W)$, all but finitely many terms in the sum act as zero on $V \otimes W$. In other words, $\rho_V \otimes \rho_W(\tilde{R}_q) \in \mathrm{End}(V \otimes W)$.

Define an invertible operator $E_{V,W}$ on $V \otimes W$ which acts as $\lambda\overline{\mu}$ on the weight subspace $V^\lambda \otimes W^\mu$. As remarked earlier, $\rho_V \otimes \rho_W(\tilde{R}_q)$ is a well-defined element of $\mathrm{End}(V \otimes W)$. Let

$$R_{V,W} = E_{V,W} \left(\rho_V \otimes \rho_W(\tilde{R}_q) \right) \tag{4.5.2}$$

Claim 4.5.1. *For any $x \in U_z^{res}(\mathfrak{sl}(2))$, V, W irreducible representations of $U_z^{res}(\mathfrak{sl}(2))$*

1. *$R_{V,W}(\rho_V \otimes \rho_W)(\Delta(x))R_{V,W}^{-1} = (\rho_V \otimes \rho_W)(\Delta^{op}(x))$*
2. *$R = R_{V,W}$ satisfies the Yang-Baxter equation:*

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12} \tag{4.5.3}$$

Proof. See [30]. □

We have therefore that

Theorem 4.5.2. *The category of finite dimensional $U_z^{res}(\mathfrak{sl}(2))$-modules of type* **1** *which are the direct sums of their weight spaces is a braided monoidal category, with braiding isomorphisms given by*

$$\sigma_{V,W}(v \otimes w) = R_{V,W}(w \otimes v) \tag{4.5.4}$$

4.6 The general case: $U_q(\mathfrak{g})$

In general we can define a quantum group $U_q(\mathfrak{g})$ for any semisimple Lie algebra $\mathfrak{g}$. The representations of the algebra $U_z^{res}(\mathfrak{g})$ where z is a root of unity give us a modular tensor category in the same way as those of $U_z^{res}(\mathfrak{sl}(2))$. This results in a rich array of examples of modular tensor categories. $U_q(\mathfrak{g})$ is a deformation of the universal enveloping algebra $U(\mathfrak{g})$ in the same way as $U_q(\mathfrak{sl}(2))$ is a deformation of $U(\mathfrak{sl}(2))$. Its representations are indexed by highest weights λ in the same way as the representations of $\mathfrak{g}$.

In this section we will give a definition of the quantum group $U_q(\mathfrak{g})$ in general, and touch briefly on its representation theory. The construction of the algebra $U_z^{res}(\mathfrak{g})$ where z is a complex number and the braiding on the category of representations of $U_z^{res}(\mathfrak{g})$ can be done almost exactly as with $\mathfrak{sl}(2)$. Chari and Pressley [30] discuss this general case extensively.

The definition of $U_q(\mathfrak{g})$ is modelled on the definition of $U_q(\mathfrak{sl}(2))$ and Serre's presentation of a semisimple Lie algebra $\mathfrak{g}$, which we give briefly here. More about this can be found in Humphreys [14].

Let $\mathfrak{g}$ be an arbitrary semisimple algebra. Suppose Π is a basis of the root system. There is a matrix associated to each semisimple Lie algebra $\mathfrak{g}$ called the *Cartan matrix*, which can be used to reconstruct $\mathfrak{g}$ by the presentation which follows. The Cartan matrix's entries are indexed by Π, and are:

$$a_{\alpha\beta} = 2(\alpha, \beta)/(\alpha, \alpha). \tag{4.6.1}$$

Then the Lie algebra has a presentation with $3|\Pi|$ generators $X_\alpha^+, X_\alpha^-, H_\alpha$, $\alpha \in \Pi$ and the relations

$$[H_\alpha, H_\beta] = 0 \qquad \left[X_\alpha^+, X_\beta^-\right] = \delta_{\alpha\beta} H_\alpha \tag{4.6.2}$$

$$\left[H_\alpha, X_\beta^+\right] = a_{\alpha\beta} X_\beta^+ \qquad \left[H_\alpha, X_\beta^-\right] = -a_{\alpha\beta} X_\beta^- \tag{4.6.3}$$

$$\mathrm{ad}_{X_\alpha^+}^{1-a_{\alpha\beta}}(X_\beta^+) = 0 \qquad \mathrm{ad}_{X_\alpha^-}^{1-a_{\alpha\beta}}(X_\beta^-) = 0 \tag{4.6.4}$$

Before giving the definition of $U_q(\mathfrak{g})$, we first define some notation to make writing out the definition more convenient.

Let $d_\alpha = \frac{(\alpha,\alpha)}{2} \in \{1, 2, 3\}$, and set

$$q_\alpha = q^{d_\alpha} \tag{4.6.5}$$

and for $n \in \mathbb{Z}$, define

$$[n]_\alpha = [n]_{q_\alpha} = \frac{q^{nd_\alpha} - q^{-nd_\alpha}}{q^{d_\alpha} - q^{-d_\alpha}} \tag{4.6.6}$$

$[n]^!_\alpha$ and $\binom{n}{k}_\alpha$ are defined similarly:

$$[n]^!_\alpha = [n]^!_{q_\alpha} \tag{4.6.7}$$

$$\binom{n}{k}_\alpha = \binom{n}{k}_{q_\alpha} \tag{4.6.8}$$

We can now define the quantum group $U_q(\mathfrak{g})$. Here as with the definition of $U_q(\mathfrak{sl}(2))$ the generators X^+_α, X^-_α, and H_α should be thought as the analogues of those in $\mathfrak{g}$. These last two equations look fairly monstrous, but are really just an expanded and deformed version of the relations 4.6.4.

Definition 4.6.1. *The quantum group $U_q(\mathfrak{g})$ has generators $X^+_\alpha, X^-_\alpha, K_\alpha, K^{-1}_\alpha$ for each $\alpha \in \Pi$, and relations*

$$K_\alpha K^{-1}_\alpha = 1 = K^{-1}_\alpha K_\alpha \tag{4.6.9}$$

$$K_\alpha K_\beta = K_\beta K_\alpha \tag{4.6.10}$$

$$K_\alpha X^+_\beta K^{-1}_\alpha = q^{(\alpha,\beta)} X^+_\beta \tag{4.6.11}$$

$$K_\alpha X^-_\beta K^{-1}_\alpha = q^{-(\alpha,\beta)} X^+_\beta \tag{4.6.12}$$

$$[X^+_\alpha, X^-_\beta] = \delta_{\alpha\beta} \frac{K_\alpha - K^{-1}_\alpha}{q_\alpha - q^{-1}_\alpha} \tag{4.6.13}$$

for all $\alpha, \beta \in \Pi$, and for $\alpha \neq \beta$

$$\sum_{s=0}^{1-a_{\alpha\beta}} (-1)^s \binom{1-a_{\alpha\beta}}{s}_{\alpha} (X^+)_\alpha^{1-a_{\alpha\beta}-s} X_\beta^+ (X^+)_\alpha^s = 0 \tag{4.6.14}$$

$$\sum_{s=0}^{1-a_{\alpha\beta}} (-1)^s \binom{1-a_{\alpha\beta}}{s}_{\alpha} (X^-)_\alpha^{1-a_{\alpha\beta}-s} (X^-)_\beta (X^-)_\alpha^s = 0 \tag{4.6.15}$$

We can define a Hopf algebra structure (Δ, ε, S) on $U_q(\mathfrak{g})$ such that for all $\alpha \in \Pi$,

$$\Delta(X_\alpha^+) = X_\alpha^+ \otimes 1 + K_\alpha \otimes X_\alpha^+ \qquad \varepsilon(X_\alpha^+) = 0 \qquad S(X_\alpha^+) = -K_\alpha^{-1} X_\alpha^+ \tag{4.6.16}$$

$$\Delta(X_\alpha^-) = X_\alpha^- \otimes K_\alpha^{-1} + 1 \otimes X_\alpha^- \qquad \varepsilon(X_\alpha^-) = 0 \qquad S(X_\alpha^-) = -X_\alpha^- K_\alpha \tag{4.6.17}$$

$$\Delta(K_\alpha) = K_\alpha \otimes K_\alpha \qquad \varepsilon(K_\alpha) = 1 \qquad S(K_\alpha) = K_\alpha^{-1} \tag{4.6.18}$$

We can set q to be a root of unity in essentially exactly the same way as with $U_q(\mathfrak{sl}(2))$: let $\mathcal{A} = \mathbb{Z}[q, q^{-1}]$ and define an $\mathcal{A}$-subalgebra $U_{\mathcal{A}}^{res}(\mathfrak{sl}(2))$ to be the $\mathcal{A}$-subalgebra of $U_q(\mathfrak{g})$ generated by X_α^+ ,X_α^-,K_α,K_α^{-1}, $(X_\alpha^+)^{(n)}$, $(X_\alpha^-)^{(n)}$, where

$$(X_\alpha^+)^{(n)} = \frac{(X_\alpha^+)^n}{[n]_q^!} \tag{4.6.19}$$

$$(X_\alpha^-)^{(n)} = \frac{(X_\alpha^-)^n}{[n]_q^!} \tag{4.6.20}$$

We will now briefly discuss the representation theory of $U_q(\mathfrak{g})$ and $U_z^{res}(\mathfrak{g})$.

The irreducible representations $V_q(\lambda)$ of type $\mathbf{1}$ of $U_q(\mathfrak{g})$ are indexed by highest weights λ and every representation is generated by a highest weight vector. The simultaneous eigenvectors of the K_α form a basis for the representation. We can use these representations to define representations of $U_z^{res}(\mathfrak{g})$ as follows:

Let $V_q(\lambda)$ be the irreducible $U_q(\mathfrak{g})$-module with highest weight λ. Let $V_{\mathcal{A}}^{res}(\lambda)$ be the $U_{\mathcal{A}}^{res}(g)$-submodule of $V_q(\lambda)$ generated by the highest weight vector v_λ, and define the *Weyl module*

$$W_z^{res}(\lambda) = V_{\mathcal{A}}^{res}(\lambda) \otimes_{\mathcal{A}} \mathbb{C} \tag{4.6.21}$$

via the homomorphism $\mathcal{A} \to \mathbb{C}$, $q \mapsto z$. Basically $W_z^{res}(n)$ has the same basis vectors and action of X^+, X^-, and H as $V_q(n)$, except with q set to z, and is defined so that it is a $U_z^{res}(\mathfrak{sl}(2))$-module.

As in the case of $\mathfrak{sl}(2)$, we will be most interested in the irreducible Weyl modules.

Claim 4.6.2. *$W_z^{res}(\lambda)$ is irreducible if either*

1. *$(\lambda + \rho, \hat{\alpha}) < \ell$ for all positive roots α*
2. *$\lambda = (\ell - 1)\rho + \ell\mu$ for some positive root μ*

Proof. See Chari & Pressley [30] □

The objects in the MTC constructed from the category of representations of $U_z^{res}(\mathfrak{g})$ are the irreducible Weyl modules $W_z^{res}(\lambda)$ such that $(\lambda + \rho, \hat{\alpha}) < \ell$ for all positive roots α.

Chapter 5
Modular Tensor Categories from $U_q(\mathfrak{sl}(2))$

The category of finite dimensional representations of $U_z^{res}(\mathfrak{sl}(2))$ which are direct sums of their weight spaces is a braided monoidal category: it is monoidal because $U_z^{res}(\mathfrak{sl}(2))$ is a Hopf algebra, and we saw that it is braided in Section 4.5. Call this category $\mathrm{Rep}_w(U_z^{res}(\mathfrak{sl}(2)))$. This category is certainly not a modular tensor category: it is not semisimple, and it has infinitely many nonisomorphic simple objects. The main goal of this chapter is to describe the passage from representations of quantum groups to modular tensor categories. The simple objects in the modular tensor category we construct will be $\{W_z^{res}(0), \ldots, W_z^{res}(\ell-2)\}$. We construct this category by first restricting to the subcategory of "tilting modules" and then quotienting this subcategory. Basically the intuition is that we take our simple objects to be $\{W_z^{res}(0), \ldots, W_z^{res}(\ell-2)\}$ and then quotient by the objects with quantum dimension zero. The simple objects in this modular tensor category will correspond to anyon types.

5.1 Quantum trace and dimension

The objects in $\mathrm{Rep}_w(U_q(\mathfrak{sl}(2)))$ are vector spaces, and so any endomorphism f has a trace $\mathrm{tr}(f)$. $\mathrm{Rep}_w(U_q(\mathfrak{sl}(2)))$ is a ribbon category, and we saw in Section 3.4 that there is a trace in any ribbon category. In $\mathrm{Rep}_w(U_q(\mathfrak{sl}(2)))$, this trace does *not* correspond to the usual trace of a linear map, and we will denote it by tr_q, the "quantum trace". It is a useful exercise to show from the definition that for any $f : V \to V$,

$$\mathrm{tr}_q(f) = \mathrm{tr}(Kf) \tag{5.1.1}$$

where tr is the usual trace of a linear map. We also define the quantum dimension $\dim_q$,

$$\dim_q(V) = \mathrm{tr}_q(\mathrm{id}_V) \tag{5.1.2}$$

For example, we can see from the definition of the Weyl module $W_z^{res}(n)$ in Section 4.4 that $\dim_q(W_z^{res}(n)) = [n+1]_z$. In particular we see that $\dim_q(W_z^{res}(\ell-1)) = 0$, so objects other than the zero object can have quantum dimension zero.

5.2 Tilting modules

We saw earlier that tensor products of irreducible $U_q(\mathfrak{sl}(2))$-modules $V_q(n)$ decompose as a direct sum of irreducible modules. This will not be the case for irreducible $U_z^{res}(\mathfrak{sl}(2))$-modules. However, $W_z^{res}(n) \otimes W_z^{res}(m)$ decomposes as a direct sum of indecomposable so-called *tilting modules*. In fact the indecomposable tilting modules

are exactly the direct summands of the tensor products of the Weyl modules. We will quotient the subcategory of tilting modules to obtain a modular tensor category.

In this section we will give a technical definition for tilting modules, define what they are explicitly in certain cases, and give an explicit decomposition for $W_z^{res}(n) \otimes W_z^{res}(m)$ for $0 \leq n, m \leq \ell - 1$.

Definition 5.2.1. *Suppose M is a $U_q(\mathfrak{sl}(2))$-module. A* Weyl filtration *for M is a sequence of submodules*

$$\{0\} = J_0 \subsetneq \cdots \subsetneq J_n = M \tag{5.2.1}$$

such that each J_k is a maximal submodule of J_{k+1} and each quotient J_{k+1}/J_k is a Weyl module.

Definition 5.2.2. *A $U_q(\mathfrak{sl}(2))$-module M is called* tilting *if both M and M^* have Weyl filtrations.*

This definition by itself is not very illuminating, but again the point is that tilting modules are the direct summands of tensor products of Weyl modules. Let $\mathbf{tilt}_\ell$ be the full subcategory of $\mathcal{C}(\mathfrak{sl}(2), \ell)$ whose objects are the tilting modules modules for $U_z^{res}(\mathfrak{sl}(2))$.

Proposition 5.2.3. $\mathbf{tilt}_\ell$ *is closed under direct sums, tensor products, duals, and taking direct summands.*

Proof. It is easy to see that $\mathbf{tilt}_\ell$ is closed under direct sums, duals, and taking direct summands. It is much harder to show that the tensor product of tilting modules is tilting, and the proof can be found in [2]. □

We can therefore restrict our attention to the indecomposable tilting modules. The indecomposable tilting modules for $U_z^{res}(\mathfrak{sl}(2))$ are indexed by integers $n \geq 0$ (corresponding to their maximal weights), and the tilting modules $T_z(n)$ for $0 \leq n < 2\ell - 2$ can be described explicitly as follows ([30]).

$T_z(n)$ has basis $\{t_0, \ldots, t_n\} \bigcup \{t'_0, \ldots, t'_r\}$, where $r = 2\ell - 2 - n$, and has the following action:

$$Kt_i = z^{n-2i} t_i \tag{5.2.2}$$

$$X^+ t_i = [n - i + 1]_z t_{i-1} \tag{5.2.3}$$

$$(X^+)^{(\ell)} t_i = ((n-i)_1) + 1) t_{i-\ell} \tag{5.2.4}$$

$$X^- t_i = [i + 1]_z t_{i+1} \tag{5.2.5}$$

$$(X^-)^{(\ell)} t_i = (i_1 + 1) t_{i+\ell} \tag{5.2.6}$$

$$Kt'_i = z^{r-2i} t'_i \tag{5.2.7}$$

$$X^+ t'_i = [r - i + 1]_z t'_{i-1} + \binom{n+i-\ell}{i}_z t_{n+i-\ell} \qquad \text{if } 0 < i \leq r \tag{5.2.8}$$

$$X^+ t'_0 = [n - \ell + 1]_z t_{n-\ell} \tag{5.2.9}$$

$$X^- t'_i = [i + 1]_z t'_{i+1} \qquad \text{if } 0 \leq i < r \tag{5.2.10}$$

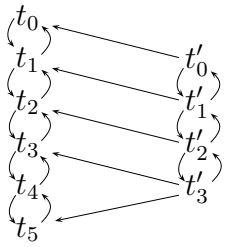
$$X^- t'_r = \binom{\ell - 1}{n - \ell + 1}_z t_\ell \tag{5.2.11}$$

$$(X^\pm)^{(\ell)} t'_i = 0 \tag{5.2.12}$$

The essential aspect of these equations can be captured diagrammatically. For example, when $\ell = 5, n = 5$, $T_z(5)$ is depicted in Figure 5.1.

It is easy to see from the figure that the $T_z(n)$ are indecomposable, and that $\{t_0, \ldots, t_n\}$ span a submodule isomorphic to $W_z^{res}(n)$. The quotient is spanned by

Figure 5.1 – The upwards pointing arrows indicate the action of X^+ and the downwards pointing arrows indicate that of X^-.



$\{t'_0, \ldots, t'_r\}$ and is isomorphic to $W_z^{res}(r)$. It is therefore clear that $T_z(n)$ has a Weyl filtration. Note that if $0 \leq n \leq \ell - 1$, $T_z(n) = W_z^{res}(n) = W_z^{res}(n)$.

Given this definition, we can compute the quantum dimension of $T_z(n)$:

$$\dim_q(T_z(n)) = \begin{cases} [n+1]_z & \text{if } 0 \leq n \leq \ell - 1 \\ [n+1]_z + [2\ell - n - 1]_z = 0 & \text{if } \ell \leq n < 2\ell - 2 \end{cases} \tag{5.2.13}$$

so we have that $\dim_q(T_z(n)) = 0$ for $n < \ell - 1$. In fact, [2] shows that

Proposition 5.2.4. $\dim_q(T_z(n)) \neq 0$ *if and only if* $n < \ell - 1$

which allows us to easily compute $\dim_q(T_z(n))$ for all n.

A useful corollary of the above proposition is the following. It gives a general form for the decomposition of any two tilting modules.

Corollary 5.2.5. *For any tilting modules T_1, T_2, there is a tilting module Z such that*

$$T_1 \otimes T_2 \simeq \left(\bigoplus_{k=0}^{\ell-2} W_z^{res}(k)^{\otimes m_k} \right) \oplus Z \tag{5.2.14}$$

where $m_k \in \mathbb{Z}$, and $\dim_q(Z) = 0$

Proof.

$$T_1 \otimes T_2 \simeq \bigoplus_{k=0}^{\infty} T_z(k)^{\otimes n_k} = \bigoplus_{k=0}^{\ell-2} W_z^{res}(k)^{\otimes n_k} \oplus \bigoplus_{k=\ell-1}^{\infty} T_z(k)^{\otimes n_k} \tag{5.2.15}$$

Take $Z = \bigoplus_{k=\ell-1}^{\infty} T_z(k)^{\otimes n_k}$. □

We can now give a decomposition of $W_z^{res}(n) \otimes W_z^{res}(m)$ into indecomposable modules for $0 \leq n, m \leq \ell - 1$. This tensor product will not decompose as a direct sum of irreducible modules in general as with the irreducible representations of $\mathfrak{sl}(2)$. However, the crucial point is that it *does* decompose as a direct sum of irreducible modules and tilting modules T with $\dim_q(T) = 0$. This means if we can "quotient out" by the tilting modules with quantum dimension zero, then any tensor product will decompose as a direct sum of irreducible modules as with representations of $\mathfrak{sl}(2)$.

Proposition 5.2.6. *Suppose* $0 \leq m, n \leq \ell - 1$. *Then*

$$W_z^{res}(n) \otimes W_z^{res}(m) \simeq \bigoplus_{\substack{i=|n-m| \\ i+n+m \text{ even}}}^{n+m} W_z^{res}(i) \tag{5.2.16}$$

if $n + m \leq \ell - 2$, *and*

$$W_z^{res}(n) \otimes W_z^{res}(m) \simeq \bigoplus_{\substack{i=|n-m| \\ i+n+m \text{ even}}}^{2\ell-4-n-m} W_z^{res}(i) \oplus \bigoplus_{\substack{i=\ell-1 \\ i+n+m \text{ even}}}^{n+m} T_z(i) \tag{5.2.17}$$

for $\ell - 1 \leq n + m < 2\ell - 2$

5.3 Construction of the MTC

We will now quotient the category $\mathbf{tilt}_\ell$ by those tilting modules with quantum dimension zero to obtain an MTC. With this aim, we make the following definitions:

Definition 5.3.1. *A morphism $f : V \to W$ is* negligible *if $\mathrm{tr}_q(fg) = \mathrm{tr}_q(gf) = 0$ for any $g : W \to V$*

Definition 5.3.2. *A module T is* negligible *if all its endomorphisms are negligible*

The following proposition characterizing negligible tilting modules follows from Proposition 5.2.3 and Corollary 5.2.5.

Proposition 5.3.3. *A tilting module T is negligible if and only if it has quantum dimension zero.*

Define the category $\mathcal{C}^{\mathrm{int}}$ be the category with objects tilting modules and morphisms

$$\mathrm{Hom}(V, W) = \mathrm{Hom}_{\mathbf{tilt}_\ell}(V, W)/\text{negligible morphisms} \tag{5.3.1}$$

Proposition 5.2.6 gives us that $\mathbf{tilt}_\ell$ is semisimple, with simple objects

$$\{W_z^{res}(0), \ldots, W_z^{res}(\ell - 2)\} \tag{5.3.2}$$

The $\{W_z^{res}(0), \ldots, W_z^{res}(\ell - 2)\}$ are all nonisomorphic because they all have different quantum dimensions.

The fusion rules in $\mathcal{C}^{\mathrm{int}}$ are given by

$$W_z^{res}(m) \otimes W_z^{res}(n) \simeq \sum_i N_{mn}^i W_z^{res}(i) \tag{5.3.3}$$

where

$$N_{mn}^{i} = \begin{cases} 1 & \text{if } |m-n| \leq i \leq m+n, i \leq 2k-(m+n), i+m+n \in 2\mathbf{Z} \\ 0 & \text{else} \end{cases} \tag{5.3.4}$$

$\mathcal{C}^{\text{int}}$ is also a ribbon category, since $\mathbf{tilt}_{\ell}$ is.

To summarize,

Proposition 5.3.4. *1. $\mathcal{C}^{int}$ is a ribbon category*

2. Any object T in $\mathcal{C}^{int}$ is isomorphic to a direct sum of Weyl modules.

3. $\mathcal{C}^{int}$ is a semisimple abelian category.

4. $\dim_{\mathcal{C}^{int}} T > 0$ *for every* $T \not\cong 0$

All that remains to show that it is a modular tensor category is to check that the S-matrix (defined in Equation 3.6.2) is invertible. A proof of this can be found in [21].

Chapter 6
From MTC to TQC

In this chapter, we explain further the relationship between TQC and modular tensor categories arising from quantum groups. We will focus mainly on the category **Fib** of Fibonacci anyons, which is the simplest anyon model that is universal for quantum computing.

We will discuss in some detail how to simulate the quantum circuit model in **Fib**. We will then discuss the universality of this simulation and algorithms for doing topological quantum computing in practice.

6.1 The Fibonacci anyon

The category **Fib** of Fibonacci anyons is a modular tensor category which is a subcategory of $\mathcal{C}^{int}(\mathfrak{sl}(2), 5)$. $\mathcal{C}^{int}(\mathfrak{sl}(2), 5)$ has simple objects V_0, V_1, V_2, V_3, which are representations of $U_z^{res}(\mathfrak{sl}(2))$ for z a 5^{th} root of unity. The simple objects in **Fib** are V_0, V_2. We will refer to them as $\mathbf{1}$ and τ respectively, $\mathbf{1}$ being the tensor unit and trivial anyon type or vacuum. The fusion rules in **Fib** can be computed easily and are as follows:

- $\tau \odot \tau = I \oplus \tau$
- $\tau \odot I = \tau$
- $I \odot I = I$

Recall that the $\oplus$ here means that when τ, τ fuse, the result is a superposition of anyons of type 1 and τ. The reason these anyons are called Fibonacci anyons is that $\tau^{\odot n} \simeq F_{n-1}\mathbf{1} \oplus F_{n+2}\tau$, where F_n is the n^{th} Fibonacci number.

We will now explain a simple way to simulate quantum circuits using Fibonacci anyons. To simulate quantum circuits, we need

- Qubits
- Systems of multiple qubits
- A way to do measurement
- Unitary gates
- A universal gate set

We will assume that we have physical capabilities to create anyons in a given initial state, rearrange anyons, fuse anyons, and measure the type of a given anyon. It turns out that initializing anyons is nontrivial: in [23] König gives a method for initializing anyons assuming a more restricted set of capabilities.

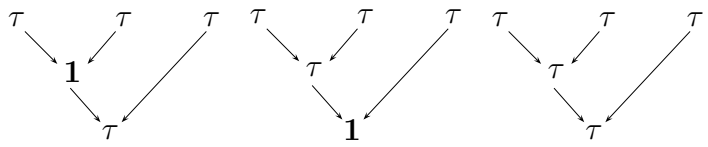
First we construct qubits. Since fusing two τ anyons has two possibilities:

$$\tau \odot \tau \simeq \mathbf{1} \oplus \tau \tag{6.1.1}$$

one obvious candidate for a qubit is a pair of anyons (τ, τ). However, the braid group B_2 is abelian, so it is only possible to implement diagonal gates by braiding these two anyons. What if we use three anyons? Consider a triplet (τ, τ, τ) of Fibonacci anyons. A simple computation shows that

$$(\tau \odot \tau) \odot \tau \simeq 2\tau \oplus 1 \tag{6.1.2}$$

This means that there are 3 fusion possibilities for 3 anyons with type τ:



Two of them have the final result τ. We use this fact to define our qubits to be triples of τ anyons with total charge τ. We saw in 6.1 that the first two qubits can fuse to be either τ or $\mathbf{1}$: denote these two possibilities by $((\tau, \tau)_{\mathbf{1}}, \tau)_\tau$ and $((\tau, \tau)_\tau, \tau)_\tau$.

There is also an equivalent formulation using quadruplets $((\tau, \tau), (\tau, \tau))_{\mathbf{1}}$ with total charge $\mathbf{1}$. We use the three-qubit formulation here, following [13].

In **Fib**, these are represented by elements of $\mathrm{Hom}(\tau, ((\tau \odot \tau) \odot \tau)) \simeq \mathrm{Hom}(\tau, 2\tau \oplus \mathbf{1}) \simeq \mathbb{C}^2$. Define

$$|0\rangle = ((\tau, \tau)_{\mathbf{1}}, \tau)_\tau \tag{6.1.3}$$

$$|1\rangle = ((\tau, \tau)_\tau, \tau)_\tau \tag{6.1.4}$$

$|0\rangle$ and $|1\rangle$ are elements of $\mathrm{Hom}(\tau, ((\tau \odot \tau) \odot \tau))$. We will call $\mathrm{span}\{|0\rangle, |1\rangle\}$ the *computational space*. There is also a *noncomputational space* spanned by $|\mathrm{NC}\rangle = ((\tau, \tau)_\tau, \tau)_{\mathbf{1}}$. One of the principal issues with this simulation is that of "leakage": some

multi-qubit operations take us out of the computational space. Since the total charge of a system of anyons is always preserved, single-qubit operations do not suffer from leakage.

Performing measurements in the $\{|0\rangle, |1\rangle\}$ basis is straightforward: just fuse the first two anyons and measure the result, then fuse the remaining two and measure again.

We have explained how 1-qubit systems are simulated. Multi-qubit systems are similar: for n qubits, we take n sets of 3 anyons: $\tau^{\odot 3n}$. For $|\varphi\rangle, |\psi\rangle \in \mathrm{Hom}(\tau, (\tau \odot \tau) \odot \tau)$, their tensor product

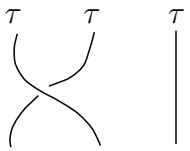
$$\begin{aligned} |\varphi\rangle \odot |\psi\rangle \in \mathrm{Hom}(\tau \odot \tau, (\tau)^{\odot 6}) &\simeq \mathrm{Hom}(\tau \oplus \mathbf{1}, 8\tau \oplus 5\mathbf{1}) \\ &\simeq \mathbb{C}^5 \oplus \mathbb{C}^8. \end{aligned}$$

The vectors $\{|i\rangle \odot |j\rangle : 0 \leq i, j \leq 1\}$ therefore span a 4-dimensional subspace of $\mathrm{Hom}(\tau \odot \tau, (\tau)^{\odot 6}) \simeq \mathbb{C}^5 \oplus \mathbb{C}^8$. We again refer to this 4-dimensional subspace as the *computational space* V.

We now turn to the problem of defining gates. **Fib** is braided, so for any n and object V in **Fib**, B_n acts on $\mathrm{Hom}(V, \tau^{\odot n})$ by composition:

$$f \mapsto \sigma \circ f \tag{6.1.5}$$

This gives a representation of the braid group on the hom sets $\mathrm{Hom}(\mathbf{1}, \tau^{\odot n})$. In fact it turns out that this representation is unitary. Braids therefore act unitarily on our qubits, and we will use them as our quantum gates. How do these braids act? The generator σ_1 of B_3,



acts on $\mathrm{Hom}(\tau, ((\tau \odot \tau) \odot \tau))$ via the unitary matrix

$$\begin{pmatrix} e^{\frac{-4\pi i}{5}} & 0 \\ 0 & e^{\frac{-2\pi i}{5}} \end{pmatrix} \tag{6.1.6}$$

with respect to the basis $\{|0\rangle, |1\rangle\}$. This can be computed either using the "universal R-matrix" in Section 4.5 or by solving for it using the fusion rules and the axioms for a braided monoidal category (see [29]).

$\mathrm{Hom}(\tau, \tau^{\odot 3})$ has another natural basis: $\{\ (\tau, (\tau, \tau)_{\mathbf{1}})_\tau,\ (\tau, (\tau, \tau)_\tau)_\tau\ \}$. It can be obtained from the basis $\{|0\rangle, |1\rangle\}$ by composing with the associativity isomorphism $\alpha_{\tau,\tau,\tau}$. The change of basis matrix is called the *F-matrix*. It is

$$\begin{pmatrix} \phi^{-1} & \sqrt{(}\phi^{-1}) \\ \sqrt{(}\phi^{-1}) & -\phi^{-1} \end{pmatrix} \tag{6.1.7}$$

where ϕ is the golden ratio. The F-matrix is also unitary.

The R and F-matrices allow us to compute the 2×2 matrix corresponding to each element of B_3 in this representation: the other generator σ_2 of B_3 acts as $F^{-1}RF$. Thus the R and F matrices are enough to compute the matrix associated to any element of the B_n acting on $\mathrm{Hom}(\mathbf{1}, \tau^{\odot n})$ or $\mathrm{Hom}(\tau, \tau^{\odot n})$.

6.2 Universality and implementations

We have explained a framework for simulating the circuit model using Fibonacci anyons. It turns out that this is universal. This means that there need to be braids which both preserve the computational space (so as to not end up with meaningless output), and perform arbitrary unitaries on the computational space.

On single qubits $((\tau,\tau),\tau)$, every braid preserves the computational space. However, on pairs of qubits $(((\tau,\tau),\tau),((\tau,\tau),\tau))$, this is not the case. Freedman et al. prove in [9] that the image of B_6 in its representation on $\mathrm{Hom}(\tau\oplus\tau,\tau^{\odot 6}) \simeq \mathbb{C}^5\oplus\mathbb{C}^8$ is dense in $SU(5)\oplus SU(8)$. It follows that any 2-qubit unitary gate can be approximated by some braid in B_6, with as little leakage into the noncomputational space as required.

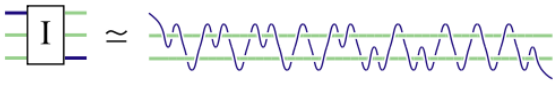
This theorem does not however give an efficient means of finding a braid whose image approximately realizes a given unitary gate. In this section we review how this problem has been approached.

The most naive solution to the problem of "topological quantum compiling" is brute force search: try braids until one is found where the image is close enough to the gate required. Since it is enough to be able to construct arbitrary 2-qubit gates, we at most have to search through the braids in B_6. This is quite a formidable task, as $SU(5)\oplus SU(8)$ has 87 free parameters.

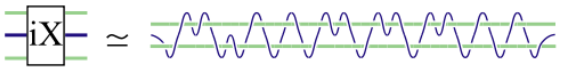
In [13], Hormozi et al. reduce the problem of implementing a universal gate set to that of implementing arbitrary single-qubit gates. This is done by giving an explicit method for constructing an approximation to a CNOT gate. They further show how to construct a CNOT gate while only moving one quasiparticle, which has obvious

practical significance: it is likely to be easier in practice to only have to move one quasiparticle.

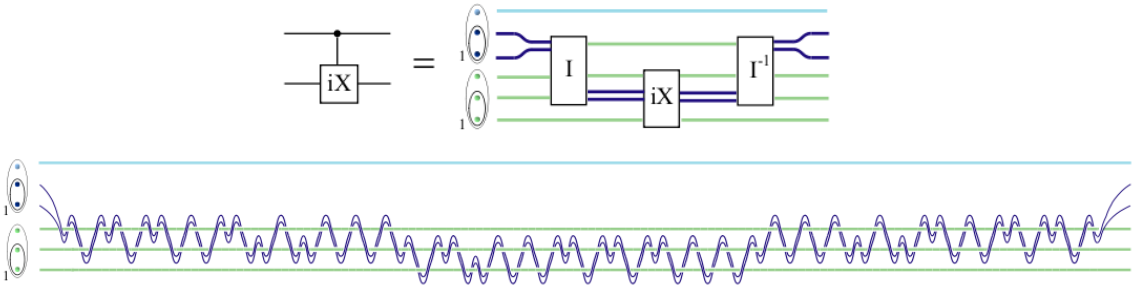
The first construction of the CNOT gate works as follows. First, find a braid which approximates the identity, but where the first and third quasiparticles swap places. The example given is (figures taken from [13])



and a braid approximating X:



Then combine these as follows to obtain an approximation to the CNOT gate:



When the mobile pair of qubits has total charge τ, the "identity" braid has (approximately) no effect on the system and so the approximate X gate is applied to the second qubit.

When the mobile pair of qubits has total charge $\mathbf{1}$, the "identity" braid obviously has an effect on the system. Since braiding the tensor unit has no effect, the overall effect on the system is none at all. So this braid approximately implements a CNOT

gate! In fact, replacing the X gate with any other gate gives us arbitrary controlled gates.

However, the algorithm for constructing single-qubit gates relies on a combination of brute force search and the Solovay-Kitaev algorithm. [5],[4], and [25] give two alternative methods for approximating single qubit gates using Fibonacci anyons. Both of these methods involve the icosahedral group in some way.

Burrello et al. ([5], [4]) use brute-force search to associate a braid to each icosahedral group element which most closely approximates it among all braids of length $\leq N$. Call this set $I(N)$.

This set $I(N)$ is then used to find a product of elements of $I(N)$ which is close to the target gate T. This involves another brute force search over the elements $\{g_1 g_2 \cdots g_n : g_i \in I(N)\}$ for some n.

The approach in [25] is related: no algorithm is given for approximating particular unitary gates, but rather a method for approximating increasingly dense meshes in $SU(2)$. The approach here is to use a brute force search to closely approximate two generators for the icosahedral group, and then use these two generators to generate a slightly deformed polytope.

In [1], Ainsworth and Slingerland study the general problem of leakage in topological quantum computing. In particular, 2 questions are answered, using only facts about representations of B_n:

1. What is the optimal number of anyons to use to model a qubit?

2. To what extent can leakage be avoided?

To address the first question, it is shown that if we use $n > 4$ anyons to model a qubit, then either:

– the representation of B_n is abelian

– there is leakage into the noncomputational space in single qubit operations

The mathematical problem that this reduces to is finding the maximum n for which there is a nonabelian d-dimensional representation of B_n. A (nontrivial) theorem shows that the answer is always $d+2$. Therefore in general for modelling qudits, the same holds if we use $n > d + 2$ anyons.

As for the second question, it is proven that if there is a system of 2 qubits where every 2-qubit gate does not cause leakage, then the anyons are Ising anyons, and therefore not universal.

They further show that there are no nonabelian anyons where all the gates on 2 qutrits or 1 qubit + 1 qutrit are leakage-free.

However, if each anyon carries a representation of a quantum group, then their tensor product does as well and thus all gates are leakage-free. However, it is conjectured that the braid group representations that occur in this way have finite image.

Rowell et al. conjecture in [31] that for any unitary modular tensor category $\mathcal{C}$, every representation of B_n on the hom sets has finite image if and only if $\dim_q(X)^2$ is an integer for every simple object X in $\mathcal{C}$. A verification of this conjecture is given for all unitary modular tensor categories with ≤ 4 simple objects.

Chapter 7
Conclusions and future work

We have given an account of the theory of modular tensor categories arising from quantum groups as they relate to topological quantum computing. We conclude with some discussion about possible future work.

This investigation started because we were interested in using facts about specific representations of B_n that arise in the modular tensor categories that we have discussed to better compile quantum gates into braids.

One interesting question that is so far unanswered is that of whether there are entangling leakage-free 2-qubit gates in universal TQC models. The work in [1] shows us that it is impossible for all gates to be leakage-free, but the possibility of there being some nontrivial group of such leakage-free is not excluded.

All of the strategies for finding single-qubit gates discussed in the previous section involve a significant amount of brute-force search. It would be interesting to see if this can be avoided or improved by using facts about braid group representations: [4] and [5] refer to results on random matrix theory to support conjectures about the proposed algorithms, but do not use any facts about braid group representations as [1] does.

Bibliography

[1] R. Ainsworth and J. K. Slingerland. Topological qubit design and leakage. *New Journal of Physics*, 13(6), June 2011.

[2] Henning Haahr Andersen. Tensor products of quantized tilting modules. *Communications in Mathematical Physics*, 149:149–159, 1992.

[3] Rodney Baxter. *Exactly solved models in statistical mechanics*. Academic Press, 1982.

[4] M. Burrello, G. Mussardo, and X. Wan. Topological quantum gate construction by iterative pseudogroup hashing. *New Journal of Physics*, 13(2), February 2011.

[5] Michele Burrello, Haitan Xu, Giuseppe Mussardo, and Xin Wan. Topological quantum hashing with the icosahedral group. *Phys. Rev. Lett.*, 104(16):160502, Apr 2010.

[6] Michele Burrello, Haitan Xu, Giuseppe Mussardo, and Xin Wan. Topological quantum hashing with the icosahedral group. *Phys. Rev. Lett.*, 104(16), Apr 2010.

[7] Vladimir Drinfeld. Quantum groups. In *Proceedings of the International Congress of Mathematicians, Berkeley (1986)*. American Mathematical Society, 1987.

[8] L. D. Faddeev, E. K. Skylanin, and L. A. Takhtajan. Quantum inverse scattering method. *Theor. Math. Phys.*, 1979.

[9] Michael Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, January 2000.

[10] Michael Freedman, Michael J. Larsen, and Zhenghan Wang. The Two-Eigenvalue Problem and Density of Jones Representation of Braid Groups. *Communications in Mathematical Physics*, 228(1):177–199, June 2002.

[11] Henning Haahr Andersen and Jan Paradowski. Fusion categories arising from semisimple lie algebras. *Communications in Mathematical Physics*, 169:563–588, 1995.

[12] Brian C. Hall. *Lie groups, Lie algebras, and representations: an elementary introduction.* Springer, 2003.

[13] L. Hormozi, G. Zikos, N. Bonesteel, and S. Simon. Topological quantum compiling. *Physical Review B*, 75(16):20, April 2007.

[14] James E. Humphreys. *Introduction to Lie Algebras and Representation Theory.* Springer, 1973.

[15] Jens Carsten Jantzen. *Lectures on quantum groups.* American Mathematical Society, 1995.

[16] Michio Jimbo. A q-difference analogue of $U(g)$ and the Yang-Baxter equation. *Letters in Mathematical Physics*, 10(1):63–69, 1985.

[17] Vaughan F. R. Jones. Index for subfactors. *Inventiones Mathematicae*, 72(1):1–25, February 1983.

[18] Vaughan F. R. Jones. A polynomial invariant for knots via von Neumann algebras. *Bulletin of the American Mathematical Society*, 12(1):103–112, January 1985.

[19] Christian Kassel. *Quantum Groups.* Springer, 1994.

[20] Christian Kassel and Vladimir Turaev. *Braid Groups.* Springer, 2008.

[21] Alexander Kirillov and Bojko Bakalov. *Lectures on Tensor Categories and Modular Functors.* American Mathematical Society, 2001.

[22] A. Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2 – 30, 2003.

[23] Robert König. Composite anyon coding and the initialization of a topological quantum computer. *Phys. Rev. A*, 81(5):052309, May 2010.

[24] G Moore and N Seiberg. Lectures on RCFT. In *'Superstrings' 89: Proceedings of the Trieste Spring School*, page 129, Sep 1989.

[25] R. Mosseri. A geometrical approach to SU(2) navigation with Fibonacci anyons. *Journal of Physics A Mathematical General*, 41(17), May 2008.

[26] Michael Mueger. From Subfactors to Categories and Topology II. The quantum double of tensor categories and subfactors. *J. Pure Appl. Alg.*, 180:159–219, November 2001.

[27] Michael Mueger. On the structure of braided crossed G-categories. In *Homotopy Quantum Field Theory*, pages 221–223. European Mathematical Society, 2010.

[28] Chetan Nayak, Steven H. Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80(3):1083–1159, Sep 2008.

[29] Prakash Panagaden and Eric Paquette. A categorical presentation of quantum computation with anyons. In Bob Coecke, editor, *New Structures for Physics*. Springer, 2011.

[30] Andrew Pressley and Vyjayanthi Chari. *A Guide to Quantum Groups*. Cambridge University Press, 1973.

[31] Eric Rowell, Richard Stong, and Zhenghan Wang. On classification of modular tensor categories. *Communications in Mathematical Physics*, 292:343–389, 2009.

[32] S. D. Stirling and Y.-S. Wu. Braided Categorical Quantum Mechanics I. *ArXiv e-prints*, September 2009.

[33] Ross Street. *Quantum Groups: A Path to Current Algebra*. Cambridge University Press, 2007.

[34] P. Narayana Swamy. Deformed heisenberg algebra: origin of q-calculus. *Physica A: Statistical Mechanics and its Applications*, 328(1-2):145 – 153, 2003.

[35] Haitan Xu and Xin Wan. Constructing functional braids for low-leakage topological quantum computing. *Phys. Rev. A*, 78(4):042325, Oct 2008.

[36] C. N. Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett.*, 19(23):1312–1315, Dec 1967.