Revista Colombiana de Matemáticas
Volumen 50(2016)2, páginas 207-272

Local unitary representations of the braid group and their applications to quantum computing

Colleen Delaney[1,✉], Eric C. Rowell[2], Zhenghan Wang[1,3]

[1]University of California Santa Barbara, Santa Barbara, CA, U.S.A.

[2]Texas A&M University, College Station, TX, U.S.A.

[3]Microsoft Station Q, Santa Barbara, CA, U.S.A.

Abstract. We provide an elementary introduction to topological quantum computation based on the Jones representation of the braid group. We first cover the Burau representation and Alexander polynomial. Then we discuss the Jones representation and Jones polynomial and their application to anyonic quantum computation. Finally we outline the approximation of the Jones polynomial by a quantum computer and explicit localizations of braid group representations.

Key words and phrases. topological quantum computation, braid group representations, localizations, quantum algebra.

2010 Mathematics Subject Classification. 81P86, 20F36.

1. Introduction

Topological quantum computation is based on the storage and manipulation of information in the representation spaces of the braid group, which consist of quantum states of certain topological phases of matter [23]. The most important unitary braid group representations for topological quantum computation are the Jones representations [11], which are described by Temperley-Lieb-Jones theories. Temperley-Lieb Jones (TLJ) theories are the most ubiquitous

examples of unitary modular categories. The Jones-Wenzl projectors, or idempotents, in TLJ theories can be used to model anyons, quasiparticle excitations of a topological phase, like those believed to exist in fractional quantum Hall liquids. Hence the proper mathematical language to discuss topological quantum computation is unitary modular category (UMC) theory and the associated topological quantum field theory (TQFT). Both UMC and TQFT are highly technical subjects. However, the representations of the braid group from UMCs or TQFTs are a more accessible point of entry to the subject. These notes provide an elementary introduction to some representations of the braid group coming from UMCs and TQFTs, and their application to topological quantum computation. We will use the *braid group* $\mathcal{B}_\infty$ to mean the direct limit of all n-strand braid groups $\mathcal{B}_n$ for all $n \geq 1$, where a representation of the braid group $\mathcal{B}_\infty$ is a compatible *sequence of representations* of $\mathcal{B}_n$.

Our focus is on the representations of the braid group discovered by Jones in the study of von Neumann algebras [11]. Jones representations are *unitary*, which is important for our application to quantum computing. These representations also have a hidden *locality* and generically dense images. Unitarity, locality, and density are important ingredients for the two main theorems that we will present:

Theorem 1.1. *The Jones representation of the braid group at $q = e^{\pm 2\pi i/r}$ can be used to construct a universal quantum computer for values of r not equal to $1, 2, 3, 4$, or 6.*

Theorem 1.2. *The Jones polynomial of oriented links at $q = e^{\pm 2\pi i/r}$ can be approximated by a quantum computer efficiently for any integer $r \geq 1$.*

While unitarity and density are easy to understand mathematically, locality is not formally defined in our notes as there are several interpretations, one of which is discussed in Section 6. Essentially, a local representation of the braid group is one coming from a local TQFT, whose locality is encoded in the gluing formula. A first approximation of locality would mean a sequence of representations of $\mathcal{B}_n$ with a compatible Bratteli diagram of branching rules.

We motivate our study of the Jones representation and its quantum applications with the Burau representation, which belongs to the classical world. The Burau representation leads to the link invariant called the Alexander polynomial, which can be computed in polynomial time on a classical computer. On the other hand, the link invariant corresponding to the Jones representation, the Jones polynomial, is $\#P$-hard to compute on a classical computer, but can be approximated by a quantum computer in polynomial time. This approximation of quantum invariants by a quantum computer is realized by the amplitudes of the physical processes of anyons, whose worldlines include braids.

The contents of these notes are as follows. In section 2, we cover the Burau representation and Alexander polynomial. In section 3, we discuss the Jones

representation and Jones polynomial. Section 4 discusses anyons and anyonic quantum computation. In section 5, we explain the approximation of the Jones polynomial by a quantum computer. Section 6 is on an explicit localization of braid group representations. While full details are not included, our presentation is more or less self-contained with the exception of Thm. 4.21, which is important for addressing the issue of *leakage*. An elementary inductive argument for Thm. 4.21 is possible and we will leave it to interested readers.

2. The Burau Representation and Alexander Polynomial

2.1. The braid group

The *n-strand braid group* $\mathcal{B}_n$ is given by the presentation

$$\mathcal{B}_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{r} \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for } i = 1, 2, \ldots, n-1 \end{array} \right\rangle.$$

The first type of relation is known as far commutativity and the second is the braid relation. Using the braid relation, one can check that all of the generators of the n-strand braid group lie in the same conjugacy class. Therefore, each n-strand braid group $\mathcal{B}_n$ is generated by a single conjugacy class when $n \geq 3$.

The names of the relations are inspired by the geometric presentation of the braid group, in which we picture braids on n "strands", and the braid generators σ_i correspond to crossing the ith strand over the $i+1$ strand. Multiplication bb' of two braid diagrams b and b' is performed by stacking b' on top of b and interpreting the result as a new braid diagram.

For example, $\mathcal{B}_3 = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$, where σ_1 braids the first two strands and σ_2 the latter two.

$\sigma_1 =$  $\qquad \sigma_2 =$ 

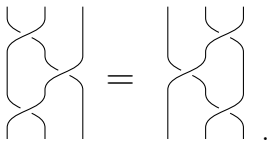
In these notes, we use the "right-handed convention" when drawing braid diagrams of braid group generators, so that the overstrand goes from bottom left to top right. As a result,

$\sigma_1^{-1} =$ 

Swapping the definitions of σ_1 and σ_1^{-1} would give the "left-handed convention".

In the picture presentation, far commutativity expresses the fact that when nonoverlapping sets of strands are braided, the result is independent of the

order in which the strands were braided. The braid relation is given by



The braid relation is called the Yang-Baxter equation by some authors, but we will reserve use of this phrase because, as will be explained shortly, there is a subtle difference between the two.

Another useful perspective is to identify $\mathcal{B}_n$ with the motion group (fundamental group of the configuration space) of n points in the disk D^2. Then the braid relation can be interpreted as saying that given three distinct points on a line in the disk, if one exchanges the first and third points while keeping the middle one stationary, then the braid trajectories are the same whether the exchange is performed in a clockwise or counterclockwise manner.

The *braid group*, denoted by $\mathcal{B}_\infty$, is formed by taking the direct limit of the n-strand braid groups with respect to the inclusion maps $\mathcal{B}_n \hookrightarrow \mathcal{B}_{n+1}$ sending $\sigma_i \mapsto \sigma_i$. That is, we identify a braid word in $\mathcal{B}_n$ with the same braid word in $\mathcal{B}_{n+1}$. In pictures, this inclusion map $\mathcal{B}_n \to \mathcal{B}_{n+1}$ adds a single strand after the braid σ.

2.2. Representations of the Braid Group

For applications of braid group representations to quantum computing, the braid group representations should be *unitary* and *local*. Moreover, for reasons that are not *a priori* clear, since the images of the braid generators σ_i will eventually be interpreted as *quantum gates* manipulating *quantum bits*, they should be of finite order and have algebraic matrix entries.

Recall that a matrix U is unitary if $U^\dagger U = UU^\dagger = I$. We denote by $\mathrm{U}(r)$ the group of $r \times r$ unitary matrices. A precise definition of locality requires interpreting the images of elements of the braid group as quantum gates, and is relegated to section 4 where quantum computation is discussed.

One important way to obtain representations of the braid group is to find solutions to the *Yang-Baxter equation*.

2.2.1. The Yang-Baxter Equation and R-matrix

Let V be a finite dimensional complex vector space with a specified basis, and let $R : V \otimes V \to V \otimes V$ be an invertible solution to the *Yang-Baxter equation* (YBE):

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

where I is the identity transformation of V. We call such a solution to the YBE an *R-matrix* (as opposed to R-operator, since we have a basis with which to work).

Any R-matrix gives rise to a (local) representation of the braid group via the identification

$\sigma_i \mapsto$ 

For example, in the 3-strand braid group, we can take

$\sigma_1 \mapsto$ 

$= R \otimes id_V$

where $R \otimes id_V$ is a map from $V \otimes V \otimes V$ to itself.

In general one considers a Yang-Baxter operator as having parameters that indicate what pair of factors in $V^{\otimes n}$ it acts on: $R_{i,i+1} = I_{i-1} \otimes R_{i,i+1} \otimes I_{n-i-1}$. Then the Yang-Baxter equation is given by

Then the braid relation and Yang-Baxter equation differ by the choice of indexing. In the former we keep track of the position of each strand, while in the latter the labeling of the strands is fixed. For example, if we label the stand as $1, 2, 3$, the braid relation becomes

$$\sigma_{12}\sigma_{13}\sigma_{23} = \sigma_{23}\sigma_{13}\sigma_{12}.$$

2.2.2. Locality and unitarity

The following R-matrix is a 4×4 solution to the Yang-Baxter equation for $V = \mathbb{C}^2$ with the standard basis and $a \in \mathbb{C}$, and as such is local.

$$R = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & \bar{a} & 0 \\ 0 & \bar{a} & a - \bar{a}^3 & 0 \\ 0 & 0 & 0 & a \end{pmatrix}$$

If R is to be unitary, its columns must be orthonormal. In particular, $\bar{a} = a^{-1}$ and

$$\langle (0, 0, \bar{a}, 0)^T, (0, \bar{a}, a - \bar{a}^3, 0) \rangle = a(a - \bar{a}^3) = 0.$$

This implies that $a^4 = 1$, whence the only possibilities for a are ± 1 or $\pm i$. One can check that each of these choices results in R being a unitary matrix.

While representations of the braid group arising from R-matrices are always local, unlike the example above they rarely unitary. There is a natural tension between these two properties that make finding such a representation difficult.

Conjeture 2.1. Any unitary R-matrix which has finite order and algebraic entries leads to a representation of the braid group with finite image.

It is in general difficult to find nontrivial solutions to the Yang-Baxter equation. Historically, the theory of quantum groups was developed to address this problem, but solutions that arise from the theory of quantum groups are rarely unitary. The state of the art is that for $\dim V = 1$ and $\dim V = 2$, all unitary solutions are known. While a classification for larger dimensions is yet unknown, there do exist nice examples of 4×4 and 9×9 unitary solutions [23].

These considerations make representations coming from solutions to the Yang-Baxter equations unlikely candidates for applications to quantum computation. Next we consider the Burau representation.

2.3. The Burau representation of the braid group

There are two versions of the Burau representation: the unreduced representation, which denoted by $\tilde{\rho}$, and the reduced representation, for which we reserve the notation ρ.

2.3.1. The unreduced Burau representation

There is a nice probabilistic interpretation of the unreduced Burau representation that is due to Jones, which we will use as an introduction to the subject [12]. We start by defining the representation for *positive braids*, braids for which all crossings are right-handed. More precisely, σ is positive if it can be written $\sigma = \sigma_{i_k}^{s_k} \cdots \sigma_{i_1}^{s_i}$ where $s_i > 0$ for each i.

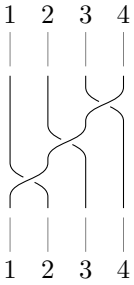
Imagine the braid diagram of a braid σ as a braided bowling alley with n lanes, where lanes cross over and under one another and at every overcrossing there is a trap door that will open with probability $1 - t$ when a ball rolls over it. Of course, due to gravity there is zero probability of a ball on a lower lane jumping up onto a lane crossing over it. Then starting from the bottom of the braid and bowling down lane i, it ends up in lane j with some probability, which we can identify as the ijth entry of a matrix.

Then for positive braids the unreduced Burau representation $\tilde{\rho} : \mathcal{B}_n \to GL_n(\mathbb{Z}[t, t^{-1}])$ can be defined by assigning each $\sigma \in \mathcal{B}_n$ to the matrix $\tilde{\rho}(\sigma)$ given by

$$\tilde{\rho}(\sigma)_{ij} = \sum_{\text{paths p from i to j}} w(p),$$

where $w(p)$ is the probability corresponding to the path p, which is always of the form $t^k(1-t)^l$ for some nonnegative integers k and l.

For a concrete example, take the following braid, call it σ, in $\mathcal{B}_4$.



Note that the labels mark the relative position of the strands, as opposed to the strands themselves. The matrix representing σ in $GL_4(\mathbb{Z}[t,t^{-1}])$ is then given by

$$\tilde{\rho}(\sigma) = \begin{pmatrix} 1-t & t(1-t) & t^2(1-t) & t^3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

While the probabilistic interpretation only makes sense for positive braids, the representation of inverses of braid generators is already determined, for once we define the representation of a generator, for example

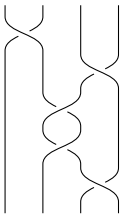
$\tilde{\rho}($ $) = \begin{pmatrix} 1-t & t & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

using that $\tilde{\rho}$ is a group homomorphism it follows that $\tilde{\rho}(\sigma_1)\tilde{\rho}(\sigma_1^{-1}) = I$. Therefore the representation of the σ_1^{-1} must be given by the inverse of $\tilde{\rho}(\sigma_1)$:

$\tilde{\rho}($ $) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \bar{t} & 1-\bar{t} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

where $\bar{t} = 1/t$. Thus left-handed crossings are assigned a factor of $\bar{t}$ for an overcrossing and $1-\bar{t}$ for an undercrossing. The remaining generators σ_i of $\mathcal{B}_n$ and their inverses can be represented by extending the construction in the natural way. Then the representation of an arbitrary braid $b = \sigma_{i_k}^{s_k} \cdots \sigma_{i_1}^{s_1}$ is given by multiplying the representations of the constituent σ_{i_j} in the braid word. This defines the unreduced Burau representation of the braid group.

As a fun example we introduce the following braid $b = \sigma_3^{-1}\sigma_2^2\sigma_3^{-1}\sigma_1^{-1}$, once drawn by Gauss (see e.g. [5, Figure 2]).



The unreduced Burau representation of the Gauss braid is given by

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ t\bar{t} + (1-t)^2\bar{t} & t(1-\bar{t}) + (1-t)^2(1-\bar{t}) & 0 & (1-t)t \\ 0 & 0 & \bar{t} & (1-\bar{t}) \\ \bar{t}^2(1-t) & \bar{t}(1-t)(1-\bar{t}) & (1-\bar{t})\bar{t} & (1-\bar{t})^2 + \bar{t}t \end{pmatrix},$$

which has been left unsimplified to make the individual contributions from paths more transparent.

The unreduced Burau representation of a braid $b \in \mathcal{B}_n$ has several properties worth mentioning.

(1) When $t = 1$, $\tilde{\rho}(b)$ is a permutation matrix. This allows one to interpret $\tilde{\rho}(b)$ as a deformation of a permutation matrix.

(2) The representation $\tilde{\rho}$ is reducible.

(3) There exists an invariant row vector (row eigenvector) of $\tilde{\rho}(b)$, independent of $b \in \mathcal{B}_n$.

The first property is clear from the construction of the unreduced Burau representation. The second and third properties are closely related, and we prove them below.

One of the nice aspects of the probabilistic interpretation of the Burau representation is that it is an immediate consequence of the definition that the entries in each row of a matrix $\tilde{\rho}(b)$ should sum to one, since probability must be conserved. Put another way,

$$\tilde{\rho}(\sigma)\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

That is, there is a one-dimensional subspace which is invariant under $\tilde{\rho}(\sigma)$, for any $\sigma \in \mathcal{B}_n$. Therefore the (unreduced) Burau representation is reducible, and

we can obtain another representation by restricting to the orthogonal subspace $\text{span}\{(1,1,\ldots,1)\}^{\perp}$. This is one way to define the *reduced* Burau representation.

Since the determinant of a matrix is equal to the determinant of its transpose, if $\det(I-\tilde{\rho}(b))=0$ for all $b\in\mathcal{B}_n$, then

$$\det((I-\tilde{\rho}(b))^T)=\det(I-\tilde{\rho}(b)^T)=0$$

for all $b\in\mathcal{B}_n$. Then since $\tilde{\rho}(b)$ has an eigenvector, $\tilde{\rho}(b)^T$ has an eigenvector v with eigenvalue 1, $\tilde{\rho}(b)^T v=v$ for some $v\neq 0$. Taking the transpose of this matrix equation, we find

$$v^T\tilde{\rho}(b)=v^T.$$

This shows that $\tilde{\rho}(b)$ has an invariant row vector v^T, proving the third property. In fact, this row vector takes the form

$$v^T=(1,t,t^2,\ldots,t^{n-1}).$$

Observing that

$$(1,\ldots,1,t^i,t^{i+1},1\ldots,1)\begin{pmatrix} I_{i-1} & 0 & 0\\ 0 & \begin{pmatrix}1-t & t\\ 1 & 0\end{pmatrix} & 0\\ 0 & 0 & I_{n-i-1}\end{pmatrix}$$

$$=(1,\ldots,1,t^i-t^{i+1}+t^{i+1},t^{i+1},1,\ldots,1),$$

it follows that v^T defines an invariant row vector for the representations of the braid group generators $\tilde{\rho}(\sigma_i)$, and hence for all $\tilde{\rho}(b)$, $b\in\mathcal{B}_n$.

These facts can be used to prove properties of the Alexander polynomial, for which we need a more concrete definition of the reduced Burau representation.

2.3.2. The reduced Burau representation

An alternative approach to defining the reduced Burau representation yields an explicit basis.

We find a basis for an invariant subspace of $\tilde{\rho}(\mathcal{B}_n)$ by looking for eigenvalues and eigenvectors of $\tilde{\rho}(\sigma_i)$. We have seen already that $(1,1,\ldots,1)^T$ is an eigenvector with eigenvalue 1. One can check that another eigenvector corresponding to eigenvalue $-t$ is given by $(0,\ldots,0,\underbrace{-t}_{i},\underbrace{1}_{i+1},0\ldots,0)^T$.

Proposition 2.1. *Let* $v_i=(0,\ldots,0,\underbrace{-t}_{i},\underbrace{1}_{i+1},0\ldots,0)^T$. *Then span*$\{v_1,\ldots,v_{n-1}\}$ *is an invariant subspace of* $\tilde{\rho}(b)$ *for all* $b\in\mathcal{B}_n$.

Proof. The image of each v_i under $\tilde{\rho}(b)$ can be written as a linear combination of the v_j.

$$\tilde{\rho}(\sigma_i)v_i = \begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ t^2 \\ -t \\ 0 \\ \vdots \\ 0 \end{pmatrix} = -tv_i$$

Similar calculations show

$$\tilde{\rho}(\sigma_i)v_{i-1} = v_{i-1}+v_t,\ \tilde{\rho}(\sigma_i)v_{i+1} = -tv_i+v_{i+1}, \text{and } \tilde{\rho}(\sigma_i)v_j = v_j \text{when } |j-i| \geq 2.$$

This verifies that the subspace spanned by the v_i is invariant, leading to the following definition. ☑

Definition 2.2. The reduced Burau representation $\rho : \mathcal{B}_n \to GL_{n-1}(\mathbb{Z}[t, t^{-1}])$ is given by $\rho(b) = \tilde{\rho}(b) \Big|_{\text{span}\{v_i\}}$.

2.3.3. Unitary Burau representations

Keeping in mind that we are looking for unitary representations of the braid group, it is natural to ask for which $t \in \mathbb{C}^*$ the reduced Burau representation $\rho : \mathcal{B}_n \to GL_{n-1}(\mathbb{Z}[t, t^{-1}])$ is unitary.

One can check that the matrix representation corresponding to a braid group generator fails to be unitary for any choice of t. For example, consider the braid  with corresponding (unreduced) Burau matrix representation $\begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix}$. Then either by direct computation or by noting that (since we can safely ignore an overall phase factor of -1 without affecting unitarity) for no choice of t does this matrix admit the familiar parametrization of elements of SU(2) as $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. By extending this observation to generators of $\mathcal{B}_n$, it follows that the unreduced Burau representation is never unitary.

However, the situation is not completely hopeless. We end with a theorem that tells us how to obtain a unitary representation from the reduced Burau representation.

Theorem 2.3. *Let $t = s^2$ where $s \in \mathbb{C}^*$, and define* $P_{n-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & s & & \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & s^{n-1} \end{pmatrix}$,

$J_{n-1} = \begin{pmatrix} s+s^{-1} & -1 & \cdots & 0 \\ -1 & s+s^{-1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ 0 & \cdots & -1 & s+s^{-1} \end{pmatrix}$, *and* $\rho_s(b) = P_{n-1}\rho(b)(P_{n-1})^{-1}$,

where ρ is the reduced Burau representation and $b \in \mathcal{B}_n$.

Then ρ_s is unitary with respect to the Hermitian matrix J_{n-1}. That is,

$$(\rho_s(b))^\dagger J_{n-1}\rho_s(b) = J_{n-1}$$

Moreover, for those $s \in \mathbb{C}^*$ for which $J_{n-1}(s)$ can be written as $J_{n-1}(s) = X^\dagger X$ for some matrix X, $X\rho_s(b)X^{-1}$ gives a unitary representation.

Exercise 2.4. Find all s such that $J_{n-1}(s)$ can be written $J_{n-1}(s) = X^\dagger X$.

There remain basic questions about the Burau representation to which the answers are not yet known.

Open problem 2.6. The Burau representation is faithful for $n = 1, 2, 3$, and is not faithful for $n \geq 5$ [2]. What about when $n = 4$?

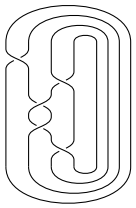
2.4. The Alexander polynomial

The reduced Burau representation of the braid group can be used to construct a link invariant called the *Alexander polynomial*. The existence of invariants which are both powerful and computable is essential to the classification of any mathematical object. Of course, Nature conspires so that these two characteristics are often hard to satisfy simultaneously. We will see that while the Alexander polynomial is computable in polynomial time, it is not quite sensitive enough to distinguish between certain types of knots.

2.4.1. From braids to links

There is a natural way to turn a braid into a link by identifying the top and bottom strands in an order-preserving manner. This operation is called a *braid closure*.

For example, one can check that the closure of the Gauss braid is the connect sum of two Hopf links.



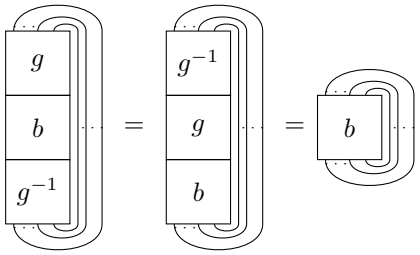
2.4.2. The Markov moves

We consider two other operations on braids, conjugation and stabilization, also known as the Markov moves of type I and type II, and show that performing either type of operation on a braid does not change the link that is obtained from the braid closure.

I. Let $b, g \in \mathcal{B}_n$. Then conjugation of the braid b by the braid g is given by the map $\mathcal{B}_n \to \mathcal{B}_n$

$$b \mapsto gbg^{-1}.$$

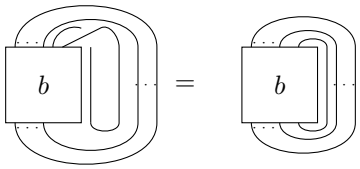
One can see that $\hat{b} = \widehat{gbg^{-1}}$ through the diagram below.



II. Let $b \in \mathcal{B}_n$, and let $\mathcal{B}_n$ be embedded in $\mathcal{B}_{n+1}$ in the standard way, by adding a rightmost strand. Then stabilization of the braid b is given by the map $\mathcal{B}_n \to \mathcal{B}_{n+1}$

$$b \mapsto b\sigma_n^{\pm 1}.$$

That is, we add a rightmost $n+1$st strand to b to identify it as a braid in $\mathcal{B}_{n+1}$, and then we braid its nth and $n+1$st strands with either an over- or under-crossing. Once again, the diagrammatic argument that $\hat{b} = \widehat{b\sigma_n}$ is clear.



This move introduces a twist in the braid closure, and hence can be undone by a Reidemeister move of type 1, so it doesn't change the link $\hat{b}$. A similar argument shows $\hat{b} = \widehat{b\sigma_n^{-1}}$.

Not only does manipulating a braid by Markov moves preserve the topology of the braid closure, but whenever two braid closures agree, their corresponding braids can be related by a finite number of Markov moves.

Theorem 2.5 (Markov)**.** *Consider the map from the set of all braids to the set of all links given by*

$$\{\mathcal{B}_n\} \to \{links\}$$

$$b \mapsto \hat{b}.$$

If $\widehat{b_1} = \widehat{b_2}$ as links, then b_1 and b_2 are related by a finite number of moves of type I or type II and their inverses.

It is easy to see that the map $b \to \hat{b}$ fails to be injective. For the simplest possible example, take the braid closure of σ_1, which gives the unknot.

It is also true, although much less trivial to show, that the map is onto. Given any link there exists a finite number of Reidemeister moves that manipulates the link until it is in the form of a closure of a braid.

The Markov theorem gives us a way to study links through braid representations, since any braid invariant that is also invariant under the Markov moves can be improved to a link invariant.

2.4.3. The Alexander polynomial

In order for a quantity to be an invariant of links, it must be invariant under the Markov moves of type I and II. From linear algebra, we know that similar matrices have the same determinant. It follows that the determinant of the representation of a braid is invariant under conjugation.

Recall the reduced Burau representation $\rho : \mathcal{B}_n \to GL_{n-1}(\mathbb{Z}[t, t^{-1}])$ and define the matrices $M(b) = I - \rho(b)$ and $\tilde{M}(b) = I - \tilde{\rho}(b)$, where I is the identity matrix with appropriate dimensions in each equation.

Definition 2.6. For $b \in \mathcal{B}_n$, the Alexander polynomial is given by

$$\Delta(\hat{b}, t) = \frac{\det(M(b))}{1 + t + \cdots t^{n-1}}.$$

This establishes the convention that the Alexander polynomial of the unknot is 1, i.e. $\Delta\left(\bigcirc\right) = 1$. We present some results from linear algebra that can be combined to prove that the Alexander polynomial is a link invariant, and state some of its properties.

Lemma 2.7. *Suppose A is an $n \times n$ matrix with the property that there exists a column vector $w = (w_i)^T$ and a row vector $u = (u_j)$ satisfying*

(1) $Aw = 0$,

(2) $uA = 0$,

(3) $w_i \neq 0$, $u_j \neq 0$ *for all* i, j.

That is, A annihilates w, A is annihilated by u, and the coordinates of w and u are all nonvanishing. Then

$$(-1)^{i+j} \frac{\det(A(i,j))}{u_i w_j}$$

is independent of i and j, where $A(i,j)$ denotes the i,jth minor of A, that is, the $(n-1) \times (n-1)$ matrix obtained by the deleting the ith row and the jth column from A.

The matrix $\tilde{M}$ satisfies the hypotheses of this lemma. Recall that $\tilde{\rho}(b)$ had eigenvector $(1, \ldots, 1)^T$ with eigenvalue 1 and invariant row vector $(1, t, t^2, \ldots, t^{n-1})$. If we choose $w = (1, \ldots, 1)^T$ and $u = (1, t, t^2, \ldots, t^{n-1})$, it follows that $\tilde{M}w = 0$ and $u\tilde{M} = 0$. Evidently the coordinates of both w and u are nonvanishing. While the details are omitted, this leads to the proof of the next lemma.

Lemma 2.8.

$$\frac{\det(M(b))}{1 + t + \cdots + t^{n-1}} = \det(\tilde{M}(1,1)).$$

This result gives us the freedom to delete any row and column of the matrix $\tilde{M}$, whose determinant recovers the Alexander polynomial.

The proof that the Alexander polynomial is indeed a link invariant entails checking the invariance of $\Delta(\hat{b}, t)$ under Markov moves using the lemmas.

There exists an efficient classical algorithm to turn any link L into a braid closure $\hat{b}$. For a braid $b \in \mathcal{B}_n$, the Burau representation matrix and its determinant can be computed in polynomial time in the number of strands n and the number and m the number of elementary braids in b.

Theorem 2.9. *The Alexander polynomial of a link can be computed in polynomial time by a Turing machine.*

Note that the size of the Burau representation matrix is only $(n-1)\times(n-1)$ for a braid in $\mathcal{B}_n$. As a comparison, we will see later the sizes of the Jones representation matrices for braids in $\mathcal{B}_n$ grow as $d^n \times d^n$ for some number $d > 1$ as $n \to \infty$.

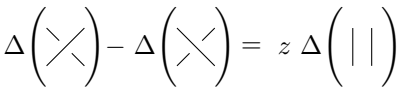
2.4.4. The Alexander-Conway polynomial, writhe, and skein relation

Having introduced the Alexander polynomial, one can define a related link invariant - the *Alexander-Conway polynomial* - through a slight renormalization and by introducing a quantity called the *writhe* of a braid.

Let $b = \sigma_{i_k}^{s_k} \cdots \sigma_{i_1}^{s_1} \in \mathcal{B}_n$. The writhe or braid exponent is given by $e(b) = \sum_{i=1}^{k} s_i$. Taking $z = t^{1/2} - t^{-1/2}$, the Alexander-Conway polynomial is defined as

$$\Delta(\hat{b}, z) = (-t^{1/2})^{n-e(b)-1}\Delta(\hat{b}, t).$$

Under this new parametrization the behavior of our knot invariant with respect to left versus right-handed crossing can be expressed in the elegant form of the *skein relation*.



Exercise 2.10. Deduce the skein relation from the definition of the Alexander-Conway polynomial and Lemma 2.8.

3. The Jones Representation and Jones polynomial

In a manner analogous to how the Alexander polynomial is defined in terms of the Burau representation, another link invariant, the *Jones polynomial*, can be studied alongside the *Jones representation*. Computing the Alexander polynomial is easy in the sense of complexity theory, since there exists a polynomial time algorithm to compute it. On the other hand, assuming that $P \neq NP$, that is, assuming the longstanding conjecture that the complexity classes corresponding to polynomial time and nondeterministic polynomial time are distinct, computing the Jones polynomial is hard in the sense that there does not exist a polynomial time algorithm.

In this section we introduce the necessary background material for constructing the Jones representation of the braid group: the quantum integers, the Temperley-Lieb and Temperley-Lieb-Jones algebra, and the Temperley-Lieb category. Section 4 covers the application of the Jones representation to quantum computing.

3.1. Quantum integers

We should conceptualize the quantum integers as deformations of the integers by q, which we can either think of as generic (a formal variable) or a specific element of $\mathbb{C}^*$.

Definition 3.1. [1] Let $n \in \mathbb{Z}$. Then *quantum n*, denoted $[n]_q$, is given by

$$[n]_q = \frac{q^{n/2} - q^{-n/2}}{q^{1/2} - q^{-1/2}}.$$

For instance, $[1]_q = 1$ and $[2]_q = q^{1/2} + q^{-1/2}$. It is an easy application of L'Hôpital's rule to show that $[n]_q \to n$ in the limit $q \to 1$, recovering the integers. This shows we can truly think of $[n]_q$ as some deformation of n. However, one must take special care when performing arithmetic with quantum integers, since the familiar rules of arithmetic need not apply. However, there is one important relation from integer arithmetic that still holds, the "quantum doubling" formula.

Proposition 3.2. $[2][n] = [n+1] + [n-1]$.

This identity will reappear once we have introduced the Temperley-Lieb algebra.

3.2. The Temperley-Lieb algebra $TL_n(A)$

Our goal is to find braid group representations with properties that are useful for quantum computation. In particular we want to be able to identify elements of the image of these representations with matrices. Towards this end we pass through either the *Temperley-Lieb algebra* or the *Temperley-Lieb-Jones algebra*. To motivate the construction of the Temperley-Lieb algebras, we recall the following theorem that dictates how the the group algebra for a finite group G decomposes into the irreducible representations of G [10].

Theorem 3.3. *Let G be a finite group, and $\mathbb{C}[G] = \{\sum a_g g \mid a_g \in \mathbb{C}\}$ be the group algebra of G over $\mathbb{C}$. Then*

$$\mathbb{C}[G] \cong \bigoplus_i (\dim V_i) V_i,$$

where the V_i are a complete set of representatives of the isomorphism classes of finite-dimensional irreducible representations of G.

[1] There are two conventions in the literature when defining the quantum integers, depending on whether a factor of $1/2$ appears in the exponents; quantum n is sometimes defined as $[n]_q = \frac{q^n - q^{-n}}{q - q^{-1}}$.

To illustrate the theorem we recall the representation theory of S_3. There are three irreducible representations: the trivial, sign, and permutation representations, say U, U', and V, respectively. Then $\mathbb{C}[S_3] = U \oplus U' \oplus 2V$. Hence, as an algebra, $\mathbb{C}[S_3]$ decomposes as $\mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$.

While we can completely describe $\mathbb{C}[G]$ when G is finite, when G is infinite, as in the case of $G = \mathcal{B}_n$, we don't have the same luxury. In order to get a handle on $\mathbb{C}[\mathcal{B}_n]$ we pass to a finite-dimensional quotient. The first step in this process is to construct the *Hecke algebra*.

3.2.1. The Hecke algebra $H_n(q)$

Hereafter we will work in one of two fields, $\mathbb{C}$ or $Q(A)$, the latter of which we use to denote the field of rational functions in the *Kauffman variable* A over $\mathbb{C}$. When we are interested in the *generic* Temperley-Lieb algebra, we work in $Q(A)$, while in general specialize to a choice of A in $\mathbb{C}$. For now we use $\mathbb{F}$ to denote the field $Q(A)$.

The elements of the braid group algebra $\mathbb{F}[\mathcal{B}_n] = \{\sum a_g g \mid g \in \mathcal{B}_n, a_g \in \mathbb{F}\}$ are called formal (or quantum) braids. To motivate what relations we should quotient out by, we record a few observations.

Recall the presentation of the braid group

$$\mathcal{B}_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{r} \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for } i = 1, 2, \ldots, n-1 \end{array} \right\rangle.$$

Taking the quotient of $\mathcal{B}_n$ by the normal subgroup generated by the σ_i^2 results in a group isomorphic to S_n. Thus there is a surjection of the braid group onto the symmetric group, and we have an exact sequence

$$1 \longrightarrow P\mathcal{B}_n \longrightarrow \mathcal{B}_n \longrightarrow S_n \longrightarrow 1.$$

This implicitly defines $P\mathcal{B}_n$, the *pure braid group* on n-strands, which will be revisited in Section 4. In particular, we can get a representation of the braid group by precomposing with a representation of the symmetric group. However, such a representation will not encode all of the information about the braid group that is needed for computation. Instead one must look for representations which do not factor through S_n.

Consider the quotient of $\mathbb{F}[\mathcal{B}_n]$ by quadratic relations $\sigma_i^2 = a\sigma_i + b$, for $i = 1, \ldots, n-1$, where a and b are independent of i. Note however that a and b are not independent of one another, since we can rescale by setting $\tilde{\sigma}_i = \sigma_i/a$. Then the relation becomes

$$\tilde{\sigma_i}^2 = \tilde{\sigma}_i + b/a^2.$$

In other words, we can just take $a = 1$, so that the relation is parametrized by b. Taking the quotient of $\mathbb{F}[\mathcal{B}_n]$ by this relation defines a Hecke algebra.

Definition 3.4. The Hecke algebra $H_n(A)$ is the quotient $\mathbb{F}[\mathcal{B}_n]/I$ of the braid group algebra, where I is the ideal generated by $\sigma_i^2 - (A - A^{-3})\sigma_i - A^{-2}$ for $i = 1, \ldots, n-1$.

A presentation on generators and relations of the Hecke algebra further elucidates its structure. Renormalizing via $q = A^{-4}$, and defining a new set of generators by $g_i = A^{-1}\sigma_i$, we can define

$$H_n(q) = \left\langle g_1, g_2, \ldots, g_{n-1} \;\middle|\; \begin{array}{r} g_i g_j = g_j g_i \text{ for } |i-j| \geq 2 \\ g_{i+1} g_i g_{i+1} = g_i g_{i+1} g_i \\ g_i^2 = q^{-1} g_i + q \end{array} \right\rangle.$$

Due to the Hecke relation $g_i^2 = q^{-1}g_i + q$, $H_n(q)$ (and hence $H_n(A)$) is finite-dimensional.

3.2.2. A presentation of the Temperley-Lieb algebra on generators and relations

In order to obtain the Temperley-Lieb algebra, we must pass through one more quotient. Reparametrizing once again, rescaling the generators of $H_n(q)$ by defining $u_i = A\sigma_i - A^2$ and $d = -A^2 - A^{-2} = -[2]_q$, the Hecke algebra relations become the following.

- $u_i u_j = u_j u_i$ when $|i-j| \geq 2$ (far commutativity)
- $u_i u_{i+1} u_i - u_i = u_{i-1} u_i u_{i-1} - u_{i-1}$ (braid relation)
- $u_i^2 = d u_i$ (Hecke relation)

To obtain the Temperley-Lieb algebra, we set the braid relation above to 0, so impose one additional relation:

- $u_i u_{i\pm 1} u_i = u_i$

Definition 3.5. The generic Temperley-Lieb algebra $TL_n(A)$ is the quotient of the Hecke algebra $H_n(q)/I$, where I is the ideal generated by $u_i u_{i\pm 1} u_i - u_i$.

The generic Temperley-Lieb algebra $TL_n(A)$ is *semisimple* (also called a *multi-matrix algebra*), a direct sum of matrix algebras $M_{n_i}(\mathbb{F})$. This is the fact that enables us to work with matrix representations of the braid group, which, if unitary, can be thought of physically as quantum gates. Understanding how $TL_n(A)$ decomposes into matrix algebras is the key to applying the Jones representation to quantum computation.

Theorem 3.6. *If A is generic, then $TL_n(A)$ is semisimple. If $A \in \mathbb{C}^*$, then $TL_n(A)$ is not in general semisimple.*

We will return to the semisimple structure of $TL_n(A)$ after introducing its picture presentation, in which computations can be performed using a graphical calculus.

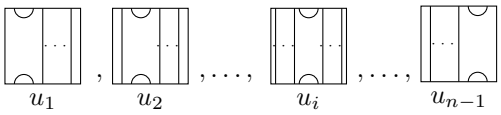
3.2.3. A picture presentation of the Temperley-Lieb algebra

In the graphical calculus the variable $d = -A^2 - A^{-2}$ previously defined in the context of the presentation of $TL_n(A)$ with generators and relations takes on an important role. The variable d is called the *loop variable*, for reasons that will soon be clear.

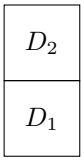
Definition 3.7. A diagram in $TL_n(A)$ is a square with n marked points on the top edge and n marked points on the bottom edge, and these $2n$ boundary points are connected by non-intersecting smooth arcs. In addition, there may be simple closed loops in the diagram.

An equivalent diagram can be obtained by multiplying by a factor of d for each closed loop removed, and we say two diagrams are the same if they are *d-isotopic*, that is, if they are isotopic and the boundary points are of the respective diagrams are paired in the same way.

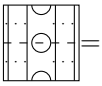
An arbitrary element of $TL_n(A)$ is a formal sum of diagrams, where each diagram is a word in the generators u_i. The diagram of u_i has a "cup" on the top edge connecting the ith and $i+1$st marked points, and a "cap" on the bottom edge connecting the ith and $i+1$st marked points. The jth marked point on the top edge is connected to the jth marked point on the bottom edge by a "through strand".



Multiplication of diagrams is performed by vertical stacking followed by rescaling- if $D_1, D_2 \in TL_n(A)$, then $D_1 \cdot D_2$ is given by stacking D_2 on top of D_1 and rescaling to a square.



The Temperley-Lieb relations, far commutativity, the braid relation, and the Hecke relation, can all be verified using the graphical calculus. For example, the Hecke relation is illustrated by

$u_i^2 =$  $= du_i.$

Exercise 3.8. Show that the generators u_i satisfy far commutativity and the braid relation.

Theorem 3.9. *The diagrammatic algebra for $TL_n(A)$ is isomorphic to the abstract Temperley-Lieb algebra given by generators and relations.*

The proof of this result is made difficult by the diagrammatic algebra being defined up to d-isotopy.

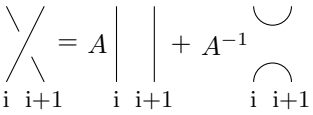
As a vector space, $TL_n(A)$ is generated by all the Temperley-Lieb diagrams in $TL_n(A)$, of which there are Catalan number $c_n = \frac{1}{n+1}\binom{2n}{n}$ many up to d-isotopy. In order to prove that the set of Temperley-Lieb diagrams forms a basis of $TL_n(A)$ as a vector space, one must show that there are no linear relations among the diagrams. This can be done by introducing an inner product on $TL_n(A)$, defined through the *Kauffman bracket* and a map called the *Markov trace*, which can be thought of as a "quantum" analogue of the braid closure.

3.2.4. The Kauffman bracket

To find finite dimensional representations of the braid group, we begin by looking for an algebra homomorphism from the braid group algebra to finite matrix algebras,

$$\rho : \mathbb{F}[\mathcal{B}_n] \to \bigoplus_i M_{n_i}(\mathbb{F}).$$

A finite dimensional representation of $\mathcal{B}_n$ is then obtained via the restriction of ρ to the braid group, $\rho\,\big|_{\mathcal{B}_n}$. The Kauffman bracket $\langle\cdot\rangle : \mathbb{F}[\mathcal{B}_n] \to TL_n(A)$ is an algebra homomorphism which we can think of as producing Temperley-Lieb diagrams from formal braids by resolving crossings in the braid group algebra.

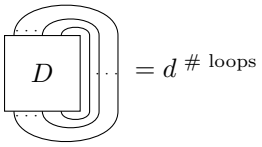


In terms of braid group generators and Temperley-Lieb generators, the Kauffman bracket is expressed by

$$\sigma_i = AI + A^{-1}u_i.$$

3.2.5. The Markov trace

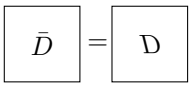
The Markov trace of a diagram is the map Tr: $TL_n(A) \mapsto \mathbb{F}$ that sends a diagram D to its tracial closure.



This defines the Markov trace on a basis of diagrams of $TL_n(A)$, and by extending linearly it is defined on all of $TL_n(A)$. From the trace one can define an inner product $\langle \cdot, \cdot \rangle : TL_n(A) \times TL_n(A) \to \mathbb{F}$ given by

$$\langle D_1, D_2 \rangle = \mathrm{Tr}(\overline{D_1} D_2).$$

where the bar over a diagram denotes the diagram obtained by reflecting across the horizontal midline.



Now the question of whether the diagrams in $TL_n(A)$ are linearly independent can be translated into the question of whether the Gram matrix $(M)_{ij} = \langle \overline{D_i}, D_j \rangle$ has determinant zero. M is a $c_n \times c_n$ matrix, where c_n is the nth Catalan number. While the details are not provided here, it is possible to express the determinant of M in the closed form

$$\det(M) = \prod_{i=1}^{n} \Delta_i(d)^{a_{n,i}}$$

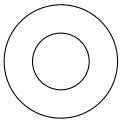
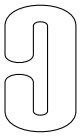
where $a_{n,i} = \binom{2n}{n-i-2} + \binom{2n}{n-i} - 2\binom{2n}{n-i-1}$ and $\Delta_i(x)$ is the ith Chebyshev polynomial of the second kind, defined recursively by $\Delta_0 = 1, \Delta_1 = x$, and $\Delta_{i+1} = x\Delta_i - \Delta_{i-1}$.

Therefore generic Temperley-Lieb diagrams are linearly independent, but whenever the loop variable d is a root of a Chebyshev polynomial appearing in the determinant of the Gram matrix, there is some linear dependence among the Temperley-Lieb diagrams. The Chebyshev polynomials are related to the quantum integers, which we will see later.

3.3. The Jones polynomial

To motivate the form that the Jones polynomial takes, we investigate the properties that would be needed for a quantity to give an invariant of a link. Given

a braid $b \in \mathcal{B}_n$, we can apply the Kauffman bracket $\langle\cdot\rangle$ to resolve the crossings, resulting in a sum of 2^n Temperley-Lieb diagrams. Then $\langle b\rangle \in TL_n(A)$, and we can apply the Markov trace. Thus we can consider their composition $\mathrm{Tr}\langle\cdot\rangle : \mathcal{B}_n \to \{\text{links}\}$. For example,

$\mathrm{Tr}\langle$  $\rangle = A$  $+ A^{-1}$  $= Ad^2 + A^{-1}d = -A^3 d$

A similar computation shows that the Markov trace of the Kauffman bracket applied to the left handed crossing evaluates to $-A^{-3}$. However, if we calculate the trace of the unknot, which is topologically equivalent to the closure of the right-handed crossed, the result is d. While $\mathrm{Tr}\langle\cdot\rangle$ is too sensitive to provide a knot invariant, it can be calibrated by multiplying a factor of $(-A^{-3})^{e(b)}$, where $e(b)$ is the writhe of the braid b introduced in Section 2.

We are now ready to define the Jones polynomial[2] of a link.

Definition 3.10. Let $b \in \mathcal{B}_n$, and let $L = \hat{b}$ be the link obtained from the braid closure of b. Then the Jones polynomial $J(L, q)$ of L is given by

$$J(L, q) = \frac{(-A^{-3})^{e(b)}\mathrm{Tr}\langle b\rangle}{d}.$$

The reason for the factor of d in the denominator is to set the convention that the Jones polynomial of the unknot be equal to 1. It is necessary to point out the the Jones polynomial is not well defined if we try to evaluate at a general link instead of a braid closure - in order to make sense of the Jones polynomial of a link, it must be oriented.

By the Markov theorem, we know that whenever two links arising from braid closures are equal, they are related by a finite number of Markov moves.

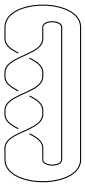
Therefore, it must be verified that the Jones polynomial is invariant under the Markov moves. An diagrammatic argument identical to that for demonstrating the invariance of the Alexander polynomial under the braid closure can be given.

Let $a, b \in \mathcal{B}_n$. Invariance under conjugation can be seen by sliding diagrams around their tracial strands. The proof-by-picture is identical to that provided for the proof of invariance of the Markov moves under braid closure, except one replaces the braid diagram b by a Temperley-Lieb diagram. Similarly if $a = b\sigma_n^{\pm 1}$, then the diagrammatic proof of invariance under stabilization is analogous to that for braids, except now we introduce a factor of $-A^{\mp 3}$ to correct for the writhe introduced by $\sigma_n^{\pm 1}$.

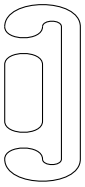
[2]Technically $J(L, q)$ is a Laurent polynomial in $q^{1/2}$, but it is still referred to as a polynomial in the literature.

3.3.1. Example: the Jones polynomial of the trefoil knot

We end this discussion of the Jones polynomial with a famous example - the right-handed trefoil knot, $\widehat{\sigma_1^3}$.



There are three crossings, and hence $2^3 = 8$ terms in the resolution $\langle \sigma_1^3 \rangle$. The terms can be organized by a binary tree of depth 3, where each edge is labeled by a "+" or a "−" according to the term in the Kauffman bracket. We compute the " $-+-$ " term as an example.

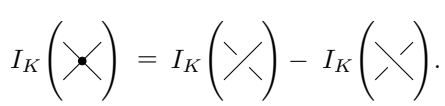


$$= -A^{-3} \cdot (A^{-1} \cdot A \cdot A^{-1}) \cdot d^2$$

One can check that $J(\widehat{\sigma_1^3}, q) = q + q^3 - q^4$. It turns out that the Jones polynomial of the left-handed trefoil knot is different. This is an improvement over the Alexander polynomial, which cannot distinguish a knot from its mirror image.

Open problem 3.11 Does there exist a nontrivial knot with the same Jones polynomial as the unknot? Are there knots which are topologically different from their mirror image but have the same Jones polynomial? How does one interpret the Jones polynomial in terms of classical topology?

Exercise 3.11. Let I_K denote an invariant of knots. Then I_K naturally extends to knots with *double points*, via



Now let k be a knot, and let $q = e^h$, where h is a formal variable. Then the Jones polynomial has the property that

$$J(k, e^h) = \sum v_i h^i$$

where the v_i are knot invariants and the series is potentially infinite. The Alexander polynomial has the same property, and in the series expansion

$$\Delta(k, z) = 1 + c_2 z^2 + c_4 z^4 + \cdots$$

the c_i are known as the *Vassiliev invariants.*
(a) Show that $v_1 = 0$.
(b) Show that if there are more than three double points, $c_2 = v_2 = 0$.
(c) Show that $v_2 = -2c_2$.

3.4. The generic Jones representation

While the Alexander polynomial was defined in terms of the Burau representation of the braid group, we were able to formulate a definition of the Jones polynomial that did not depend on the Jones representation. However, in order to approximate the Jones polynomial on a quantum computer, the Jones representation of the braid group must be understood. The definition of the Jones representation depends on how the Temperley-Lieb algebras decompose into direct sums of matrix algebras.

Definition 3.12. The Jones representation $\rho_{k,n}$ at level k of the n-strand braid group is given by the image of the braid group under the Kauffman bracket

$$\langle\cdot\rangle : \mathbb{F}[\mathcal{B}_n] \to TL_n(A) = \bigoplus_i M_{n_i}(\mathbb{F}).$$

To be precise, the braid group algebra $\mathbb{F}[\mathcal{B}_n]$ is resolved into the Temperley-Lieb algebra $TL_n(A)$ via the Kauffman bracket $\langle\cdot\rangle$, and then after identifying the Temperley-Lieb algebra as a direct sum of matrix algebras $\bigoplus_i M_{n_i}(\mathbb{F})$, restricting to the braid group gives a representation of $\mathcal{B}_n$.

There is a standard way to decompose an algebra as a direct sum of matrix algebras by finding its *matrix elements*, elements e_{ij} satisfying $e_{ij}e_{kl} = \delta_{jk}e_{il}$. To motivate the form of that such elements take in $TL_n(A)$, we work out the solution for some small values of n.

3.4.1. Example: matrix decomposition of $TL_2(A)$

$TL_2(A)$ is generated as a vector space by the diagrams  and  which we denote by 1 and u_1, respectively. We look for elements e_1 and e_2 satisfying $e_1^2 = e_1$, $e_2^2 = e_2$, and $e_1e_2 = e_2e_1 = 0$. For then we could identify

$$e_1 \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } e_2 \longrightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

The choice of $e_1 = 1-\frac{1}{d}u_1$ and $e_2 = \frac{1}{d}u_1$ results in two matrix elements. Indeed, the following equations show that idempotency and centrality of these choices of e_i follow from the Hecke relation.

$$e_1^2 = (1-\frac{1}{d}u_1)(1-\frac{1}{d}u_1) = 1-\frac{2}{d}u_1+\frac{1}{d^2}u_1^2 = 1-\frac{2}{d}u_1+\frac{d}{d^2}u_1 = 1-\frac{1}{d}u_1 = e_1,$$

$$e_2^2 = (\frac{1}{d}u_1)^2 = \frac{1}{d^2}u_1^2 = \frac{1}{d}u_1 = e_2, \text{ and}$$

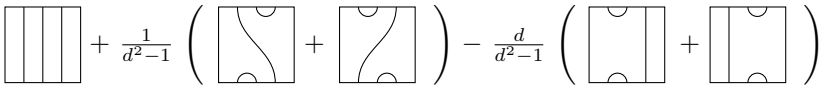
$$e_1e_2 = (1-\frac{1}{d}u_1)\frac{1}{d}u_1 = e_2e_1 = \frac{1}{d}u_1-\frac{1}{d}u_1 = 0.$$

Therefore, the decomposition of a generic Temperley-Lieb algebra at $n = 2$ is given by $TL_2(A) \cong \mathbb{F} \oplus \mathbb{F}$.

3.4.2. Example: matrix decomposition of $TL_3(A)$

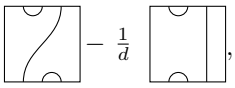
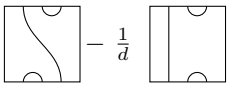
As a vector space $TL_3(A)$ is spanned by  ,  ,  ,  , and  . By a dimension argument, it is immediate that if $TL_3(A)$ is to be a matrix algebra, then we must have $TL_3(A) \cong \mathbb{F} \oplus M_2(\mathbb{F})$. Thus one must find an idempotent element p to identify with the matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

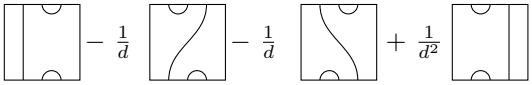
The element



has the desired property. We will come to know this element of $TL_3(A)$ as the *Jones-Wenzl projector* p_3.

One can check that the following $\tilde{e}_{ij}$, once properly normalized, extend p to a set of matrix elements.

$\tilde{e}_{11} =$  , $\tilde{e}_{21} =$  , $\tilde{e}_{12} =$ 

$\tilde{e}_{22} =$ 

Already in the case of $n = 3$, our matrix elements are becoming unwieldy. We remark that if $TL_n(A) \cong \bigoplus M_{n_i}(\mathbb{F})$, then the dimension of the Temperley-Lieb algebra, namely the Catalan number c_n, can be written as a sum of squares

$$\frac{1}{n+1}\binom{2n}{n} = \sum_i n_i^2.$$

For example, this relation gives the decompositions $14 = 1 + 4 + 9$, $42 = 1 + 16 + 25$, and $132 = 1 + 25 + 25 + 81$.

The general theory of how $TL_n(A)$ decomposes into matrix algebras is governed by elements of the Temperley-Lieb algebra called the *Jones-Wenzl projectors*, which are minimal central idempotents. While the details of the general theory are beyond the scope of these notes, studying the Jones-Wenzl projectors is essential for using the graphical calculus to compute the Jones representation, of which we provide an example in Section 4.

3.5. The Jones-Wenzl projectors p_n

The following theorem characterizes the Jones-Wenzl projectors.

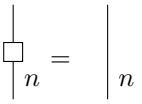
Theorem 3.13. *There exists a unique nonzero element p_n in $TL_n(A)$ such that*
(1) $p_n^2 = p_n$,
(2) $u_i p_n = p_n u_i = 0$ for all $i = 1, \ldots, n-1$.

The proof of this theorem is outlined as follows. First we prove uniqueness. Suppose that p_n and p_n' satisfy (1) and (2), and write $p_n = c_0 \cdot 1 + \sum_{i=1}^{n-1} c_i u_i$, where we have simply used the fact that $\{1, u_1, \ldots, u_{n-1}\}$ form a basis of $TL_n(A)$ as a vector space. Immediately, the condition $p_n^2 = p_n$ forces $c_0 = 1$, since

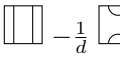
$$p_n^2 = (c_0 \cdot 1 + \sum_{i=1}^{n-1} c_i u_i)^2 = c_0^2 + \cdots = p_n.$$

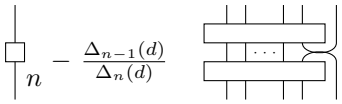
Hence $c_0^2 = c_0$, and so $c_0 = 1$. So we can write $p_n = 1 + \sum_{i=1}^{n-1} c_i u_i$ and $p_n' = 1 + \sum_{i=1}^{n-1} c_i' u_i$. Then one can check that $p_n' = p_n p_n' = p_n$.

As for existence, we provide an explicit construction. We will use the notations

$p_n =$  $=$

to represent the nth Jones-Wenzl projector.

Define $p_1 =$  , $p_2 =$  $-\frac{1}{d}$  and define p_n inductively by

$p_{n+1} =$ 

where $\Delta_n = \mathrm{Tr}(p_n)$ is the Markov trace of the nth Jones-Wenzl projector. It is straightforward to verify that this construction results in idempotent objects that annihilate the generators of the Temperley-Lieb algebra.

Open problem 3.14. Does every diagram u_i appear in p_{n+1}? (This question was answered affirmatively by Brannan and Collins after this manuscript was prepared. [3])

3.5.1. The recursive definition of p_n and the quantum doubling formula

The coefficients Δ_n can be calculated explicitly. For now we will take it as fact that $\Delta_n = (-1)^n[n+1]$.

We can recover the formula $[2][n] = [n+1]+[n-1]$ from quantum arithmetic that we proved previously. Recall that $d = -A^2 - A^{-2} = -q^{1/2} - q^{-1/2} = -[2]_q$. Taking the Markov trace of both sides of the recursive formula for p_{n+1} gives

$$Delta_{n+1} = d\Delta_n - \frac{\Delta_{n-1}(d)}{\Delta_n(d)}\Delta_n.$$

and hence

$$(-1)^{n+1}[n+2] = (-1)^n[n+1](-[2]) - (-1)^{n-1}[n].$$

After simplifying this becomes

$$[n+2] = [2][n+1] - [n],$$

which after rearranging and reindexing the terms recovers the quantum doubling formula.

3.6. The non-generic Jones representation of the braid group

The generic Jones representation of the braid group was given by the image of a braid in the matrix algebra decomposition of the generic Temperley-Lieb algebra. What happens for specific $A \in \mathbb{C}^*$? Towards physical applicaitons the first question one might ask is what values of A result in a unitary Jones representation.

Let $A \in \mathbb{C}$ and suppose $\rho(\sigma_i)^\dagger = \rho(\sigma_i^{-1})$ for $i = 1, 2, \ldots, n$. Then assuming $u_i^\dagger = u_i$, one can check that

$$\rho(\sigma_i)^\dagger\rho(\sigma) = (A^\dagger + (A^{-1})^\dagger u_i^\dagger)(A + A^{-1}u_i) = |A|^2 + |A^{-1}|^2 du_i + u_i(A^\dagger A^{-1} + (A^{-1})^\dagger A)$$

is equal to 1 when $|A| = 1$. One can also show that $u_i^\dagger = u_i$ and $|A| = 1$ are actually necessary conditions for ρ to be a unitary representation. That is, $A \in S^1$. This answers the question of unitarity.

More can be said about what happens for specific value of the Kauffman variable A. Recall the recursive definition of the Jones-Wenzl projector p_{n+1}, which involves the coefficient $\frac{\Delta_{n-1}}{\Delta_n}$. Thus if A is a root of Δ_n, the Jones-Wenzl projector p_{n+1} is undefined. The following proposition characterizes when A is a root of Δ_n.

Proposition 3.14. $\Delta_n = (-1)^n[n+1] = (-1)^n \frac{A^{2n+2}-A^{-2n-2}}{A^2-A^{-2}}$.

Corollary 3.15. *The Jones representation is well-defined when A is not a root of unity.*

To see what can go wrong when A is a root of unity, consider $TL_2(A) = \mathbb{C}[1, u_1]$ when A is a primitive eighth root of unity. Then $-A^{-2} = A^2$ and hence $d = -A^2 - A^{-2} = 0$. But then $TL_2(A) = \mathbb{C}[1, x]$ where $x^2 = 0$, which is not a matrix algebra. For suppose $TL_2(A)$ were a matrix algebra. Then the dimension would force the isomorphism $TL_2(A) \cong \mathbb{C} \oplus \mathbb{C}$, and there would exist two central idempotents e_1 and e_2. Let $e_1 = a + bx$. Then $(a + bx)^2 = a^2 + 2abx + b^2x^2 = a^2 + 2abx = a + bx$, which has no consistent solution.

This is illustrative of a general problem that we may not necessarily get a matrix algebra when A is a root of unity. We bypass this difficulty by passing to a quotient of the Temperley-Lieb algebra which is semi-simple, called the *Temperley-Lieb Jones algebra*. Then the non-generic Jones representation is defined in analogy with the generic definition, as the image of the braid group in a matrix algebra decomposition of $TLJ_n(A)$.

3.7. The Temperley-Lieb-Jones algebra $TLJ_n(A)$

Let $r \geq 3$, and let be A is a primitive $4r$th root of unity if r is even or a primitive $2r$th root of unity if r is odd.

Definition 3.16. The Temperley-Lieb-Jones algebra, denoted by $TLJ_n(A)$, is the semisimple algebra formed by taking the quotient of $TL_n(A)$ by the $(r-1)$st Jones-Wenzl projector p_{r-1}.

Open problem 3.17 Given a finite-dimensional algebra, taking the quotient by a Jacobson radical gives a semisimple algebra. Is the Jones-Wenzl quotient the same as the Jacobson quotient?

Now that we understand how the Jones representation is defined as a matrix representation, we turn to the matters of computing representation, studying its properties, and understanding how it can be used to perform quantum computation.

3.8. The Temperley-Lieb category $TLJ(A)$

The Jones representations of an n-strand braid group are determined by how $TL_n(A)$ or $TLJ_n(A)$ decomposes into matrix algebras. In order to discuss the physical applications, we must make the connection between $TLJ_n(A)$ and anyons. This requires organizing the Temperley-Lieb-Jones algebras $\{TLJ_n\}$ in a *Temperley-Lieb category.* The objects of this category will be finite sets of points $a_1, \ldots, a_n$ in the unit interval $[0, 1]$, allowing for the empty set, each

point colored by an element of the *label set* $\mathcal{L} = \{0, 1, \ldots, k\}$ where at each marked point there is a Jones-Wenzl projector p_{a_n}.

Given two objects, which we label $X_{a_1,\ldots,a_n}$ and $X_{b_1,\ldots,b_m}$, where the subscript indicates the integer labeling of the specified points, the morphisms are as follows. If $m + n$ is odd, then the only morphism between the two objects is the zero morphism. If however $m + n$ is an even number, then the set of morphisms is given by the span of all Temperley-Lieb-Jones diagrams connecting the points X_{a_i} and X_{b_j}, together with disjoint unions of loops colored by natural numbers. That is,

$$\mathrm{Hom}(X_{a_1,\ldots,a_n}, X_{b_1,\ldots,b_m}) = \mathbb{F}[\text{colored TL diagrams connecting } \sum a_i + \sum b_j]$$

modulo the following three relations.

- $\bigcirc_i = \Delta_i$
- relative d-isotopy
- $p_{k+1} = 0$

Note that since p_{k+1} vanishes in $TLJ(A)$, the recurrence relation for Jones-Wenzl projectors implies that p_m vanishes for all $m > k + 1$. The following three properties of the category are immediate from the definition.

Proposition 3.17.

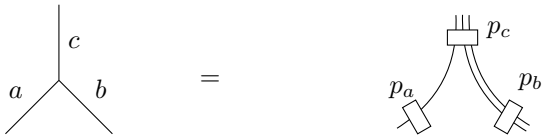
(1) $TLJ(A)$ is a $\mathbb{C}$-linear category

(2) $Hom(X, X)$ is an algebra for all X

(3) $Hom(X, Y)$ is a $Hom(X, X)-Hom(Y, Y)$ bimodule

3.8.1. Trivalent vertices

The trivalent vertex is the most fundamental part of the Temperley-Lieb category and the key to understanding the morphism spaces.The following figure from [23] gives the resolution of a labeled trivalent vertex into Temperley-Lieb diagrams.



The labeling of the trivalent vertex is subject to the following conditions:

(1) $a+b+c$ is even ("parity")

(2) $a+b \geq c, b+c \geq a$, and $c+a \geq b$ ("triangle inequality")

(3) $a+b+c \leq k$ ("positive energy condition")

For example, the trivalent vertex with each edge labeled by 2 is depicted below.

The following definition frames some of the objects we have already encountered in the TLJ category.

Definition 3.18.

(1) As an algebra, $TLJ_n(A)$ is the Hom space of n points on the unit interval, each marked by 1, with itself. We will denote this by $\mathrm{Hom}(1^{\otimes n}, 1^{\otimes n})$. More generally, the shorthand a stands for the object with one point in the unit interval, marked by a.

(2) The *colored Temperley-Lieb-Jones algebra* is given by $\mathrm{Hom}(a^{\otimes n}, a^{\otimes n})$, where $a \in \{0, 1, \ldots, k\}$.

(3) The Jones representation for $TLJ_n(A)$ is given by its image on $\bigoplus_{n_i} \mathrm{Hom}(i, 1^{\otimes n})$. The colored Jones representation is defined analogously for the colored Temperley-Lieb-Jones algebra.

3.8.2. Physical interpretation of $TLJ(A)$

We want to have a physical interpretation to go along with our definition of $TLJ(A)$. Morphisms in the category, which are Temperley-Lieb-Jones diagrams, depict quantum processes of *anyons*, the quasi-particle excitations of a 2D topological quantum system, such as those theorized to exist in fractional quantum Hall states.

In terms of the mathematical formalism:

Definition 3.19. An object X in the Temperley-Lieb-Jones category is simple if the morphism space $\mathrm{Hom}(X, X) \cong \mathbb{C}$, in which case we say X is an anyon.

The number of distinct types of anyons is dictated by k, the level of the theory, and each type of anyon has an associated number, called its quantum dimension.

Definition 3.20. The quantum dimension of $a \in \mathcal{L}$, thought of as a representative of an isomorphism class of simple objects, is given by the loop value $d_a = \bigcirc_a$.

The structure of the category captures the notion of fusion of particles.

Definition 3.21. The fusion rules are the collection $\{N_{ab}^c = \dim Hom(a \otimes b, c) \mid a, b, c \in L\}$. More compactly, the fusion rules are implicitly defined through the equation

$$a \otimes b = \bigoplus_c N_{ab}^c c$$

where c runs over the label set $\{0, 1, 2, \ldots, k\}$.

Anyons generalize bosons (like photons) and fermions (like electrons) in two dimensions. Given n indistinguishable particles, with locations $x_1, \ldots, x_n$, then the type of particle is determined by what happens to their wavefunction $\psi(x_1, \ldots, x_n)$ upon interchanging their locations. For bosons, interchanging produces no change, while for fermions, a negative sign is generated by the interchange of any particles. That is

$$\psi(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = \pm\psi(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n)$$

depending on whether the particles are bosons or fermions. When we allow the wavefunction to be altered by an arbitrary phase $e^{i\theta}$, then we have an *anyon*. For natural reasons one only considers rational phases of the form $e^{i\pi p/q}$ where $p, q \in \mathbb{Z}$. The reason allowing an arbitrary phase produces this more general picture in two dimensions is due to the fact that there are no nontrivial knots in $\mathbb{R}^4$. More precisely, if $S^1 \hookrightarrow \mathbb{R}^4$ is an embedding, then the image of S^1 can always be isotoped to the trivial knot.

For topological quantum computation, we are interested in values of k for which the corresponding topological phase of matter features anyons which are *nonabelian*, i.e. those for which the representations of the braid group have non-abelian image for n large enough.

4. Anyon Systems and Anyonic Quantum Computation

In this section we describe the algebraic theory of anyon systems, which is given by the Temperley-Lieb-Jones category $TLJ(A)$ for a fixed $A = \pm \mathrm{i}\, e^{\pm 2\pi i/4r}$, whose associated TQFT is known as the *Jones-Kauffman theory at level k*. The focus will be on two theories, the *Ising theory* and the *Fibonacci theory*. In this section, we will use the terms anyon and Jones-Wenzl projector interchangeably. Anyons can be modeled by simple objects in unitary modular categories; Jones-Wenzl projectors represent simple objects in Jones-Temperley-Lieb categories.

Anyons can be harnessed to store and manipulate quantum bits, or *qubits*, leading to a model of quantum computation whose topological nature endows

it with a special robustness. Braiding the anyons gives a *quantum gate* that acts on qubits via the Jones representation. Given a specific anyon model of level k described by a Temperley-Lieb Jones category $TLJ(A)$, understanding the image of the Jones representation $\rho_{k,n} : \mathcal{B}_n \to TLJ_n(A) \cong \bigoplus_{n_i} M_{n_i}(\mathbb{C})$ is tantamount to assessing the power of the anyons to perform quantum computation. At minimum the images of the braid group representations must be infinite and dense in order for the model to be *universal* for quantum computation by braiding alone, that is, powerful enough to accurately and efficiently perform quantum computation.

This section is organized as follows. First we introduce the Ising and Fibonacci theories. Then for each of the two theories we investigate the dimensions of certain Jones representations by counting admissible labelings of fusion trees, and demonstrate how to encode a qubit with two dimensional representations. Then we show how to compute the Jones representation of the four-strand braid group at level 2, and trivial total charge. After introducing the R-symbols and F-symbols, data coming from the categorical structure of TLJ theories, we sketch how to compute the Jones representation of the three-strand braid group at level 3, with nontrivial total charge. Finally, with representations for the Ising theory and Fibonacci theory in hand, we present some results about their images and interpret the consequences for their corresponding anyonic models of quantum computation.

4.1. Introduction

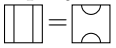
We begin by setting the parameters of the theory $TLJ(A)$ that will describe our anyon model. Pick an integer $r \geq 3$, and choose $A \in \{\pm ie^{\pm 2\pi i/4r}\}$. This choice of the Kauffman variable ensures that the associated braid group representations are unitary, which is necessary for them to be physically meaningful. Then the level of the theory for this choice of A is $k = r-2$. For each level, there are 4 essentially equivalent theories, depending on which of the four choices of A are made. Then the loop variable d can be expressed in terms of the level by the equation

$$d = -A^2 - A^{-2} = e^{\pm 4\pi i/4r} - e^{\mp 4\pi i/4r} = 2(\cos \pi/r) = 2\cos\frac{\pi}{k+2}.$$

The first few levels $k = 1, 2, 3$ then correspond to $d = 1, \sqrt{2}, \phi$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.

4.1.1. Level 1

As a warmup to the $TLJ(A)$ theories that will be useful for quantum computation, we begin with level $k = 1$. The loop variable becomes $d = 2\cos\frac{\pi}{3} = 1$, giving us the freedom to create and destroy loops as we please without having to account for them with a multiplicative factor.

The $(k+1)$st Jones-Wenzl projector that vanishes in $TLJ_n(A)$ is given by $p_2 =$  and hence  in the level 1 theory. This category is equivalent to the category of super-vector spaces; it describes the trivial free fermion topological theory.

4.1.2. The Ising and Fibonacci theories

We first introduce the two anyon models in parallel, choosing

$$A = \begin{cases} ie^{-2\pi i/16} & k = 2 \text{ (Ising)} \\ ie^{2\pi i/20} & k = 3 \text{ (Fibonacci)} \end{cases}.$$

$TLJ(A)$ is a *unitary modular category* (UMC) when k is even, as for the Ising theory, and a unitary pre-modular tensor category when k is odd. As for $k = 3$, it contains the Fibonacci sub-theory, which is a UMC of rank 2.

For level $k = 2$ ($r = 4$), the simple Jones-Wenzl projectors are $\{p_0, p_1, p_2\}$. Thought of as anyons, the projectors have an alternative physical labeling $\{1, \sigma, \psi\}$, corresponding to the vacuum (ground state), *Ising anyon*, and *Majorana fermion*, respectively. The fusion rules for the Ising theory, in their most succinct form, are given by $1 \otimes x = x \otimes 1 = x$ for $x \in \{1, \sigma, \psi\}$, $\sigma \otimes \sigma = 1 \oplus \psi$, $\sigma \otimes \psi = \psi \otimes \sigma = \sigma$, and $\psi \otimes \psi = 1$. The relation $\sigma \otimes \sigma = 1 \oplus \psi$ means that when two σ particles are fused, there are two possible fusion channels. This is what allows one to encode quantum information in the corresponding representation space.

To prove that $1, \sigma$, and ψ are the only simple objects when $k = 2$, we need to compute the spaces $\mathrm{Hom}(x, x)$. A nice way to do this is to use the inner product $\langle \cdot, \cdot \rangle$ that was previously defined on the Temperley-Lieb algebra in terms of the Markov trace. Specializing A to the particular root of unity, we have the following property.

Proposition 4.1. *For $A = \pm \mathrm{i}\, e^{\pm 2\pi i/4r}$, this inner product is positive definite on all $Hom(X, Y)$.*

For level $k = 3 (r = 5)$, the simple Jones Wenzl projectors are $\{p_0, p_1, p_2, p_3\}$. The subset $\{p_0, p_2\}$ or $\{1, \tau\}$ corresponding to the vacuum and the *Fibonacci anyon* generates the Fibonacci subtheory. The Fibonacci fusion rules are given by $1 \otimes \tau = \tau \otimes 1 = \tau$, and $\tau \otimes \tau = 1 \oplus \tau$. Like in the Ising theory, it is this multi-fusion channel that we will use to encode a qubit.

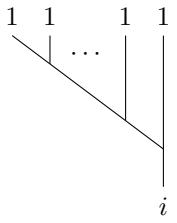
4.1.3. Notation

Unfortunately, two different things have been denoted by 1's: the $TLJ(A)$ label $1 \in \mathcal{L}$, and the ground state 1 in an anyon system such as for the Ising and

Fibonacci theories corresponding to $0 \in \mathcal{L}$. Typically it will be clear from the context and which is meant and for the moment we will use $\mathcal{L}$ when labeling diagrams to avoid confusion.

Having chosen $A = \pm ie^{\pm 2\pi i/r}$, we consider the Jones representation $\rho_{k,n,i} : \mathcal{B}_n \to TLJ_n(A) \to M_{n_i}(\mathbb{C})$. Such a representation is parametrized by the level k of the theory, the number of strands n in the braid group, and the *total charge* i.

Define the vector space $V_{k,n,i}$ to be the $\mathbb{C}$-span of the *fusion trees*



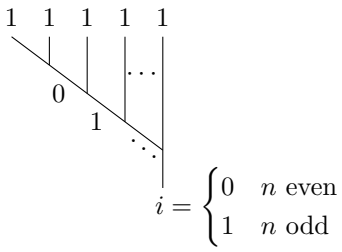
where the internal edges are admissibly labeled by elements of the label set $\mathcal{L} = \{0, 1, 2, \ldots, k\}$. Physically, an admissible labeling of a fusion tree corresponds to a possible fusion process of the corresponding anyons.

Our ultimate goal is to understand the image of the Jones representation $\rho_{k,n,i}(\mathcal{B}_n)$ in $U(V_{k,n,i})$, the unitary transformations on the vector space $V_{k,n,i}$, and interpret them as quantum gates. As a first step we count admissible labelings of Ising and Fibonacci fusion trees to get the dimension of the representations for small n, looking for a two-dimensional representation in which to encode a qubit in order to get single-qubit gates. We will eventually also want a representation of at least dimension four, so that we can produce two-qubit gates. We will see that single and double-qubit gates can be enough to build universal quantum computers.

As a warm up to the Ising and Fibonacci theories, we first consider $k = 1$.

4.1.4. Dimensions of level 1 representations

When $k = 1$, the label set has two elements, $\mathcal{L} = \{0, 1\}$. Depending on whether n is even or odd, by a parity argument there is only one way to admissibly label the fusion tree by elements of $\mathcal{L}$.



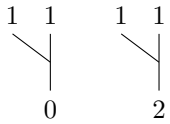
Thus when $k = 1$ we have a one-dimensional representation of the braid group $\mathcal{B}_n$.

4.2. Dimensions of Level 2 representations

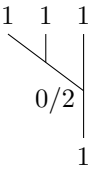
Predictably, the dimension of the representation of $\mathcal{B}_n$ gets more complicated as we increase the level of the theory. To motivate the general pattern, we work through the first few values of n explicitly, labeling fusion trees with elements of $\mathcal{L} = \{0, 1, 2\}$.

4.2.1. Dimensions of level 2 representations for the Ising theory

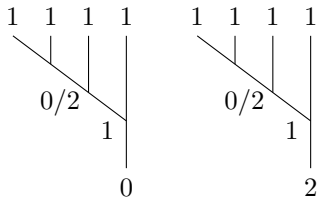
For $n = 2$, there are two admissible values of i for the fusion tree, resulting in two one-dimensional representations.



When $n = 3$, the value of i is determined, but there are two different ways to label the edges of the fusion tree consistently, giving a two-dimensional representation.



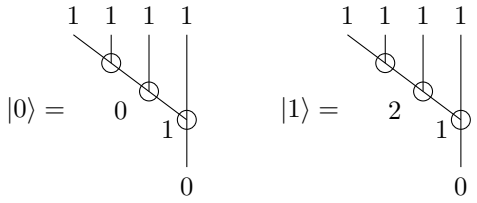
When $n = 4$, there are two distinct values of i, and for each value of i, two different ways to label the edges of the fusion tree. Therefore we get two separate two-dimensional representations.



Both of these representations are isomorphic to $\mathbb{C}^2$. The representation $\rho_{2,4,0}$ corresponding to the lefthand fusion tree is presented in the following section. The other representation $\rho_{2,4,2}$ is different, but similar, and is left to the reader as an exercise.

4.2.2. The Majorana qubit

We introduce a convenient piece of notation for fusion trees. Often we want to make the identification of certain fusion trees corresponding to a two-dimensional representation with the standard orthonormal basis vectors $|0\rangle$ and $|1\rangle$ of $\mathbb{C}^2$. To make this identification, we typically need to normalize a fusion tree. Instead of carrying around a potentially cumbersome normalization factor along with the fusion trees, we use open circles at the vertices of the fusion tree to indicate that it is normalized. The usual notation for a qubit is as a superposition of the states 0 and 1, $\alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. By identifying $|0\rangle$ and $|1\rangle$ with the fusion trees



we arrive at the famous *Majorana qubit.*

4.2.3. How the Fibonacci theory got its name

The counting arguments used above to produce the dimensions of the Jones representations of $\mathcal{B}_n$ for $k = 2$ can also be used to analyze the dimensions of the Jones representation for the Fibonacci subtheory, by considering what happens when we label the top of the fusion tree by 2's.Technically, the theory of Fibonacci anyons uses the *colored Jones representation* where instead of considering $\mathrm{Hom}(i, 1^{\otimes n})$, we replace the label 1 with another label a in $\mathcal{L} = \{0, 1, 2, \ldots, k\}$ and consider $\mathrm{Hom}(i, a^{\otimes n})$ for $a \in \mathcal{L}$. In particular, we are

looking for a basis of $\mathrm{Hom}(1, \tau^n)$, where τ is the Fibonacci anyon. This still provides a representation of the n-strand braid group, where the braids have been "colored" by τ.

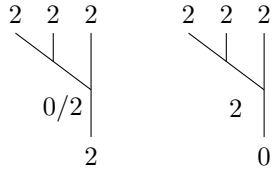
***Remark* 4.2.** It is possible to obtain the same representation through the uncolored Jones representation with the right choice of Kauffman variable A up to a character because $1 \otimes 3 = 2$.

The anyon model $\{1, \tau\}$ is called the Fibonacci theory because the Fibonacci numbers appear as the dimensions of the spaces $\mathrm{Hom}(1, \tau \otimes \cdots \otimes \tau)$. Hereafter we use the $TLJ(A)$ labels and anyon labels interchangeably.

When $n = 1$ there is one admissible fusion tree, but $i \neq 0$, and hence $\dim(V_{3,1,0}) = 0$.

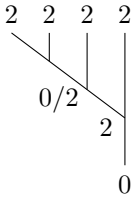
When $n = 2$, there are two ways to label a fusion tree, one of which has trivial total charge, and hence $\dim(V_{3,2,0}) = 1$.

When $n = 3$, the image splits into a one-dimensional space isomorphic to $\mathbb{C}$ and a two-dimensional space, isomorphic to $\mathbb{C}^2$.

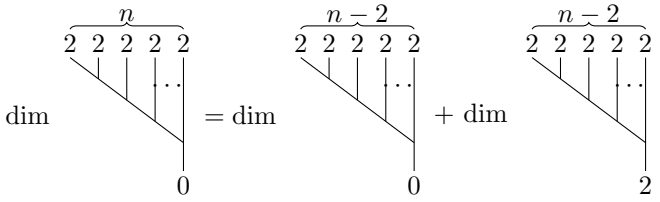


Evidently $\dim(V_{3,3,0}) = 1$.

Now if $n = 4$ and $i = 0$, we get $\dim(V_{3,4,0}) = 2$.



So far the dimensions form the sequence $0, 1, 1, 2 \ldots$, the first few Fibonacci numbers. Using the Fibonacci fusion rule $\tau \otimes \tau = 1 \oplus \tau$, we can make an observation about how the Fibonacci fusion trees are nested in one another.



This shows that the Fibonacci representation always splits into two subrepresentations as $\rho_{3,\tau^{\otimes n}} = \rho_{3,\tau^{\otimes n},1} \oplus \rho_{3,\tau^{\otimes n},\tau} : \mathcal{B}_n \to U(F_{n-1}) \oplus U(F_n)$, corresponding to the total charge 1 and total charge τ. Moreover the dimensions satisfy the recurrence relation

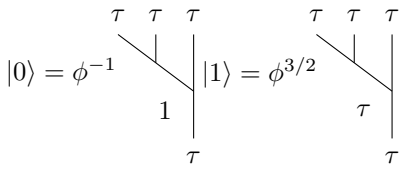
$$f_{n,0} = f_{n-2,0} + f_{n-2,2} = f_{n-2,0} + f_{n-1,0},$$

which is exactly the relation that defines the Fibonacci numbers F_n. Therefore we have that $\dim V_{3,\tau^{\otimes n},0} = F_{n-1}$. That is, the dimensions of the spaces $\mathrm{Hom}(i, \tau^{\otimes n})$ are governed by the Fibonacci numbers.

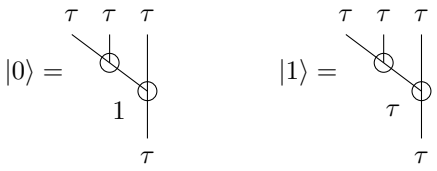
Algebraizing this fusion rule, we get the equation $x^2 = 1 + x$, whose solutions are the golden ratio ϕ and its Galois conjugate. The golden ratio also satisfies the identity $\phi = \phi^{-1} + 1$, which will be useful for calculations in the Fibonacci theory.

4.2.4. The Fibonacci qubit

To build a qubit with Fibonacci anyons, we identify

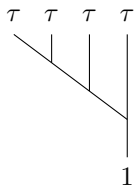


or in the new notation



4.2.5. Dense versus sparse qubit encodings

The qubit encoding above using three Fibonacci anyons is called a *dense encoding.* By raising the number of anyons, like in the two-dimensional representation



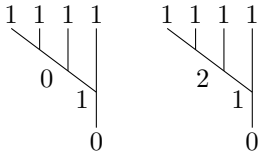
we obtain a *sparse* encoding. While the dense encoding is mathematically easier to work with, the sparse encoding is physically preferable. This is because the total charge i of an anyon system is a boundary condition, and in an experimental set up, letting the boundary condition correspond to the ground state is energetically more favorable.

Now that we have found two-dimensional representations $\rho_{2,4,0/2}$ and $\rho_{3,\tau^{\otimes 3},\tau}$, we would like to be able to compute these them explicitly and write down their matrices with respect to an orthonormal basis on the vector spaces $V_{k,n,i}$.

4.3. Computing Jones Representations and $\rho_{2,4,0}(\sigma_1)$

To illustrate a general method for computing the Jones representation of the generators σ_i of the braid group $\mathcal{B}_n$, we calculate the Jones representations $\rho_{2,4,0}(\sigma_1)$.

Recall the two fusion trees that span $V_{2,4,0}$, shown below, which we now call $\tilde{e}_0$ and $\tilde{e}_1$.

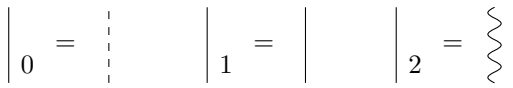


The first step is to turn these vectors into an orthonormal basis using Gram-Schmidt orthonormalization.

4.3.1. Notation

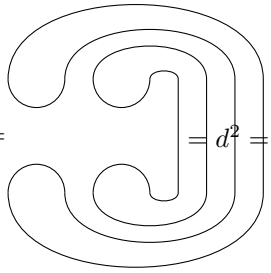
It will be convenient to introduce another notation for elements of $\mathrm{Hom}(i, 1^{\otimes n})$, in which the need to label every edge of a fusion tree is eliminated. Edges labeled by the ground state 0 become dashed edges, edges labeled by a 1 are usual lines,

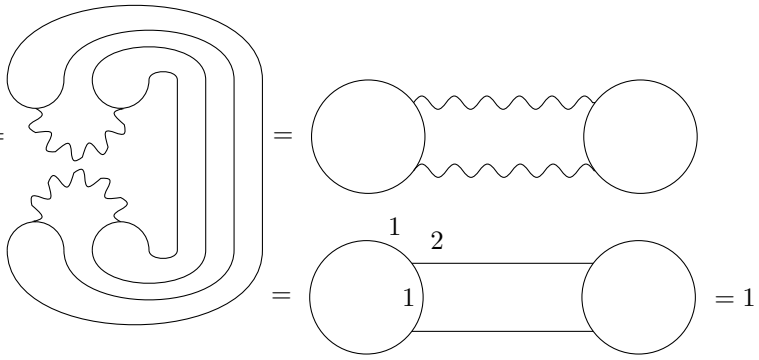
and edges labeled by a 2 become wavy lines.

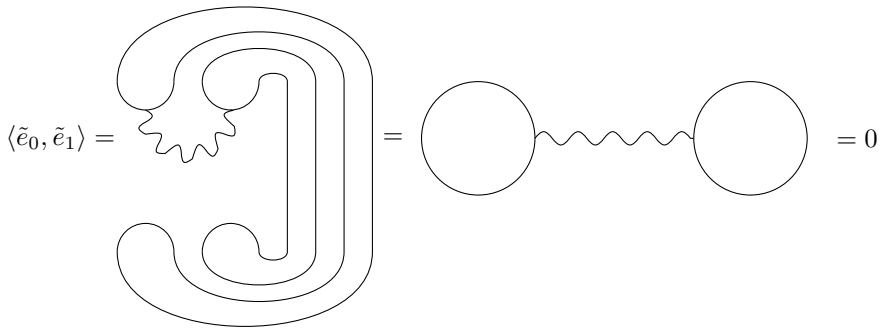


Under this new notation $\tilde{e}_0$ and $\tilde{e}_1$ become

Hereafter we will drop the dashed lines labeling the ground state. Towards applying Gram-Schmidt we find the inner products $\langle \tilde{e}_i, \tilde{e}_j \rangle$ using the graphical calculus.

$\langle \tilde{e}_0, \tilde{e}_0 \rangle =$  $= d^2 = 2$

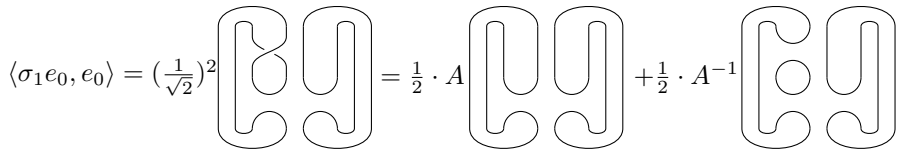
$\langle \tilde{e}_1, \tilde{e}_1 \rangle =$ 



Exercise 4.3. Verify that $\langle \tilde{e}_1, \tilde{e}_1 \rangle$=2 and $\langle \tilde{e}_0, \tilde{e}_1 \rangle = 0$ in the manner shown above, inserting the appropriate Jones-Wenzl projectors at the trivalent vertices and using the graphical calculus.

Since $\langle \tilde{e}_0, \tilde{e}_1 \rangle = 0$, the choices $e_0 = \frac{1}{\sqrt{2}}\tilde{e}_0$ and $e_1 = \tilde{e}_1$ define an orthonormal basis $\{e_0, e_1\}$ of $V_{2,4,0}$. Then with respect to this basis, $\rho(\sigma_1) = \begin{pmatrix} \langle e_0, \sigma_1 e_0 \rangle & \langle e_0, \sigma_1 e_1 \rangle \\ \langle e_1, \sigma_1 e_0 \rangle & \langle e_1, \sigma_1 e_1 \rangle \end{pmatrix}$.

For example,



$$= \tfrac{1}{2}(A \cdot d^2 + A^{-1} d^3) = -A^{-3}$$

,

where the crossings were resolved using the Kauffman bracket. Similar calculations for the remaining matrix entries show that

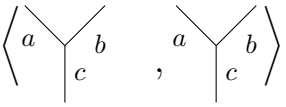
$$\rho(\sigma_1) = \begin{pmatrix} -A^{-3} & 0 \\ 0 & A \end{pmatrix}.$$

By repeating the same method to find the remaining generators $\rho(\sigma_2)$ and $\rho(\sigma_3)$, one can calculate the image $\rho_{4,2,0}(b)$ for any $b \in \mathcal{B}_4$.

This outlines an elementary way to find the Jones representation. While it has the benefit that it uses only knowledge of the Kauffman bracket and arithmetic, as n gets larger it becomes inefficient to do by hand. Additional data in $TLJ(A)$ coming from its structure as a UMC provide more tools to find $\rho_{n,k,i}$ using graphical calculus, namely the *θ-symbols*, *R-symbols*, and *F-symbols*.

4.4. θ-symbols, R-symbols, and F-symbols

Take any admissibly-labeled trivalent vertex e_c^{ab}, i.e. an element of $\mathrm{Hom}(c, a \otimes b)$. Then the θ-symbol $\theta(a, b, c)$ is defined to be the the inner product $\langle e_c^{ab}, e_c^{ab} \rangle$ of the trivalent tree vector e_c^{ab}.

$\theta(a,b,c) =$ 

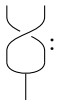
Another version of the unitary θ-symbol is related to the quantum dimensions of the charges a, b, and c via

$$\sqrt{d_a d_b d_c} = \theta_u(a, b, c).$$

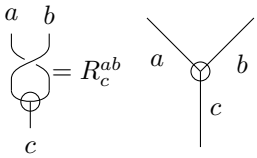
Once these symbols are determined for an anyon model they can be used to help calculate the desired braid group representation by substituting a θ-symbol whenever the inner product of two trivalent vertices appears.

4.4.1. R-symbols

Another set of symbols allows one to resolve crossings in the graphical calculus. Braiding gives a linear map

 $: \mathrm{Hom}(c, a \otimes b) \to \mathrm{Hom}(c, b \otimes a)$.

It is in fact an isomorphism, with inverse given by the opposite crossing. Since $\mathrm{Hom}(c, b \otimes a)$ is one-dimensional in TLJ theory, and we already have a preferred basis for it, namely the trivalent vertex labeled by a, b, and c, the equation

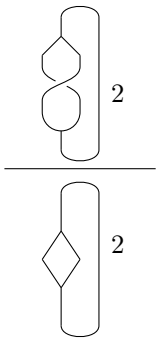


holds, where R_c^{ab} is a scalar, which we call the *braiding eigenvalue* or R-symbol. There is a general formula that gives the R-symbols, for any Kaufmann variable A and any Temperley-Lieb category, given by

$$R_c^{ab} = (-1)^{\frac{a+b-c}{2}} A^{\frac{-[a(a+2)+b(b+2)-c(c+2)]}{2}}.$$

One can also calculate the R-symbols from their defining relation by taking the inner product of both sides of the equation with the trivalent vertex labeled by

a, b, and c, which we demonstrate in the following example with R_2^{22}, where the labels "2" on the right hand side of the equation indicate that every edge in the diagram is labeled by a 2.

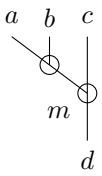
$R_2^{22} =$ 

By resolving the top diagram via the Kauffman bracket and inserting Jones-Wenzl projectors p_2 at the appropriate vertices, R_2^{22} can be calculated by hand. However, doing so efficiently requires familiarity with the graphical calculus and its shortcuts.

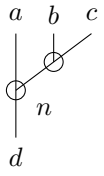
Exercise 4.4. Calculate R_2^{22} using the graphical calculus and compare with the formula.

4.4.2. F-symbols

The other hero in the theory is the F-symbols, which tells us how to make changes of basis in the fusion vector spaces. We consider the space $\mathrm{Hom}(d, (a \otimes b) \otimes c)$, with orthonormal basis given by $\{e_{d,m}^{(ab)c}\}$, where

$e_{d,m}^{(ab)c} =$ 

Similarly, we can consider the orthonormal basis $\{e_{d,n}^{a(bc)}\}$ of $\mathrm{Hom}(d, a \otimes (b \otimes c))$, where

$e_{d,n}^{a(bc)} =$ 

.

Then $F : \{e_{d,m}^{(ab)c}\} \to \{e_{d,m}^{a(bc)}\}$ is the change of basis matrix, satisfying

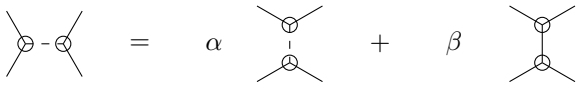
$$e_{d,m}^{(ab)c} = \sum F_{d,nm}^{abc} e_{d,n}^{a(bc)}.$$

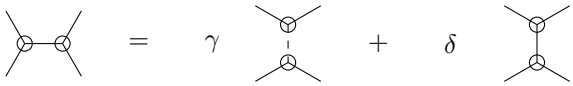
In terms of the graphical calculus, the F-symbols allow one go back and forth between different ways to associate fusion vertices. The F-symbols are notoriously hard to find, although there is a general formula. Similar to the method described in the previous section for computing the R-symbols by tracing out their defining relation, there is a way to calculate them using the graphical calculus.

For example, the two fusion trees 

and 

each give a basis for the space $\mathrm{Hom}(2 \otimes 2, 2 \otimes 2)$, where each edge that is not explicitly labeled is understood to be labeled with a 2. Therefore they satisfy the following equations.





The constants can be determined by taking the trace of each equation in two different ways: once vertically and once horizontally. That is, once connecting top and bottom edges and once connecting left and right edges. The calculations can then be simplified using the θ-symbols. The F-matrix is then given by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Exercise 4.5. Use the graphical calculus to show that the F-matrix is given by

$$\begin{pmatrix} \phi^{-1} & \phi^{-1/2} \\ \phi^{-1/2} & -\phi^{-1} \end{pmatrix}.$$

4.5. Calculating the representation $\rho_{3,\tau^{\otimes 3},\tau}$ for the Fibonacci theory

Equipped the R and F symbols, the images of Jones representations can be systematically computed using the graphical calculus.

4.5.1. The Fibonacci R and F-symbols

When $A = \pm ie^{2\pi i/10}$, using the formula $R_c^{ab} = (-1)^{\frac{a+b-c}{2}} A^{\frac{-[a(a+2)+b(b+2)-c(c+2)]}{2}}$ we find

$$R_0^{22} = A^{-8} = e^{-4\pi i/5}, R_2^{22} = -A^{-4} = -e^{-2\pi i/5}.$$

The Fibonacci F-matrix is given by

$$F = \begin{pmatrix} \phi^{-1} & \phi^{-1/2} \\ \phi^{-1/2} & -\phi^{-1} \end{pmatrix}.$$

Either of these quantities can be found using the method outlined in the previous section.

4.5.2. The Jones representation $\rho_{3,\tau^{\otimes 3},\tau}$

Given the R and F-symbols, $\rho(\sigma_1)$ and $\rho(\sigma_2)$ take the form

$$\rho(\sigma_1) = \begin{pmatrix} R_1^{\tau\tau} & 0 \\ 0 & R_\tau^{\tau\tau} \end{pmatrix}, \ \rho(\sigma_2) = F\rho(\sigma_1)F^{-1}$$

Explicitly, the generators σ_1 and σ_2 have representations

$$\rho(\sigma_1) = \begin{pmatrix} \xi^{-2} & 0 \\ 0 & -\xi^{-1} \end{pmatrix}, \ \rho(\sigma_2) = \begin{pmatrix} \phi^{-1}\xi^2 & -\phi^{-1/2}\xi \\ -\phi^{-1/2}\xi & -\phi^{-1} \end{pmatrix},$$

where $\xi = e^{2\pi i/5}$ and ϕ is the golden ratio.

Having introduced the main tools for calculating braid group representations, we turn to studying their images.

4.6. The image of the braid group representation

The basic questions that must be addressed in order to assess the utility of these representations for quantum computation are the following:

Question 4.6.

(1) Is the image $\rho_{k,n,i}(\mathcal{B}_n)$ in $U(V_{k,n,i})$ finite or infinite?

(2) If it is infinite, what is the compact Lie group $\overline{\rho_{k,n,i}(\mathcal{B}_n)}$?

The first question was answered by Jones in his seminal 1984 paper [11], and the second by Freedman, Larsen, and Wang in 2002 [8].

Theorem 4.6 (Jones)**.** *For $k \in \{1, 2, 4\}$, $\rho_{k,n,i}(\mathcal{B}_n)$ is a finite group. For other values of k and $n \geq 3$, $\rho_{n,k,i}(\mathcal{B}_n)$ is infinite, except for when $k = 8$ and $n = 4$.*

Theorem 4.7 (Freedman, Larsen, W.)**.** *When $\overline{\rho_{k,n,i}(\mathcal{B}_n)}$ is infinite, $SU(V_{k,n,i}) \subset \overline{\rho_{k,n,i}(\mathcal{B}_n)}$.*

We will see that quantum computation is performed by applying unitary matrices to quantum bits, so this result has important applications.

While we have stated very general results about the images of braid group representations whose proofs are beyond the scope of these notes, there are more elementary ways that can reproduce these results in the $k = 2$ and $k = 3$ case, to address whether the Ising and Fibonacci models can be useful for quantum computation.

4.6.1. The image of $\rho_{2,4,0}$

The following theorem characterizes the image of the Jones representation of the four-strand braid group at level 2 and trivial total charge.

Theorem 4.8.

(1) For $k = 2$, the Temperley-Lieb-Jones algebra $TLJ_n(A)$ is isomorphic to a Clifford algebra.

(2) The sequence

$$1 \to \mathbb{Z}_2^n \to \rho_{2,n,i}(\mathcal{B}_n) \to S_n \to 1$$

is exact projectively for $n \neq 3$. When $n = 3$, the sequence

$$1 \to \mathbb{Z}_2^2 \to \rho_{2,3,i}(\mathcal{B}_n) \to S_3 \to 1$$

is exact projectively. In particular, the projective image of the braid group representation $\rho_{2,3,i}$ is finite.

To prove the first part of the theorem, we'll need to know that the Majorana version of a Clifford algebra is the $\mathbb{C}$-span of vectors $\{e_1, \ldots, e_{n-1}\}$, subject to the relation $e_i e_j + e_j e_i = 2\delta_{ij}$. The $k = 2$ Temperley-Lieb-Jones algebra in terms of generators and relations is the $\mathbb{C}$-span of the diagrams $\{u_1, \ldots, u_{n-1}\}$, modulo the relation $p_3 = 0$.

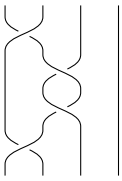
In order to show that these two algebras are isomorphic, we need a conversion between the generators e_i of the Clifford algebra and the u_i of the Temperley-Lieb-Jones algebra. Recall $\sigma_i = A + A^{-1}u_i$, and define $g_i = -A^{-1}\sigma_i = -1 - A^{-2}u_i$. Since A is an eighth root of unity when $k = 2$, $g_i^2 = 1 - du_i$. On the other hand, the e_i can be written as $e_i = (\sqrt{-1})^{i-1} g_i^2 g_{i-1}^2 \cdots g_1^2$, so that $g_i = \sqrt{-1} e_i e_{i+1}$. Then one can check that their mutual definitions with respect to the g_i agree.

The proof of the second part of the theorem can be found in [11]. We present some of the details here that are independent of the value of n.

Recall the pure braid group $P\mathcal{B}_n$, which is defined implicitly through the short exact sequence

$$1 \to P\mathcal{B}_n \to \mathcal{B}_n \to S_n \to 1,$$

and can be interpreted as a group of braid diagrams whose strands begin and end in the same position. For example, the following braid on four strands is a pure braid.



An important class of pure braids are those of the form σ_i^2 for any generator σ_i of $\mathcal{B}_n$, since certain conjugates of σ_i^2 form a generating set A_{ij} of $P\mathcal{B}_n$, where

$$A_{ij} = (\sigma_j \sigma_{j-1} \cdots \sigma_{i+1}) \sigma_i^2 (\sigma_j \sigma_{j-1} \cdots \sigma_{i+1})^{-1}, \quad i < j.$$

Then one can argue that the sequence

$$1 \to \rho(P\mathcal{B}_n) \to \rho(\mathcal{B}_n) \to \rho(S_n) \to 1$$

is also exact. This reduces the problem of showing that the image of the braid group is finite projectively (up to a scalar which is a root of unity) to the problem of showing that the image of the pure braid group is finite projectively.

The following proposition contains the relations needed in order to show the pure braid group image is finite projectively.

Proposition 4.9. *Let g_i be defined as above.*

(1) $g_i^2 g_{i+1}^2 + g_{i+1}^2 g_i^2 = 0$

(2) $g_i g_{i\pm1}^2 g_i^{-1} = i g_i^2 g_{i\pm1}^2$

The proof of this proposition is an exercise for the reader in the graphical calculus.

The first part of Proposition 4.9 tells us that the g_i^2's commute up to an overall minus sign, and furthermore we can deduce that $g_i^{16} = 1$. Then it follows from the second part of the proposition that the projective image of the pure braid group is generated by g_i^2.

Thus when $k = 2$ the Jones representation of the braid group has finite projective image.

The physical consequence of 4.8 is the following result, the proof of which requires some familiarity with the mathematical formalism of quantum computation, which is discussed in the next subsection.

Corollary 4.10. *The Ising theory cannot be used for universal quantum computation by braiding alone.*

This means that the set of quantum gates that come from the matrix representations $\rho_{2,n,i}$ of the braiding of the anyons $\{1, \sigma, \psi\}$ of the Ising model is not powerful enough to build a universal quantum computer. In order to prove this corollary, one needs to know about the mathematical formalism of quantum computation, which will be discussed shortly.

One the other hand, all of $SU(2)$ is contained in $\overline{\rho_{3,\tau^{\otimes 3},i}(\mathcal{B}_3)}$.

4.6.2. The image of $\rho_{3,\tau^{\otimes 3},\tau}$

The following theorem characterizes the closed images of $\rho_{3,\tau^{\otimes 3},i}$ in $U(V_{3,\tau^{\otimes 3},i})$.

Theorem 4.11. $\overline{\rho_{3,\tau^{\otimes 3},i}(\mathcal{B}_n)} \supset SU(V_{3,\tau^{\otimes 3},i})$.

4.6.3. Proof of the theorem

We begin by showing that the image is infinite. Of course, it suffices to demonstrate the existence of an element in the image which is of infinite order.

Recall that the generators σ_1 and σ_2 have representations

$$\rho(\sigma_1) = \begin{pmatrix} \xi^{-2} & 0 \\ 0 & -\xi^{-1} \end{pmatrix} \text{ and } \rho(\sigma_2) = \begin{pmatrix} \phi^{-1}\xi^2 & -\phi^{-1/2}\xi \\ -\phi^{-1/2}\xi & -\phi^{-1} \end{pmatrix} = F\sigma_1 F,$$

where ϕ is the golden ratio and $\xi = e^{2\pi i/5}$. Since the matrix representation of σ_1 is diagonal, it is easy to see that its order is just the least common multiple of the orders of the roots of unity appearing on the diagonal, and hence σ_1 has order 10. Since all elements of the braid group are in the same conjugacy class, it follows that σ_2 has order 10 as well.

Consider $\sigma_1^m\sigma_2$, where $\sigma_1^{10} = 1$ and $m = 1, 2, \ldots, 9$. We claim that when $m = 4$ and $m = 9$, both elements $\sigma_1^m\sigma_2$ are of infinite order, and moreover, they don't commute. To see that they do not commute, suppose

$$(\sigma_1^4\sigma_2)(\sigma_1^9\sigma_2) = (\sigma_1^9\sigma_2)(\sigma_1^4\sigma_2).$$

Then using that σ_1 has order ten, it follows that

$$\sigma_1^4\sigma_2\sigma_1^{-1}\sigma_2 = \sigma_1^{-1}\sigma_2\sigma_1^4\sigma_2$$

and hence

$$\sigma_1^5\sigma_2 = \sigma_2\sigma_1^5.$$

But one can check using the definitions of σ_1 and σ_2 that this is not the case.

To prove that $\sigma_1^4\sigma_2$ and $\sigma_1^9\sigma_2$ are of infinite order, we use established results about when small sums of roots of unity vanish [4]. Suppose $\sigma_1^4\sigma_2$ is of finite order, then there will be two roots of unity $\lambda_i, i = 1, 2$ such that $\mathrm{Tr}(\sigma_1^4\sigma_2) =$

$\lambda_1 + \lambda_2$ and $\lambda_1\lambda_2 = \det(\sigma_1^4\sigma_2) = \xi$. The trace $\mathrm{Tr}(\sigma_1^4\sigma_2)$ can be written as an integral identity of ξ and λ_1. But this possibility is not among such sums as classified in [4]. Similarly, we can show $\sigma_1^9\sigma_2$ is of infinite order. Putting $g_1 = \sigma_1^4\sigma_2$ and $g_2 = \sigma_1^9\sigma_2$, this shows that $\overline{\{g_1^m\}} = SO(2)$ and $\overline{\{g_2^m\}} = SO(2)$ both inject into $SU(2)$, proving the theorem.

The physical corollary of this mathematical result is that $\{\rho(\sigma_1), \rho(\sigma_2)\}$ is a universal gate set for a single qubit.

Corollary 4.12. *Braiding Fibonacci anyons is enough to get any single qubit quantum gate.*

But what about n-qubit gates from this representation? In general, one would need n-qubit space $(\mathbb{C}^2)^{\otimes n}$ to be contained in $\mathrm{Hom}(3, \tau^{\otimes n}, 1)$. However, we will see that it is enough to get all two-qubit gates.

In the next section we provide the background necessary to assess the power of the images of the Jones representations as quantum gates and prove the two physical corollaries stated in this section for the Ising and Fibonacci theories.

4.7. Quantum gates and universal quantum computation

Classically, a decision problem is the following: given a sequence of functions $\{f_n\} : \mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ on n-bit strings, compute $f_n(x)$ for all $x \in \mathbb{Z}_2^n$. "Quantizing" this set up, we have a quantum decision problem - given a sequence of $\{f_n\}$ on $\mathbb{C}[\mathbb{Z}_2^n] \cong (\mathbb{C}^2)^{\otimes n}$, the space of n-qubits, find a unitary matrix U such that $U|x\rangle = |f_n(x)\rangle$. Such matrices are written with respect to the *computational basis* $\mathbb{Z}_2^n$ of $(\mathbb{C}^2)^{\otimes n}$.

We are always concerned with *efficient approximation* when performing computation. The correct notion of efficiency is that U should be a composition of gates, of polynomial length in n, the number of qubits.

The building blocks of which such a U is composed are elements of a small *gate set*, say, $S = \{g_1, \ldots, g_m\}$, where each g_i is a 2×2 or 4×4 unitary matrix, i.e. each acts on a one qubit ($\mathbb{C}^2$) or two-qubit ($\mathbb{C}^2 \otimes \mathbb{C}^2$) subspace of $(\mathbb{C}^2)^{\otimes n}$. These gate sets, while acting on a few qubits at a time, are extended trivially on the remaining qubits by tensoring with the identity. A gate set is said to be *universal* if we can build any unitary matrix to arbitrary accuracy with a finite number of elements of our gate set. More precisely, if we consider the set of all quantum circuits on $(\mathbb{C}^2)^{\otimes n}$ that can be built from our gate set, then it is universal if it is dense in $SU(2^n)$. (Recall that we are interested in things up to a phase.) The rest of this section is devoted to demonstrating that single and double-qubit operators are enough to get universal quantum computation.

4.7.1. Single-qubit gates

Some of the most foundational results in quantum computation are the following theorems concerning the gates

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix},\ \text{and } CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}.$$

Theorem 4.13. *The gate set $\{H, T, CNOT\}$ consisting of the Hadamard, $\frac{\pi}{8}$ phase-shift, and controlled-not gates is universal for quantum computation.*

The first two gates in the set are enough to generate all single-qubit operations.

Theorem 4.14. *Let G be the set of all compositions of H and T. Then $\overline{G} \supset SU(2)$.*

Therefore, if the Hadamard and $\frac{\pi}{8}$ matrices can either be realized exactly or efficiently approximated by matrices coming from the images of Jones representations, then the corresponding anyon model is sufficient to perform any single-qubit computation.

Of course, it is preferable to realize gates exactly rather than to approximate them.

Question 4.16. Which matrices in $U(2)$ can be realized exactly by a braid up to an overall phase?

The following theorem is an answer to this question for $\mathcal{B}_3$ in the Fibonacci theory [14].

Theorem 4.15. *Let $\omega = e^{2\pi i/10}$ and let $u, v \in \mathbb{Z}[\omega]$ satisfying $|u|^2 + \frac{|v|^2}{\phi} = 1$. Then any matrix of the form*

$$M = \begin{pmatrix} u & \bar{v}\phi^{1/2}\\ v\phi^{-1/2} & -\bar{u}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \omega^k\end{pmatrix}$$

can be realized exactly by a braid in $\mathcal{B}_3$ in the Fibonacci theory.

If in addition to single-qubit operations an *entangling* gate like $CNOT$ can be realized, then the anyon model can be used to build a universal quantum computer.

4.7.2. Two-qubit gates and entanglement

The notion of entanglement is key to understanding universality.

Definition 4.16. A gate g in $U(4)$ is not entangling if either $g = A \otimes B$ or SWAP $g = A \otimes B$, where $A, B \in U(2)$ and SWAP $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. If a gate is not of this form, then it is called entangling.

The simplest example of an entangling gate is the CNOT gate. To show that CNOT is entangling, we must prove that neither CNOT nor SWAP CNOT can be written as a tensor product $A \otimes B$, for any $A, B \in U(2)$. Recall that the CNOT has the following matrix with respect to the computational basis.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

If a matrix M can be written $M = M_1 \otimes M_2$, where M_1 has eigenvalues λ_i and M_2 has eigenvalues μ_j, then the eigenvalues of M are of the form $\lambda_i \mu_j$. CNOT has eigenvalues $1, 1, 1, -1$. So if there were matrices A and B with eigenvalues λ_1, λ_2 and μ_1, μ_2 respectively, then they would have to satisfy the system of equations

$$\begin{cases} \lambda_1 \mu_1 = 1 \\ \lambda_1 \mu_2 = 1 \\ \lambda_2 \mu_1 = 1 \\ \lambda_2 \mu_2 = -1 \end{cases}.$$

But $\det \lambda_{ij} = 0$, so this cannot happen. The same argument applies to show that SWAP CNOT cannot be written as a tensor product. Therefore the CNOT gate is entangling.

Any four-by-four unitary matrix, that is, any two-qubit quantum gate, can be written as a tensor product of single-qubit gates and an entangling gate, as the following theorem states.

Theorem 4.17. *Given any entangling gate E, any matrix in $U(4)$ can be written as a finite product of some number of E's and matrices in $U(2)$ up to an overall phase.*

This takes care of two-qubit gates. To be able to construct n-qubit gates from one and two-qubit gates we need the following definition.

Definition 4.18. A matrix is 2-level if it is not the identity only on a 2-dimensional subspace.

An important example of a 2-level matrix for our purposes is of the kind

$$\left(\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & 0 \\ \hline & 0 & U \end{array}\right),$$

where $U \in U(2)$.

The following lemma collects the facts that allow local unitary computation.

Lemma 4.19. *Every unitary matrix M is a product of 2-level unitary matrices. Every 2-level matrix can be realized as a product of 1-qubit gates and CNOTs.*

The results we have collected thus far imply the following theorem.

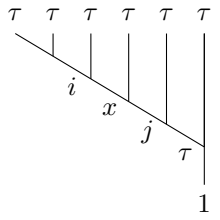
Theorem 4.20. *The CNOT gate, together with SU(2) forms a universal gate set. That is, if $U \in SU(2^n)$, then U can be written as a tensor product of CNOT gates and 2×2 unitary matrices.*

All of the linear algebra is now in place to understand what is needed for a small gate set to be universal.

4.8. Ising and Fibonacci quantum computers

Since the image of $\rho_{2,4,0}$ is finite in $U(2)$, we can't get a universal gate set from the Ising theory. On the other hand, we have shown that the closure of the image of $\rho_{3,\tau^{\otimes 3},\tau}$ contains $SU(2)$, and hence can produce any single-qubit gate. Moreover, the image of $\rho_{3,\tau^{\otimes 6},1} : \mathcal{B}_6 \to U(5)$ can be used to approximate an entangling gate, as implied by the theorem below.

In the dense encoding, we choose the two-qubit computation subspace in $V_{3,\tau^{\otimes 6},1}$ as indicated by the fusion tree below.



$V_{3,\tau^{\otimes 6},1}$ is 5-dimensional. When $x = 1$, there is only one admissible labeling, so it spans a one-dimensional subspace of $V_{3,\tau^{\otimes 6},1}$. We will not use this subspace for computation, so it will be called a non-computational subspace. When

$x = \tau$, then all choices of $i, j \in \{1, \tau\}$ are admissible, so we obtain a natural two-qubit subspace of $V_{3,\tau^{\otimes 6},1}$. We will denote the 4 basis elements as $\{e_{ij}\}$. Ideally, we would like to find an entangling braid $b \in \mathcal{B}_6$ on $V_{3,\tau^{\otimes 6},1}$ so that the resulting matrix $\rho(b)$ is the identity on the non-computational subspace and an entangling gate on the two-qubit subspace. But we do not know the existence of such braiding gates. It would be extremely interesting to know if such "no leakage" entangling braiding gates exist or not. But in practice, we will use the following density theorem to find entangling braiding gates with arbitrarily small leakage to the non-computational subspace.

Theorem 4.21.

(1) $SU(5) \subset \overline{\rho_{3,\tau^{\otimes 6},1}(\mathcal{B}_6)}$.

(2) Any matrix in $SU(4)$ *can be approximated to any precision by the gate set* $\{\rho(\sigma_i), i = 1, ..., 5\}$ *on the computational subspace* $\mathbb{C}[\{e_{ij}\}], i, j \in \{1, \tau\}$.

The proof of this theorem is not elementary so we omit the details. Presumably we can use an inductive argument using irreducibility and density of one-qubit gates Thm. 4.11. Therefore a universal gate set can be built from braiding Fibonacci anyons, proving Theorem 1.1 for $r = 5$.

Open problem 4.24. Is there a two-qubit entangling gate that can be realized by braiding exactly in the Fibonacci theory?

4.9. General TLJ theory for quantum computing

In earlier sections, we explain Ising and Fibonacci theories. In general any TLJ theory can be used for anyonic quantum computation.

The Jones-Kauffman theory at level $k = r - 2 \geq 1$ is the TQFT associated to the TLJ theory with the choice of

$$A = \begin{cases} ie^{-2\pi i/4r} & k \equiv 0 \mod 2 \\ ie^{2\pi i/4} & k \equiv 1 \mod 2 \text{ and } k \equiv 1 \mod 4 \\ -ie^{-2\pi i/4} & k \equiv 1 \mod 2 \text{ and } k \equiv -1 \mod 4. \end{cases}$$

When k is even, the TLJ category is a unitary modular category modeling anyons, while when k is odd, it is a unitary pre-modular category modeling fermions. This generalizes the Ising and Fibonacci theories.

5. Approximation of The Jones polynomial

Recall that unlike the Alexander polynomial, for which their exists a polynomial time algorithm, computing the Jones polynomial is hard. The classical complexity of computing the Jones polynomial exactly at roots of unity is summarized in the following theorem [22, 9].

Theorem. *For $r \neq 1,2,3,4,6$, computing the Jones evaluations $J(L, e^{2\pi i/r})$ exactly is #P hard. Moreover, the Jones evaluations $\{J(L, e^{2\pi i/r})\}$ for all links L at $r \neq 1,2,3,4,6$ is dense in $\mathbb{C}$.*

However, the Jones evaluations at roots of unity could be efficiently approximated by a quantum computer. In this section we discuss an algorithm for such an approximation which is a consequence of the efficient simulation of TQFTs with several clarifications [7]. Our approximation goes through the Jones representations of the braid group, necessitating a choice of a braid closure to turn braids into links. For our algorithm, we use the plat closure of braids with an even number of strands. It was observed that if instead the braid closure is used, the approximation is potentially easier [13]. Approximations have variations [15], and our approximation is an additive one. Strictly speaking, we approximate the normalized Jones evaluations: $J(L, e^{\pm 2\pi i/r})$ divided by d^n. For the plat closures of braids $b \in \mathcal{B}_{2n}$, the unlink of n-components has the largest absolute value d^n. It is known that the distributions of Jones evaluations $J(L, e^{\pm 2\pi i/r})$ for $r \neq 1,2,3,4,6$ are limiting to a Gaussian as $n \to \infty$ [9]. Hence, a Jones evaluation is typically small. Our BQP-complete theorem for an additive approximation with an error scaling as the inverse of a polynomial in n the number of strands and m the braid length, implies that the normalized Jones evaluation cannot be always exponentially small because otherwise, we could just set the approximation to be 0.

Recall that the Jones evaluation $J(L, e^{\pm 2\pi i/r})$ is a map from the set of oriented links to $\mathbb{Z}[q^{\pm 1/2}]$ for $q = e^{\pm 2\pi i/r}$. In order to turn the evaluation at roots of unity into a computation problem, we must encode a link L and the Jones evaluation $J(L, e^{\pm 2\pi i/r})$ as bit strings, whereupon it becomes a Boolean map $\mathbb{Z}_2^n \to \mathbb{Z}_2^{m(n)}$, that sends the bit strings encoding of the input L to the bit strings encoding of the output $J(L; e^{\pm 2\pi i/r})$.

How does one turn a link into a bit string? First one presents L as the plat-closure of some braid, say $L = \widehat{\sigma_{i_k}^{s_k} \cdots \sigma_{i_1}^{s_1}}$. Then the integers $\{i_j\}$ and $\{s_j\}$ can be written in terms of their binary expansions and finally converted into bit strings.

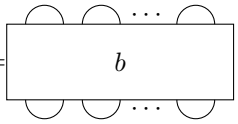
As for encoding $J(L, e^{\pm 2\pi i/r})$ as a bit string, one can use the binary expansions of its real and imaginary parts. In general these binary expansions will be infinitely long. In our algorithm we are going to approximate the evaluations. Therefore, once we are given the error ϵ, we can decide where to truncate the infinite bit strings.

The following table organizes the known complexity results concerning the computation and approximation of the Jones polynomial at roots of unity of order $r \neq 1,2,3,4,6$ [22, 15, 7, 8].

	Exactly	Approximately
Classically	#P	No FPRAS
Quantum mechanically	?	BQP-complete

5.1. Approximating Jones evaluations by a quantum computer

How is the Jones polynomial of a link L evaluated by an anyonic quantum computer at a root of unity? Suppose $b \in \mathcal{B}_{2n}$ is a braid whose closure gives the link L. Physically, a "cup" state is prepared by creating n pairs of anyons from the vacuum. Then the anyons are braided by b. Then measurement is performed by projecting onto a "cap state". This computes $|\langle \text{ cap } |\rho(b)| \text{ cup } \rangle|^2$, which recovers the normalized Jones evaluations. The figure below illustrates the process, which corresponds to the mathematical operation of taking the plat closure of b.

$\langle \text{ cap } |\rho(b)| \text{ cup } \rangle =$ 

Classically, this computation is hard, as one might expect given the exponential size of $\rho(b)$. However, there exists an efficient quantum algorithm to approximate the evaluations of the Jones polynomial [7], cf. Theorem 1.2. Precisely, we have:

Theorem 5.1. *Let $q = e^{\pm 2\pi i/r}$, $d = 2\cos\pi/r$,$\hat{\sigma}^P$ the plat closure of $\sigma \in \mathcal{B}_{2n}$, and $J(\hat{\sigma}^P, q) : \bigsqcup_{n=1}^{\infty} \mathcal{B}_{2n} \to \mathbb{Z}[q^{\pm 1/2}]$ the Jones evaluation. Given $m = |\sigma|$, n, there exists a quantum circuit of size polynomial in n, m and $1/\epsilon = poly(n, m)$ such that U_L outputs a random variable $Z(\sigma)$, where $0 \leq Z(\sigma) \leq 1$, and*

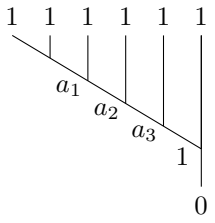
$$\left| \frac{|J(\hat{\sigma}^P, q)|^2}{d^n} - Z(\sigma) \right| < \epsilon.$$

Such an approximation is called an "additive" scheme. The full details of the proof are not provided here and can be found in [23, 1]. We will simply illustrate the main steps and ideas.

5.2. Encoding basis vectors as bit strings

For an illustration of this step, that of converting basis vectors into bit strings, we consider the case $k = 3$ and the six-strand braid group $\mathcal{B}_6$. Given the fusion

tree in $\mathrm{Hom}(0, 1^{\otimes 6})$, we attach a qubit at each vertex with basis $|i_1 i_2 i_3 i_4\rangle$,



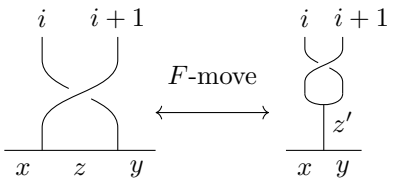
where $i_j \in \{0, 1\}$ and $a_j \in \{0, 2\}$. If $a_j = 0$, we take $i_j = 0$, and if $a_j = 2$, then we take $i_j = 1$. Then we can define the map $a_1 a_2 a_3 \mapsto |i_1 i_2 i_3 i_4\rangle$. This gives an efficient embedding of a basis of $V_{3,6,0}$ into bit strings.

5.3. Simulating the Jones representation

When we use anyons for quantum computation, we choose a computational subspace $(\mathbb{C}^2)^{\otimes l}$ in $V_{k,1^{\otimes m},0}$. Now for the simulation of the Jones representation $V_{k,m,0}$, we seek a quantum circuit U which makes the following diagram commute. By turning basis into bit strings, $V_{k,m,0}$ is embedded as a subspace in $(\mathbb{C}^2)^{\otimes(m-2)}$. The Jones representation of $\mathcal{B}_m$ is extended to $(\mathbb{C}^2)^{\otimes(m-2)}$ by the identity on the orthonormal complement of embedded $V_{k,m,0}$.

$$\begin{array}{ccccc} (\mathbb{C}^2)^{\otimes l} & \hookrightarrow & V_{k,1^{\otimes m},0} & \hookrightarrow & (\mathbb{C}^2)^{\otimes(m-2)} \\ & & \downarrow{\scriptstyle \rho(\sigma)} & & \downarrow{\scriptstyle U} \\ & & V_{k,1^{\otimes m},0} & \hookrightarrow & (\mathbb{C}^2)^{\otimes(m-2)} \end{array}$$

We must compute the braid group action on the basis of $V_{k,m,0}$. By thinking about how the braid group generators act on $V_{k,m,0}$, we are led to pieces of fusion trees like the ones below, those diagrams now being drawn horizontally.



The diagram on the left can be changed to the form on the right via an F-move, and then the braiding can be removed using an R-symbol. In this manner, by stacking the braid group generators on a basis element of $V_{k,1^{\otimes m},0}$ and then using the graphical calculus to resolve it into a linear combination of our computational basis elements, the Jones representation can be calculated for

any n. The important observation is that the extended Jones representation is now local: the 2-level matrix in the definition of the Jones representation acts now on only two qubits. In physical terms, since everything is localized, we only need to concern ourselves with two qubits at a time.

Finally, due to the fusion rules for basis elements of $V_{k,1^{\otimes m},0}$, the Jones representation is a composition of a sequence of multi-qubit controlled 2-qubit gates on $(\mathbb{C}^2)^{\otimes(m-2)}$. Such controlled gates can be implemented efficiently on a quantum computer using a few ancillary qubits. Therefore, we can approximate the Jones evaluations efficiently by a quantum computer.

6. Localization of braid group representations

The quantum circuit model is explicitly local: the n-qubit spaces are tensor powers $(\mathbb{C}^2)^{\otimes n}$ and the n-qubit circuits are composed of gates (e.g. promotions of SWAP, CNOT) that act nontrivially on just a few adjacent qubit spaces.

In contrast, the topological model relies upon gates that are not explicitly local, coming from representations of the braid group. So far we have met several families of $\mathcal{B}_n$ representations: the local representations ρ^R associated with an R-matrix, the Burau representations ρ and their reduced versions $\tilde{\rho}$ and the Jones representations (generic and specialized). In subsection 4.6.2 we gave a detailed version of Theorem 1.1, which is the main result of [8]. Consequently, the quantum circuit model (hence a quantum Turing machine) can be efficiently simulated on a topological quantum computer via certain level k Jones representations of the braid group.

The main theorem (i.e. Theorem 1.2) of [7] is a partial converse: the specialized Jones polynomial can be efficiently approximated on the quantum circuit model (cf. Section 5). This is achieved by exploiting a *hidden locality* in topological quantum field theory, which we now outline. Recall from Subsection 4.1.3 that the labels for the Temperley-Lieb-Jones category at level k are $\mathcal{L} := \{0, \ldots, k\}$. The $\mathcal{B}_n$ representation obtained from the standard faithful $TL_n(A)$-module is $\mathcal{H} := \bigoplus_j \mathrm{Hom}(j, 1^{\otimes n})$. Here each direct summand $\mathcal{H}_j = \mathrm{Hom}(j, 1^{\otimes n})$ is an irreducible $\mathcal{B}_n$ representation associated with a disk with n interior points marked with the anyon type 1 and the boundary labelled j. Now we decompose our n-punctured disks into $n-1$ pairs of pants by making $n-2$ concentric circular cuts for each boundary label j. The gluing and disjoint union axioms then show that

$$\mathcal{H} = \bigoplus_{(i_1,\ldots,i_{n-1})\in\mathcal{L}^{n-1}} \mathrm{Hom}(1^{\otimes 2}, i_1) \otimes \mathrm{Hom}(1 \otimes i_1, i_2) \otimes \cdots \otimes \mathrm{Hom}(1 \otimes i_{n-2}, i_{n-1}).$$

Here the boundary label is $j = i_{n-1}$. Now we set $V = \bigoplus_{(a,b,c)} \mathrm{Hom}(a \otimes b, c)$ and distribute $\otimes$ over $\oplus$ to realize $\mathcal{H}$ inside $V^{\otimes(n-1)}$. The complement $\mathcal{H}^{\perp}$ of $\mathcal{H}$ inside $V^{\otimes(n-1)}$ does not typically admit a braid group action. Alternatively we can be slightly more efficient and take $U = \bigoplus_{(b,c)} \mathrm{Hom}(1 \otimes b, c)$. The upshot is

that the specialized Jones representations of $\mathcal{B}_n$ can be realized inside a vector space of the form $V^{\otimes f(n)}$, but with $\mathcal{B}_n$ only acting on a certain *hidden* subspace. One may employ the same technique for the Fibonacci representations.

Exercise 6.1. Set $k = 2$ and show that $\dim(V) = 10$, while $\dim(U) = 4$. Observe that for the $\mathcal{B}_3$ representation we have $\dim(V_{3,1}) = 2$, where $V_{3,1}$ is embedded into either $V^{\otimes 2}$ or $U^{\otimes 2}$, and so has a very large complement.

This gross inefficiency motivates the following:

Question 6.2. When can a family of $\mathcal{B}_n$ representations be realized locally (uniformly for all n, and "on the nose")?

Eventually we will restrict to unitary representations, but first we must make sense of what sort of families we are interested in.

6.1. Sequences of $\mathcal{B}_n$ Representations

Notice that we have natural injective group homomorphisms $\iota : \mathcal{B}_n \to \mathcal{B}_{n+1}$ given by $\iota(\sigma_i) = \sigma_i$, for $1 \leq i \leq n-1$ allowing us to identify $\mathcal{B}_n$ as a subgroup of $\mathcal{B}_{n+1}$[3]. Which families of representations respect these identifications? For precision's sake we phrase the following in terms of group algebras [20]:

Definition 6.2. An indexed family of complex $\mathcal{B}_n$-representations (ρ_n, V_n) is a *sequence of braid representations* if there exist injective algebra homomorphisms $\varphi_n : \mathbb{C}\rho_n(\mathcal{B}_n) \to \mathbb{C}\rho_{n+1}(\mathcal{B}_{n+1})$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C}\mathcal{B}_n & \xrightarrow{\rho_n} & \mathbb{C}\rho_n(\mathcal{B}_n) \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \varphi_n} \\ \mathbb{C}\mathcal{B}_{n+1} & \xrightarrow{\rho_{n+1}} & \mathbb{C}\rho_{n+1}(\mathcal{B}_{n+1}) \end{array}$$

Example. If R is a solution to the Yang-Baxter equation on a vector space V, then it is easy to see that $\rho_n : \mathbb{C}\mathcal{B}_n \to \mathrm{End}(V^{\otimes n})$ given by $\rho_n(\sigma_i) = I_V^{\otimes i-1} \otimes R \otimes I_V^{\otimes n-i-1}$ is a sequence of braid representations: take $\varphi_n : \mathrm{End}(V^{\otimes n}) \to \mathrm{End}(V^{\otimes n+1})$ to be $\varphi_n(f) = f \otimes I_V$.

The Jones representations (specialized or not) and the (related) Fibonacci representations $\rho_{n,\tau}$ are sequences in this sense. For example, for the generic Jones representation we have $\mathbb{C}\rho_n(\mathcal{B}_n) = TL_n(A)$ and $\mathbb{C}\rho_{n+1}(\mathcal{B}_{n+1}) = TL_{n+1}(A)$. Letting $\varphi_n(u_i) = u_i$ we see that the appropriate diagram commutes.

Example. The Burau (reduced or unreduced) representations do not form a sequence of $\mathcal{B}_n$ representations in our sense. Indeed in the case where $\tilde{\rho}$ is

[3]Of course there are many less natural injective homomorphisms, for example $\sigma_i \mapsto (\sigma_{n-i+1})^{-1}$ can be verified as an injective homomorphism.

irreducible, we have $\mathbb{C}\tilde{\rho}(\mathcal{B}_n) \cong M_{n-1}(\mathbb{C})$ (for all n). Since there are no injective homomorphisms from $M_{n-1}(\mathbb{C})$ to $M_n(\mathbb{C})$, the required map φ_n does not exist.

Exercise 6.3. Show that the standard permutation representations of S_n, lifted to $\mathcal{B}_n$ in the obvious way via $(i\ i+1) \mapsto \sigma_i$ is not a sequence in our sense.

Now we can describe what we mean by a *localization* of a sequence of braid group representations.

Definition 6.4. Suppose (ρ_n, V_n) is a sequence of braid representations. A *localization* of (ρ_n, V_n) is a braided vector space (W, R) with $R \in \mathrm{U}(W^{\otimes 2})$ such that for all $n \geq 2$ there exist injective algebra homomorphisms $\psi_n : \mathbb{C}\rho(\mathcal{B}_n) \to \mathrm{End}(W^{\otimes n})$ satisfying $\psi_n \circ \rho(b) = \rho_R(b)$ for $b \in \mathcal{B}_n$.

This definition may seem a bit complicated at first, but encapsulates the notion of "on the nose" local realizations of a sequence of $\mathcal{B}_n$ representations. From the point of view of quantum computation, we are trying to discover when the singleton gate set $\{R\}$ can simulate all braiding gates. In spite of the slightly mystifying definition, the idea is quite simple: we want to find a single solution to the Yang-Baxter equation R on a vector space W so that

(1) For each n, (ρ_n, V_n) is a sub-representation of $(\rho_R, W^{\otimes n})$. Notice that we distinguish between equivalent irreducible sub-representations of V_n: if ℓ isomorphic copies of some fixed irreducible U appears in V_n then $W^{\otimes n}$ must contain at least ℓ copies of U. This is a distinction at the level of algebras: $\mathbb{C}^2$ is not a faithful representation of $M_2(\mathbb{C}) \oplus M_2(\mathbb{C})$, but $\mathbb{C}^2 \oplus \mathbb{C}^2$ is.

(2) There are no irreducible $\mathcal{B}_n$-subrepresentations of $W^{\otimes n}$ that do not appear in V_n. Whereas the hidden locality of [7] has a large non-computational space upon which the braid group does not act, we are asking that there is no such axillary space.

Comparing with the property **F** conjecture, we obtain:

Conjeture 6.6. Suppose (V, R) is a unitary solution to the YBE such that R has finite (projective) order, with corresponding $\mathcal{B}_n$-representations $(\rho_R, V^{\otimes n})$. Then $\rho_R(\mathcal{B}_n)$ is a finite group (projectively).

If the words *unitary* or *finite order* are omitted Conjecture 6.1(a) is false, see [20] for examples.

6.2. Non-localizable representations

In the braided fusion category setting Conjecture 6.1 is closely related to another fairly recent conjecture (see [19, Conjecture 6.6]). Braided fusion categories are naturally divided into two classes according to the algebraic complexity of their fusion rules. In detail, one defines the *Frobenius-Perron dimension* $\mathrm{FPdim}(X)$ of an object X in a fusion category $\mathcal{C}$ to be the largest

eigenvalue of the fusion matrix N_X corresponding to tensoring with X on the left. If $\mathrm{FPdim}(X_i) \in \mathbb{N}$ for all simple X_i then one says $\mathcal{C}$ is *integral* while if $\mathrm{FPdim}(X_i)^2 \in \mathbb{N}$ for all simple X_i then $\mathcal{C}$ is said to be *weakly integral*. An object X in a braided fusion category $\mathcal{C}$ is said to have *property* $\boldsymbol{F}$ if the $\mathcal{B}_n$-representations on $\mathrm{End}(X^{\otimes n})$ have finite image for all n. Then a version of Conjecture 6.6 of [19] states: *an object X has property $\boldsymbol{F}$ if, and only if,* $\mathrm{FPdim}(X)^2 \in \mathbb{N}$. Some recent progress towards this conjecture can be found in [18, 21] and further evidence can be found in [17, 16]. Combining with Conjecture 6.1 we make the following:

Conjeture 6.7. Let X be a simple object in a braided fusion category $\mathcal{C}$. The representations $(\rho_X, \mathrm{End}(X^{\otimes n}))$ are localizable if, and only if, $\mathrm{FPdim}(X)^2 \in \mathbb{N}$.

The main result of this section is to indicate that the specialized Jones representations are not localizable unless $r = 1, 2, 3, 4$ or 6. That is, the sequence of representations coming from the Temperley-Lieb algebras at all other roots of unity are not localizable. In the next section we will show the converse for $r = 4$ and $r = 6$, with the other cases being trivial since the corresponding categories are pointed (and hence the representations are 1-dimensional).

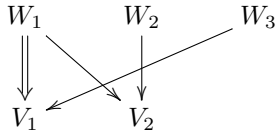
To any sequence of multi-matrix algebras $\mathcal{S} := \mathbb{C} = A_1 \subset \cdots \subset A_j \subset A_{j+1} \subset \cdots$ with the same identity one associates the *Bratteli diagram* which encodes the combinatorial structure of the inclusions. The Bratteli diagram for a pair $M \subset N$ of multi-matrix algebras is a bipartite digraph Γ encoding the decomposition of the simple N-modules into simple M-modules, and the inclusion matrix G is the adjacency matrix of Γ. More precisely, if $N \cong \bigoplus_{j=1}^{t} \mathrm{End}(V_j)$ and $M \cong \bigoplus_{i=1}^{s} \mathrm{End}(W_i)$ the inclusion matrix G is an $s \times t$ integer matrix with entries:

$$G_{i,j} = \dim \mathrm{Hom}_M(\mathrm{Res}^N_M V_j, W_i)$$

i.e. the multiplicity of W_i in the restriction of V_j to M. For an example, denote by $M_n(\mathbb{C})$ the $n \times n$ matrices over $\mathbb{C}$ and let $N = M_4(\mathbb{C}) \oplus M_2(\mathbb{C})$ and $M \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$ embedded in N as matrices of the form:

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & A \end{pmatrix} \oplus \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

where $a, b \in \mathbb{C}$ and $A \in M_2(\mathbb{C})$. Let V_1 and V_2 be the simple 4- and 2-dimensional N-modules respectively, and W_1, W_2 and W_3 be the simple M-modules of dimension 1, 1 and 2. Then the Bratteli diagram and corresponding inclusion matrix for $M \subset N$ are:

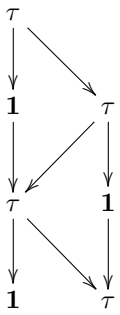


and

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The Bratteli diagram for the sequence $\mathcal{S}$ is the concatenation of the Bratteli diagrams for each pair (A_k, A_{k+1}), with corresponding inclusion matrix G_k. We organize this graph into levels (or stories) corresponding to each algebra A_k so that the Bratteli diagram (A_{k-1}, A_k) is placed above the vertices labelled by simple A_k-modules, and that of (A_k, A_{k+1}) is placed below. Having fixed an order on the simple A_k-modules we record the corresponding dimensions in a vector $\mathbf{d}_k$. Observe that $\mathbf{d}_{k+1} = G_k^T \mathbf{d}_k$.

Let us illustrate this for the Fibonacci theory corresponding to the colored TLJ-theory at $A = ie^{2\pi i/20}$. Here we have two labels $\mathbf{1}$ and τ as in subsection 4.2.3. Decomposing the simple $TLJ_n(A)$ modules for this theory as $TLJ_{n-1}(A)$ modules for $n = 1, 2, \ldots$ we have:



For each $n > 1$, $TLJ_n(A)$ has two simple modules: $V_{\mathbf{1},n} := \mathrm{Hom}(\mathbf{1}, \tau^{\otimes n})$ and $V_{\tau,n} := \mathrm{Hom}(\tau, \tau^{\otimes n})$. Moreover, $\mathbb{C}\rho_n(\mathcal{B}_n) = TLJ_n(A)$ so these are irreducible $\mathcal{B}_n$-representations. Let us compute the inclusion matrices as above, ordering the modules $[V_{\mathbf{1},n}, V_{\tau,n}]$ in spite of the alternating arrangement of the Bratteli diagram. Since $V_{\mathbf{1},n}|_{\mathcal{B}_{n-1}} \cong V_{\tau,n-1}$ and $V_{\tau,n}|_{\mathcal{B}_{n-1}} \cong V_{\mathbf{1},n-1} \oplus V_{\tau,n-1}$ we have: are $G = G_n = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ for all $n > 1$. By computing powers of G one can see that $\dim(V_{\mathbf{1},n}) = f_{n-1}$ and $\dim(V_{\tau,n}) = f_n$ where $f_0 = 1, f_1 = 1, f_2 = 1, f_3 = 2, \ldots$ is the Fibonacci sequence.

Now suppose that we could find a Yang-Baxter matrix R on a space W of dimension d localizing the sequence of $\mathcal{B}_n$-representations $(\rho_n, V_{\mathbf{1},n} \oplus V_{\tau,n})$. Using the algebra injections ψ_n, the space $W^{\otimes n}$ becomes a $TLJ_n(A)$-module and hence $W^{\otimes n} \cong a_n V_{\mathbf{1},n} \oplus b_n V_{\tau,n}$ as $TLJ_n(A)$ (or $\mathcal{B}_n$) modules with $a_n \geq 1$, $b_n \geq 1$ multiplicities. Notice that $d^n = a_n f_{n-1} + b_n f_n$ for all $n > 1$. We can use G to inductively express the multiplicities (a_n, b_n). Indeed, since restricting $a_n V_{\mathbf{1},n} \oplus b_n V_{\tau,n}$ to $\mathcal{B}_{n-1}$ we get $b_n V_{\mathbf{1},n-1} \oplus (a_n + b_n) V_{\tau,n-1}$, we have

$G(a_n, b_n)^T = (a_{n-1}, b_{n-1})$. Notice also that $G(f_{n-2}, f_{n-1})^T = (f_{n-1}, f_n)$. Thus the formula $d^n = a_n f_{n-1} + b_n f_n$ valid for all $n > 1$ gives us the two equations: $\langle (a_n, b_n), G(f_{n-2}, f_{n-1})\rangle = d^n$ and $\langle G(a_n, b_n), (f_{n-1}, f_n)\rangle = d^{n-1}$. But since $G^T = G$ we have

$$d^n = \langle (a_n, b_n), G(f_{n-2}, f_{n-1})\ rangle = \langle G(a_n, b_n), (f_{n-1}, f_n)\rangle = d^{n-1},$$

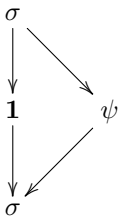
a contradiction. So the Fibonacci theory cannot be localized.

This may seem a bit *ad hoc*, but in fact this can be generalized whenever the Bratteli diagram for $\mathbb{C}\rho_n(\mathcal{B}_n) \subset \mathbb{C}\rho_{n+1}(\mathcal{B}_{n+1})$ is periodic of some period k. In this case there is a strictly positive integer-valued square matrix G that describes the inclusion of $\mathbb{C}\rho_n(\mathcal{B}_n) \subset \mathbb{C}\rho_{n+k}(\mathcal{B}_{n+k})$. One then applies the the Perron-Frobenius theorem to see that some vector of multiplicities $\mathbf{b}_n$ is an eigenvector of G corresponding to the largest eigenvalue λ of G. This implies that $\lambda \in \mathbb{Z}$, since G and $\mathbf{b}_n$ are integral, which often leads to a contradiction (see [20] for details).

6.3. Jones representation at levels 2 and 4

In this section we give explicit localizations for the Jones representations at levels 2 and 4.

For the Ising theory (level 2) an explicit localization appears in [6]. The objects are $\mathbf{1}, \sigma$ and ψ where $\mathrm{FPdim}(\sigma) = \sqrt{2}$ and $\mathrm{FPdim}(\psi) = 1$. The Bratteli diagram is:



and the matrix

$$\frac{-e^{-\pi i/4}}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

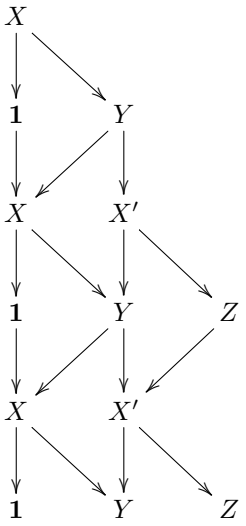
gives an explicit localization (see [6, Section 5]).

At level 4 ($A = ie^{-2\pi i/24}$), the categorical model is a rank 5 category with simple objects $\mathbf{1}, Z$ of dimension 1, Y of dimension 2 and X, X' of dimension $\sqrt{3}$. The fusion rules for this category are determined by:

$$X \otimes X \cong \mathbf{1} \oplus Y, \quad X \otimes X' \cong Z \oplus Y \tag{1}$$

$$X \otimes Y \cong X \oplus X', \quad Z \otimes X \cong X'. \tag{2}$$

The Bratteli diagram (starting at level 1) is shown in below.



We have $TLJ_n(A) \cong \mathrm{End}(X^{\otimes n})$ for each n, where the isomorphism is induced by

$$g_i \leftrightarrow Id_X^{\otimes i-1} \otimes c_{X,X} \otimes Id_X^{\otimes n-i-1} \in \mathrm{End}(X^{\otimes n}).$$

Here $c_{X,X}$ is the (categorical) braiding on the object X. The irreducible sectors of $TLJ_n(A)$ under this isomorphism are the $\mathrm{End}(X^{\otimes n})$-modules $H_{n,W} := \mathrm{Hom}(W, X^{\otimes n})$ where W is one of the 5 simple objects in $\mathcal{C}$. Observe that for n even W must be one of $\mathbf{1}, Y$ or Z while for n odd W is either X or X'. We have the following formulae for the dimensions of these irreducible representations (for n odd):

$$\dim \mathrm{Hom}(X, X^{\otimes n}) = \frac{3^{\frac{n-1}{2}}+1}{2}, \quad \dim \mathrm{Hom}(X', X^{\otimes n}) = \frac{3^{\frac{n-1}{2}}-1}{2},$$

$$\dim \mathrm{Hom}(\mathbf{1}, X^{\otimes n+1}) = \frac{3^{\frac{n-1}{2}}+1}{2}, \quad \dim \mathrm{Hom}(Y, X^{\otimes n+1}) = 3^{\frac{n-1}{2}},$$

$$\dim \mathrm{Hom}(Z, X^{\otimes n+1}) = \frac{3^{\frac{n-1}{2}}-1}{2}$$

We present the explicit localization, referring the reader to [20] for a complete proof. Here $\omega = e^{2\pi i/3}$ is a 3rd root of unity.

$$R = \frac{i}{\sqrt{3}} \begin{pmatrix} \omega & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega \\ 0 & \omega & 0 & 0 & 0 & \omega & 1 & 0 & 0 \\ 0 & 0 & \omega & \omega^2 & 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & \omega^2 & 0 \\ \omega & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & \omega & \omega & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 1 & \omega & 0 & 0 \\ 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & \omega & 0 \\ 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega \end{pmatrix}$$

In fact we have a complete characterization of localizable (uncolored) Jones representations, verifying Conjecture 6.2 in these cases:

Theorem 6.5. *The Jones representation at level k can be localized if and only if $k \in \{1, 2, 4\}$.*

This should be compared with Theorem 1.1 from which it follows that the Jones representations are universal for quantum computation precisely when the representations are not localizable.

References

[1] D. Aharonov, V. Jones, and Z. Landau, *A polynomial quantum algorithm for approximating the Jones polynomial*, Algorithmica **5** (2009), no. 3, 395–421.

[2] S. Bigelow, *The Burau representation is not faithful for $n = 5$*, Geometry & Topology **3** (1999), 397–404, arXiv:math/9904100v2.

[3] M. Brannan and B. Collins, *Dual bases in Temperley-Lieb algebras, quantum groups, and a question of Jones*, (2016), arXiv:1608.03885v2 [math.QA].

[4] J. Conway and A. Jones, *Trigonometric Diophantine equations (on vanishing sums of roots of unity)*, Acta Arithmetica **30** (1976), no. 3, 229–240.

[5] M. Epple, *Orbits of asteroids, a braid, and the first link invariant*, Math. Intelligencer **20** (1998), no. 1, 45–52.

[6] J. Franko, E. C. Rowell, and Z. Wang, *Extraspecial 2-groups and images of braid group representations*, J. Knot Theory Ramifications **15** (2006), no. 4, 1–15.

[7] M. H. Freedman, A. Kitaev, and Z. Wang, *Simulation of topological field theories by quantum computers*, Comm. Math. Phys. **227** (2002), no. 3, 587–603.

[8] M. H. Freedman, M. J. Larsen, and Z. Wang, *A modular functor which is universal for quantum computation*, Comm. Math. Phys. **227** (2002), no. 3, 605–622.

[9] M.H. Freedman, M. J. Larsen, and Z. Wang, *The two-eigenvalue problem and density of Jones representation of braid group*, Comm. Math. Phys. **228** (2002), no. 1, 177–199.

[10] W. Fulton and J.Harris, *Representation theory, a first course*, Springer, New York, 1991.

[11] V.F.R. Jones, *Braid groups, Hecke algebras and type II_1 factors*, Geometric methods in operator algebras **123** (1983), 242–273.

[12] ———, *Hecke-algebra representations of braid groups and link polynomials*, Ann. Math. **126** (1987), 335–288.

[13] S.P. Jordan and P.W. Shor, *Estimating Jones polynomials is a complete problem for one clean qubit*, Quantum Information and Computation **8** (2008), no. 8, 681–714.

[14] V. Kliuchnikov, A. Bocharov, and K. M. Svore., *Asymptotically optimal topological quantum compiling*, Physical Review Letters **112** (2014), no. 140504, 335–288.

[15] G. Kuperberg, *How hard is it to approximate the Jones polynomial?*, (2009), arXiv:0908.0512v2 [quant-ph].

[16] M.J. Larsen and E.C. Rowell, *An algebra-level version of a link-polynomial identity of Lickorish*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 3, 623–638.

[17] M.J. Larsen, E.C. Rowell, and Z. Wang, *The N-eigenvalue problem and two applications*, Int. Math. Res. Not. **2005** (2005), no. 64, 3987–4018.

[18] D. Naidu and E.C. Rowell, *A finiteness property for braided fusion categories*, Algebr. Represent. Theory **15** (2011), no. 5, 837–855.

[19] E. C. Rowell, R. Stong, and Z. Wang, *On classification of modular tensor categories*, Comm. Math. Phys. **292** (2009), no. 2, 343–389.

[20] E. C. Rowell and Z. Wang, *Localization of unitary braid representations*, Comm. Math. Phys. **311** (2012), no. 3, 595–615, arXiv:1009.0241v2 [math.RT].

[21] E.C. Rowell, *Braid representations from quantum groups of exceptional Lie type*, Rev. Un. Mat. Argentina **51** (2010), no. 1, 165–175.

[22] D.L. Vertigan, *On the computational complexity of Tutte, Jones, Homfly and Kauffman invariants*, Dissertation, University Of Oxford, 1991.

[23] Z. Wang, *Topological quantum computation*, American Mathematical Society, Providence (2008), http://www.math.ucsb.edu/zhenghwa/data/course/cbms.pdf.

(Recibido en julio de 2016. Aceptado en noviembre de 2016)

Department of Mathematics
University of California Santa Barbara
Santa Barbara, CA, U.S.A.
e-mail: cdelaney@math.ucsb.edu

Department of Mathematics
Texas A&M University
College Station, TX, U.S.A
e-mail: rowell@math.tamu.edu

Department of Mathematics, Microsoft Station Q
University of California Santa Barbara
Santa Barbara, CA, U.S.A.
e-mail: zhenghwa@microsoft.com