Mathematical Physics, Spring 2021

Braiding Matrices for Fibonacci Anyons

Kevin Loo

Yau Mathematical Sciences Centre, Tsinghua University, Beijing, 100084, China

Abstract: We review an interesting model that is capable of supporting universal topological quantum computation, known as the Fibonacci anyon model. Its capability can be shown by considering the $SU(2)_3$ Chern-Simons theory, which the Fibonacci theory is its even part. In particular, we will sketch the proof that a quantum circuit computation can be efficiently approximated by an intertwining action of a braid that corresponds to a unitary operation arbitrarily close to any desired operation.

Contents

1 Introduction **1**

2 Fibonacci Anyons **2**

2.1 Fusing Fibonacci Anyons 3

2.2 Braiding Fibonacci Anyons 5

2.3 Computing with Fibonacci Anyons 8

3 Universal Topological Quantum Computation **9**

3.1 Braid Group Representations 10

3.2 Topological Modular Functor 11

3.3 Projectively Dense Jones Representations 11

Nature isn't classical . . . and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

—Richard Feynman, 1981. *Simulating Physics with Computers.*

1 Introduction

A topological quantum computer is constructed using a system in a non-abelian topological phase. The computation is performed by creating quasiparticles, braiding them, and measuring their final state. One interesting quasiparticle model is the Fibonacci anyon model, which is known for its simplicity and its close relationship with the $\mathbb{Z}_3$ parafermion theory – a theory that actually describes the observed quantum Hall state at filling factor $\nu = 12/5$ [1, 2]. A given braid can be shown to perform the same quantum computation in either theory (up to an irrelevant overall abelian phase) [3]. Therefore, the Fibonacci theory and the associated braiding may be physically relevant for fractional quantum Hall topological quantum computation in high-mobility 2D semiconductor structures.

2 Fibonacci Anyons

The **Fibonacci anyon** model, or known in some literature as the **"Golden theory"**, is one of the simplest models of non-abelian statistics [3–6]. In this model, there are only two fields – the identity, $\mathbf{1}$, and a single nontrivial field usually called τ which represents the non-abelian quasiparticle. (Note there is no field representing the underlying electron in this simplified theory). This model has only a single nontrivial fusion rule:

$$\tau \times \tau = \mathbf{1} + \tau, \tag{0.1}$$

which makes it particularly simple[1] in that any cluster of quasiparticles can fuse only to $\mathbf{1}$ or τ. This results in the Bratteli diagram (Fig. 1).

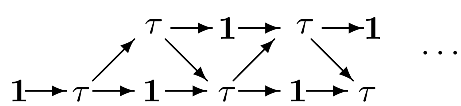

Figure 1. Bratteli diagram for Fibonacci anyons.

Bratteli diagram. Bratteli diagram is a useful technique for counting conformal blocks. In Fig. 1 we give the Bratteli diagram for the fusion of multiple τ fields. Starting with $\mathbf{1}$ at the lower left, at each step moving from the left to the right, we fuse with one more τ field. At the first step, the arrow points from $\mathbf{1}$ to τ since $\mathbf{1} \times \tau = \tau$. At the next step τ fuses with τ to produce either τ or $\mathbf{1}$ and so forth. Each conformal block is associated with a path through the diagram. Thus to determine the number of blocks in $\langle \tau\tau\tau\tau \rangle$ we count the number of paths of four steps in the diagram starting at the lower left and ending at $\mathbf{1}$.

$SO(3)_2$ theory. We may construct Fibonacci anyons as the $j = 0$ and $j = 1$ quasiparticles in $SU(2)_3$ satisfying the fusion rules of Fibonacci anyons; here we simply omit the $j = 1/2$ and $j = 3/2$ quasiparticles from $SU(2)_3$. This is perfectly consistent since half-integral j will never arise from the fusions of integral j's. This model with only integer spins can be called $SO(3)_2$ or, sometimes, 'the even part of $SU(2)_3$'. As a result of the connection to $SU(2)_3$, sometimes $\mathbf{1}$ is called q-spin "0" and τ is called q-spin "1" [3].

Why Fibonacci? The dimension of the Hilbert space with n quasiparticles, viz. the number of paths through the Bratteli diagram terminating at $\mathbf{1}$, is given by the Fibonacci number[2] $\mathrm{Fib}(n-1)$, hence the name Fibonacci anyons. Similarly the number terminating at τ is $\mathrm{Fib}(n)$.

[1] The Fibonacci anyon model is comparatively simpler than the Ising TQFT and its close relative, $SU(2)_2$, which have two fusion channels for a pair of σ quasiparticles, $\sigma \times \sigma \sim \mathbf{1} + \psi$, used for storing quantum information.

[2] The $(n-1)$-th Fibonacci number, denoted as $\mathrm{Fib}(n-1)$, is defined by $\mathrm{Fib}(1) = \mathrm{Fib}(2) = 1$ and $\mathrm{Fib}(n) = \mathrm{Fib}(n-1) + \mathrm{Fib}(n-2)$ for $n > 2$.

Therefore, the quantum dimension of the τ particle is the *golden mean*, $d_\tau = \phi \equiv (1+\sqrt{5})/2$, hence the alternative name "golden" theory.

Fibonacci anyons and qubits. The Fibonacci model is the simplest known non-abelian model that is capable of universal quantum computation [5], which will be discussed in the next section. This model has some interesting properties, i.e. its Hilbert space can be understood via fusion rules and a basis changing F-matrix, and braiding of two particles can be understood as a rotation R operator that produces a phase dependent on the quantum number of the two particles. One can thus always encode qubits in the quantum number of some group of particles. It is therefore instructive to study these properties in detail. Many of the principles that are described in the following subsections can be generalised to other non-abelian models.

2.1 Fusing Fibonacci Anyons

The detailed structure of the Hilbert space is one of the important features of non-abelian systems. A given state in the space can be described by a "fusion path" or "fusion tree".

Fusion tree diagram. The space spanned by the conformal blocks resulting from the fusion of fields is independent of the order of fusion (which field is fused with which field first). However, fusing fields together in different orders results in a different basis for that space. A convenient way to denote fusion of fields in a particular order is using fusion tree diagrams as follows.

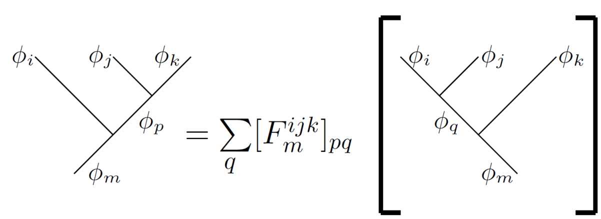

Figure 2. A fusion tree diagram depicts the basis states obtained by fusing fields together on different orders of fusion (although the space spanned by these states is independent of the order). The F-matrix converts between the possible bases.

Both diagrams in Fig. 2 show the fusion of three initial fields ϕ_i, ϕ_j, ϕ_k. One could fuse together ϕ_j and ϕ_k to form ϕ_p which then fused with ϕ_i to form ϕ_m, as shown on the left of Fig. 2. The diagram on the right depicts an equally well choice of fusing ϕ_i and ϕ_j together first before fusing the result with ϕ_k. The mathematical relation between these two bases is given in the equation shown in Fig. 2 in terms of the so-called F-matrix (for "fusion"), which is an important property of any given CFT or TQFT.

Two τ particles. By the fusion rule (0.1), or examining the Bratteli diagram, two τ particles may fuse into two possible orthogonal degenerate states – one in which they fuse to form **1** and the other in which they fuse to form τ. A convenient notation [4] for these two states is $|(\bullet,\bullet)_{\mathbf{1}}\rangle$ and $|(\bullet,\bullet)_{\tau}\rangle$, with each $\bullet$ representing a particle.

Three τ particles. When a third is added to two particles already in the $\mathbf{1}$ state, $|(\bullet,\bullet)_{\mathbf{1}}\rangle$, it must fuse to form τ, which we will denote as $|((\bullet,\bullet)_{\mathbf{1}},\bullet)_{\tau}\rangle \equiv |0\rangle$. If the third is added to two in the τ state, it may fuse to form either τ or $\mathbf{1}$, giving the two states $|((\bullet,\bullet)_{\tau},\bullet)_{\tau}\rangle \equiv |1\rangle$ and $|((\bullet,\bullet)_{\tau},\bullet)_{\mathbf{1}}\rangle \equiv |N\rangle$. Therefore we have a three dimensional Hilbert space for three particles, shown using several notations in Fig. 3.

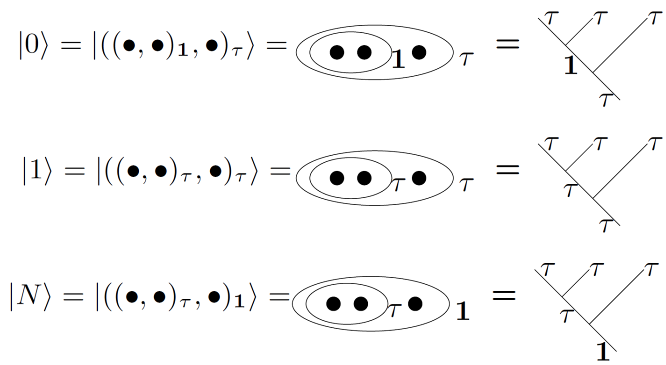

Figure 3. The three Fibonacci particles represent a qubit; the three possible states are labelled (far left) as the logical $|0\rangle$, $|1\rangle$ and noncomputational $|N\rangle$ of the qubit. Here, the "quantum number" of an individual particle is τ. Other common notations are the parenthesis (left) and ellipse (middle) notations, where each black dot is a particle, and each pair of parenthesis or ellipse around a group of particles is labelled at the lower right with the total quantum number associated with the fusion of that group. Analogously in the fusion tree notation (right), particles are described by the branching of the tree, and each line is labelled with the quantum number corresponding to the fusion of all the particles in the branches above it. For instance, on the top line the two particles on the left fuse to form $\mathbf{1}$ which then fuses with the remaining particle on the right to form τ.

An opposite order. Instead of fusing the particles from left to right as in Fig. 3, it is possible to fuse the two particles on the right first, and then fuse with the particle furthest on the left last. The three resulting states in this opposite order can be denoted as $|(\bullet,(\bullet,\bullet)_{\mathbf{1}})_{\tau}\rangle$, $|(\bullet,(\bullet,\bullet)_{\tau})_{\tau}\rangle$, and $|(\bullet,(\bullet,\bullet)_{\tau})_{\mathbf{1}}\rangle$. As mentioned previously, different fusion orders results in a different basis set for that space (although the space of states that is spanned by fusion of non-abelian particles is independent of the fusion order). The change of basis is encoded in the F**-matrix**,

$$|(\bullet,(\bullet,\bullet)_i)_k\rangle = \sum_j (F_k^{\tau\tau\tau})_{ij}\, |((\bullet,\bullet)_j,\bullet)_k\rangle\,, \tag{0.2}$$

where i, j, k take the values of the fields $\mathbf{1}$ or τ.

1. **State $|N\rangle$.** We have $|(\bullet,(\bullet,\bullet)_{\tau})_{\mathbf{1}}\rangle = |((\bullet,\bullet)_{\tau},\bullet)_{\mathbf{1}}\rangle$ since in either fusion order there is only a single state that has total topological charge $\mathbf{1}$ (the overall quantum number of a group of particles is independent of the basis). Clearly, $(F_{\mathbf{1}}^{\tau\tau\tau})$ is trivially unity.

2. **States $|0\rangle$ and $|1\rangle$.** These two states of the three-particle space, however, transform nontrivially under change of fusion order, where the two-by-two matrix $(F_\tau^{\tau\tau\tau})$ is

$$(F_\tau^{\tau\tau\tau}) = \begin{pmatrix} F_{\mathbf{11}} & F_{\mathbf{1}\tau} \\ F_{\tau\mathbf{1}} & F_{\tau\tau} \end{pmatrix} = \begin{pmatrix} \phi^{-1} & \sqrt{\phi^{-1}} \\ \sqrt{\phi^{-1}} & -\phi^{-1} \end{pmatrix}. \tag{2.1}$$

Four τ particles. For the Fibonacci theory [6], there is a *consistency condition*, known as the **pentagon identity** [7–10], which makes the calculation of the F-matrix easy. This condition simply says that one should be able to make changes of basis for four particles in several possible ways and get the same result in the end. As an example, we have

$$\begin{aligned} |(\bullet,(\bullet,(\bullet,\bullet)_{\mathbf{1}})_\tau)_{\mathbf{1}}\rangle &= |((\bullet,\bullet)_{\mathbf{1}},(\bullet,\bullet)_{\mathbf{1}})_{\mathbf{1}}\rangle \\ &= |(((\bullet,\bullet)_{\mathbf{1}},\bullet)_\tau,\bullet)_{\mathbf{1}}\rangle \end{aligned} \tag{2.2}$$

where both equalities can be deduced from the fusion rules alone. In the first equality, the rightmost two particles on both sides are in a state $\mathbf{1}$. Given that on the left-hand side, the overall quantum number is $\mathbf{1}$, then on the right-hand side, when we fuse the leftmost two particles they must fuse to $\mathbf{1}$ such that the overall quantum number remains $\mathbf{1}$. For the second equality, we may express it in terms of the F-matrix (0.2) as

$$\begin{aligned} |(\bullet,(\bullet,(\bullet,\bullet)_{\mathbf{1}})_\tau)_{\mathbf{1}}\rangle &= F_{\mathbf{11}}\,|(\bullet,((\bullet,\bullet)_{\mathbf{1}},\bullet)_\tau)_{\mathbf{1}}\rangle + F_{\mathbf{1}\tau}\,|(\bullet,((\bullet,\bullet)_\tau,\bullet)_\tau)_{\mathbf{1}}\rangle \\ &= F_{\mathbf{11}}\,|((\bullet,(\bullet,\bullet)_{\mathbf{1}})_\tau,\bullet)_{\mathbf{1}}\rangle + F_{\mathbf{1}\tau}\,|((\bullet,(\bullet,\bullet)_\tau)_\tau,\bullet)_{\mathbf{1}}\rangle \\ &= \sum_j \left(F_{\mathbf{11}}F_{\mathbf{1}j} + F_{\mathbf{1}\tau}F_{\tau j}\right)|(((\bullet,\bullet)_j,\bullet)_\tau,\bullet)_{\mathbf{1}}\rangle \end{aligned} \tag{2.3}$$

Comparing to the second equality in (2.2) yields $F_{\mathbf{1}\tau}(F_{\mathbf{11}} + F_{\tau\tau}) = 0$ and $F_{\mathbf{11}}F_{\mathbf{11}} + F_{\mathbf{1}\tau}F_{\tau\mathbf{1}} = 1$. This, and other similar consistency identities, along with the requirement that F be unitary, completely fix the Fibonacci F-matrix to be precisely that given in Eq. (2.1) (up to a gauge freedom in the definition of the phase of the basis states).

2.2 Braiding Fibonacci Anyons

For non-abelian anyon systems, adiabatically braiding anyons around each other results in a unitary operation (i.e. nontrivial rotation) on a degenerate many-anyon Hilbert space. As the anyons are braided (wound) around each other, they pick up some topological phase due to the Aharonov-Bohm effect[3]. Here we attempt to determine which unitary operation results from which braid.

[3]We can think of anyons as being composite particles consisting of a flux Φ and a ring of charge q. When a particle circulates another particle, its charge q goes around the flux Φ, thus acquiring a phase factor $U = e^{iq\Phi}$ due to the Aharonov-Bohm effect. The statistical angle of these anyons is then $\varphi = q\Phi/2$. Non-abelian charges and fluxes can generate unitary matrices instead of phase factors. In this case a circulation of one anyon around another can lead to a final state in superposition. The anyons that have such statistics are called non-abelian, while anyons that obtain a simple phase factor are called abelian.

Two τ particles, again. Let us consider what happens to two Fibonacci particles when they are braided around each other. The fields $\mathbf{1}$ and τ have conformal dimensions[4] $\Delta_{\mathbf{1}} = 0$ and $\Delta_\tau = 2/5$, respectively. One can use the operator product expansion (OPE) of two arbitrary fields ϕ_i and ϕ_j,

$$\lim_{z \to w} \phi_i(z)\phi_j(w) = \sum_k C_{ij}^k \, (z-w)^{\Delta_k - \Delta_i - \Delta_j} \phi_k(w), \tag{2.4}$$

to determine the phase accumulated when two particles wrap around each other. This will result in two possibilities. On the one hand, taking two τ fields around each other clockwise results in $\mathbf{1}$ with a phase $-8\pi/5 = 2\pi(-2\Delta_\tau)$. On the other hand, the same operation may result in τ with a phase $-4\pi/5 = 2\pi(-\Delta_\tau)$.

Once the phase accumulated for a full wrapping of two particles is known, the clockwise exchange of two particles (half of a full wrapping) gives a phase of $\pm 4\pi/5$ if the fields fuse to $\mathbf{1}$ or $\pm 2\pi/5$ if the fields fuse to τ. To determine these signs, we will invoke another consistency condition, known as the **hexagon identity**[5] [7, 9, 10], which in essence assure that the rotation operations are consistent with the F-matrix, viz. we can rotate before or after changing bases and we get the same result. We can then determine that the R**-matrix** (for "rotation") is given by

$$\begin{aligned} R\,|(\bullet,\bullet)_{\mathbf{1}}\rangle &= e^{-4\pi i/5}\,|(\bullet,\bullet)_{\mathbf{1}}\rangle\,, \\ R\,|(\bullet,\bullet)_{\tau}\rangle &= -e^{-2\pi i/5}\,|(\bullet,\bullet)_{\tau}\rangle\,, \end{aligned} \tag{2.5}$$

i.e. $R^{\mathbf{1}}_{\tau\tau} = e^{-4\pi i/5}$ and $R^{\tau}_{\tau\tau} = -e^{-2\pi i/5}$. In general, with the R-matrix and F-matrix, one can determine the unitary operation that results from performing any braid on any number of particles. This leads naturally to the notion of a braid group.

Definition. The **braid group** on n particles (can be thought of as n strands) has the well-known presentation:

$$B_n = \left\{ \sigma_1, \cdots, \sigma_{n-1} \,\middle|\, \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i, \ |i-j| \geq 2, \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \ 1 \leq i \leq n-1 \end{array} \right\}, \tag{2.6}$$

where the braid group generators σ_i are the half right twists of the i-th strand about the $(i+1)$-th strand.

Remark. *A Fibonacci theory with the opposite chirality (an "antiholomorphic theory") also exists, in which case one accumulates the opposite phase. A nonchiral (or "achiral") theory can also exist; it is a combination of two chiral Fibonacci theories with opposite chiralities.*

Three τ particles, again. In Fig. 4, the braid group is generated by σ_1 and σ_2. As mentioned above, the Hilbert space of three particles is three dimensional as shown in Fig. 3. The unitary

[4] It is known [7] that the topological spin Θ_τ of a Fibonacci field τ is $\Theta_\tau \equiv e^{2\pi i \Delta_\tau} = e^{4\pi i/5}$.

[5] One can prove that $\Delta_\tau = 2/5$ by using the hexagon identity and pentagon identity.

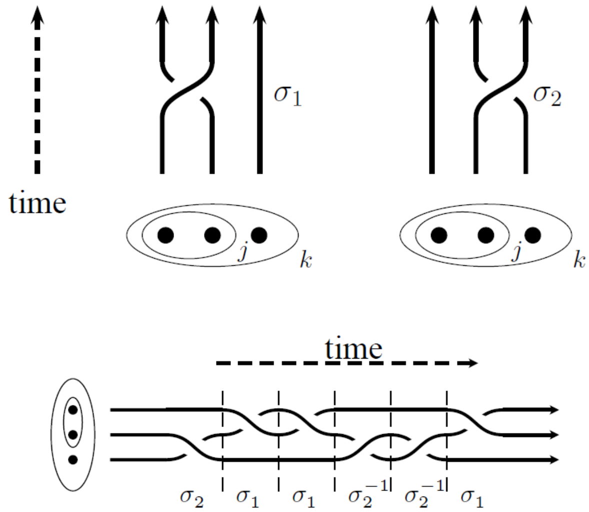

Figure 4. **Top**: The two elementary braid operations σ_1 and σ_2 on three particles. **Bottom**: Using these two braid operations and their inverses, an arbitrary braid on three strands can be built. The braid shown here is written as $\sigma_2\sigma_1\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1$.

operation corresponding to the braid σ_1 is determined from (2.5) to be

$$\begin{pmatrix} |0\rangle \\ |1\rangle \\ |N\rangle \end{pmatrix} \rightarrow \underbrace{\left(\begin{array}{cc|c} e^{-4\pi i/5} & 0 & 0 \\ 0 & -e^{-2\pi i/5} & 0 \\ \hline 0 & 0 & -e^{-2\pi i/5} \end{array}\right)}_{\rho(\sigma_1)} \begin{pmatrix} |0\rangle \\ |1\rangle \\ |N\rangle \end{pmatrix}. \tag{2.7}$$

Evaluating the effect of σ_2 is less trivial. We can perform the operation $\rho(\sigma_2) = F^{-1}RF$, viz. we first make a basis change using F in order to determine how the two rightmost particles fuse, then rotates these two rightmost particles using R, and finally undo the basis change. Explicitly, let us consider what happens to the state $|0\rangle$. We first use (0.2) to write

$$|0\rangle = F_{\mathbf{11}}\,|(\bullet,(\bullet,\bullet)_{\mathbf{1}})_\tau\rangle + F_{\tau\mathbf{1}}\,|(\bullet,(\bullet,\bullet)_\tau)_\tau\rangle\,. \tag{2.8}$$

Rotating the two right particles then gives

$$R\,|0\rangle = e^{-4\pi i/5}F_{\mathbf{11}}\,|(\bullet,(\bullet,\bullet)_{\mathbf{1}})_\tau\rangle - e^{-2\pi i/5}F_{\tau\mathbf{1}}\,|(\bullet,(\bullet,\bullet)_\tau)_\tau\rangle\,. \tag{2.9}$$

and then we transform back to the original basis using the inverse of (0.2) to yield

$$\begin{aligned} \rho(\sigma_2)\,|0\rangle &= ([F^{-1}]_{\mathbf{11}}e^{-4\pi i/5}F_{\mathbf{11}} - [F^{-1}]_{\mathbf{1}\tau}e^{-2\pi i/5}F_{\tau\mathbf{1}})\,|0\rangle \\ &\quad + ([F^{-1}]_{\tau\mathbf{1}}e^{-4\pi i/5}F_{\mathbf{11}} - [F^{-1}]_{\tau\tau}e^{-2\pi i/5}F_{\tau\mathbf{1}}\,|1\rangle \\ &= -e^{-\pi i/5}/\phi\,|0\rangle - ie^{-i\pi/10}/\sqrt{\phi}\,|1\rangle\,. \end{aligned} \tag{2.10}$$

Similar results can be derived for the other two basis states to give the matrix

$$\rho(\sigma_2) = \left(\begin{array}{cc|c} -e^{-\pi i/5}/\phi & -ie^{-i\pi/10}/\sqrt{\phi} & 0 \\ -ie^{-i\pi/10}/\sqrt{\phi} & -1/\phi & 0 \\ \hline 0 & 0 & -e^{-2\pi i/5} \end{array}\right). \tag{2.11}$$

The braid operations σ_1 and σ_2 as well as their inverses generate all possible braids on three strands. We can thus use Eqs. (2.7) and (2.11) to determine the unitary operation resulting from any braid on three strands, with the unitary operations being built up from the elementary matrices $\rho(\sigma_1)$ and $\rho(\sigma_2)$ in the same way that the complicated braids are built from the braid generators σ_1 and σ_2. In particular, the braid $\sigma_2\sigma_1\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1$ shown in Fig. 4 corresponds[6] to the unitary matrix $\rho(\sigma_1)\rho(\sigma_2^{-1})\rho(\sigma_2^{-1})\rho(\sigma_1)\rho(\sigma_1)\rho(\sigma_2)$.

2.3 Computing with Fibonacci Anyons

Having stated the properties of Fibonacci anyons, we would like to show how to do quantum computation using these anyons, viz. how to construct our qubits.

Single qubit. As suggested by Freedman *et al.* [5], we shall use *three (quasi)particles* to represent a qubit (many other schemes[7] for encoding qubits are also possible). We represent the two states of the qubit as $|0\rangle$ and $|1\rangle$ states, as shown in Fig. 3, with an additional state $|N\rangle$ being a "noncomputational" state. We arrange in such a way that the overall quantum number of the three particles must remain unchanged under any amount of braiding. In other words, at the beginning and end of our computations, there will be no amplitude in this state. Any amplitude that ends up in this state is known as **"leakage error"**. Note that the braiding matrices $\rho(\sigma_1)$ and $\rho(\sigma_2)$ are block diagonal and thus never mix the noncomputational state $|N\rangle$ with the computational space $|0\rangle$ and $|1\rangle$. Therefore, braiding the three particles gives us a way to do single qubit operations with *no leakage*.

Multiple qubits. Let us now turn to multiple qubits, each encoded with three particles. To perform universal quantum computation, in addition to being able to perform single qubit operations, we must also be able to perform two-qubit entangling gates [11, 12]. Such two-qubit gates will necessarily involve braiding together (physically "entangling"!) the particles from two different qubits. The result of Freedman *et al.* [5] generally guarantees that these braids exist corresponding to any desired unitary operation on a two-qubit Hilbert space. This is equivalent to saying that the braids have *dense images*.

[6]The order is reversed since the operations that occur at earlier times are written to the left in conventional braid notation, but on the right when multiplying matrices together.

[7]A naive choice might be to use two particles for a qubit and declare the two states $|(\bullet,\bullet)_{\mathbf{1}}\rangle$ and $|(\bullet,\bullet)_\tau\rangle$ to be the two orthogonal states of the qubit. However, one can never change $|(\bullet,\bullet)_{\mathbf{1}}\rangle$ to $|(\bullet,\bullet)_\tau\rangle$ by a single qubit operation, viz. braiding (rotating) once the two particles around each other. In other words, it is not possible to change the overall quantum number of a group of particles by braiding within that group.

Dense image. A quantum state is said to be able to support universal quantum computation as long as the set of braids has a **"dense image"** in the set of unitary operations. (In other words, the braid group representations should have dense images in the unitary group.) This means that *there exists a braid that corresponds to a unitary operation arbitrarily close to any desired operation.* The closer one wants to approximate the desired unitary operation, the longer the braid typically needs to be, although only logarithmically so (i.e, the necessary braid length grows only as the *log* of the allowed error distance to the target operation). We shall sketch a proof of this result in the next section.

In such a theory that allows universal quantum computation, one always needs to encode a qubit with at least three particles so that one is able to do single qubit operations by braiding particles within a qubit. To perform two-qubit operations one needs to braid particles constituting one qubit with the particles constituting another qubit. In general, it is always the case that one can achieve a unitary operation by braiding n particles around each other with an arbitrary braid, or by moving (weaving) a single particle around $n-1$ others that remain stationary [13].

Practical construction of braids. The problem of actually finding the braids for a qubit that correspond to desired unitary operations, while apparently complicated, turns out to be straightforward [3, 4]. With the iterative algorithm proposed by Solovay and Kitaev [12], one can put together many short braids to efficiently construct a long braid arbitrarily close to any desired target unitary operation. Such a braid is polylogarithmically long in the allowed error distance to the desired operation and hence the search is only algebraically hard in the length of the braid.

Further, finding braids for multi-qubit is a much more formidable task. The full Hilbert space for six Fibonacci particles (constituting two qubits) is now 13 dimensional, and searching for a desired result in such a high dimensional space is extremely hard even for a powerful classical computer. Therefore, the problem needs to be tackled by divide-and-conquer approaches, building up two-qubit gates out of simple braids on three particles [3, 4]; a detailed discussion can be found in [14] Section IV.B.c.

3 Universal Topological Quantum Computation

We claimed that Fibonacci anyons were capable of supporting universal topological quantum computation. In this section, we *sketch a proof* of this claim within the context of a more general question: *which topological states are universal for quantum computation* or, in starker terms, *for which topological states is the entire gate set required to efficiently simulate an arbitrary quantum circuit to arbitrary accuracy.*

A general braid is composed of copies of a single operation (Figure 5) and its inverse. For Fibonacci anyons, "positive braids" will prove to be sufficient, where there is no necessity to ever use the inverse operation. In this section, we shall see why.

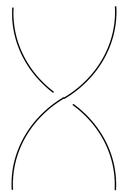

Figure 5. A single operation of braiding in a state supporting universal quantum computation.

3.1 Braid Group Representations

We shall assume a single species of quasiparticle, σ (a general case of Fibonacci anyon τ). When there are n σ's at fixed positions $z_1, \cdots, z_n$, there is an exponentially large ($\sim (d_\sigma)^n$-dimensional) ground state subspace V_n of Hilbert space. For quantum computation with anyons, the qubits must be located in the "Fibonacci" state space, since a general V_n has no natural tensor factoring (it can have prime dimension), where some directions in V_n are discarded from the computational space and so one must always guard against unintended "leakage" into the discarded directions.

Braiding the σ's produces a **representation** ρ_n,

$$\rho_n : B_n \rightarrow U(V_n) \tag{2.1}$$

from the braid group B_n on n strands into the unitary transformations of V_n. Here, since only the projective reduction in the projective group[8] $PU(V_n)$ has physical significance, we do not care about the overall phase of the wavefunction.

We would like to be able to enact an arbitrary unitary transformation such that up to phase, $\rho_n(B_n)$ is **dense** in $PU(V_n)$, i.e. *the intersection of all closed sets containing* $\rho_n(B_n)$ *should simply be* $PU(V_n)$. In other words, an arbitrary unitary transformation can be approximated, up to a phase, by a transformation in $\rho_n(B_n)$ to within any desired accuracy. This is the condition which our topological phase must satisfy.

For a modestly large number (≥ 7) of σ's, it was shown [5, 15] that the braid group representations associated with $SU(2)_k$ Chern-Simons theory at level $k \neq 1, 2, 4$ are dense in $SU(V_n, k)$, and hence in $PU(V_n, k)$. This type of representation is known as the **Jones representation**[9] or **Jones-Witten representation**. This representation satisfies a key **"two eigenvalue property" (TEVP)**, defined as follows.

Definition. Let G be a compact Lie group and φ a faithful, irreducible, unitary representation. The pair (G, φ) has TEVP if there exists a conjugacy class $[g]$ of G such that:

1. $[g]$ generates a dense set in G.

[8] $PU(V_n)$ is a set of unitary transformations on V_n with two transformations identified if they differ only by a phase.

[9] Formally, the Jones representation of the braid groups is defined as $\rho(\sigma_i) = q - (1+q)e_i$, where $q = e^{\frac{2\pi i}{r}}, r \geq 3$ and e_i is the basis of projectors that generate, with the identity 1, the Temperley-Lieb-Jones algebras.

2. For any $g \in [g]$, g acts on φ with exactly two distinct eigenvalues whose ratio is not ± 1.

The TEVP simply means that the image matrix of each braid generator σ_i under the Jones representation has exactly two distinct eigenvalues whose ratio is not ± 1. A salient feature of the Jones representation is that it splits as a direct sum of irreducible representations indexed by some 2-row Young diagrams, which we will refer to as *sectors*.

Definition. A Young diagram $\lambda = [\lambda_1, \cdots, \lambda_s], \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s$ is called a $(2, r)$ **diagram** if $s \leq 2$ (at most two rows) and $\lambda_1 - \lambda_2 \leq r - 2$. An irreducible representation corresponding to a $(2, r)$ diagram $\lambda = [\lambda_1, \lambda_2]$ is known as a **sector**, denoted by $\rho_{[\lambda_1, \lambda_2]}$.

3.2 Topological Modular Functor

The Jones representation of a braid group is, in fact, equivalent to the representation of the $SU(2)_k$ (Witten-)Chern-Simons modular functor at an r-th root of unity, $q = e^{\frac{2\pi i}{r}}$, which is used to build a universal quantum computer. The equivalence of these two representations was established in [5, 16].

Definition. A **modular functor** assigns to a compact surface Σ a complex vector space $V(\Sigma)$ and to a diffeomorphism of the surface (preserving structures) a linear map of $V(\Sigma)$.

Here we consider $V(\Sigma)$ that always has a positive definite hermitian inner product $\langle\ ,\ \rangle_h$ and the induced linear maps that are unitary (preserve $\langle\ ,\ \rangle_h$). There are usually additional structures to a modular functor [17, 18], but these can be dropped when we consider quantum-$SU(2)_k$-invariants of braiding.

An $SU(2)_k$ Chern-Simons modular functor is a **topological modular functor (TMF)**[10], which gives a family of representations of the braid group and mappling class groups. Here we will consider the $SU(2)_3$ Chern-Simons modular functor of braids at the fifth root of unity $q = e^{\frac{2\pi i}{5}}$ (level $k = 3$), which can be used to build the so-called "Chern-Simons5" (**CS5**) model which efficiently and fault tolerantly simulates the computations of an exact quantum circuit model. The details can be found in [5].

3.3 Projectively Dense Jones Representations

We shall sketch a proof of our claim, known as the *density theorem*[11] in [5], which states that the closed image of some Jones representation ρ_n is densely generated by elements σ_i satisfying the TEVP. Here we will be content with doing the simplest nontrivial case: six Fibonacci anyons τ with total charge 1 and ground state subspace $V_6 \cong \mathbb{C}^5 \cong 2$ qubits $\oplus$ non-computational $\mathbb{C}$.

[10] The TMF is the strictly 2-dimensional part of a topological quantum field theory (TQFT).

[11] A more general theorem for cases $r \geq 5, r \neq 6, 10, n \geq 3$ or $r = 10, n \geq 5$ [15] leads to the result that the $SU(2)_k$ Chern-Simons modular functor at an r-th root of unity is universal for quantum computation if $r \neq 3, 4, 6$.

Theorem (Density theorem)**.** *Let $\rho := \rho_{[3,3]} \oplus \rho_{[4,2]} : B_6 \to U(5) \times U(8)$ be the Jones representation of the braid group B_6 at the 5-th root of unity $q = e^{\frac{2\pi i}{5}}$. Then the closure of the image of $\rho(B_6)$ in $U(5) \times U(8)$ contains $SU(5) \times SU(8)$.*

By the equivalence theorem [5, 16], this is the same representation $\rho : B_6 \to U(5) \times U(8)$ in the $SU(2)_3$ Chern-Simons modular functor at the 5-th root of unity. The proofs of the density for $\rho_{[3,3]}$ and $\rho_{[4,2]}$ are similar. One may prove both cases at the same time and give separate argument for the more complicated case $\rho_{[4,2]}$ when necessary.

Let H be the closure of the image, $\overline{\text{image}(\rho)}$, of $\rho_{[3,3]}$ (or $\rho_{[4,2]}$) in $U(5)$ (or $U(8)$) which we will try to identify. By Theorem 3.1 in [5], H is a compact subgroup of $U(m)$ ($m = 5$ or 8) of positive dimension. Denote by φ the induced m-dimensional faithful, irreducible complex representation of H. The representation φ is faithful since H is a subgroup of $U(m)$. Let H_0 be the identity component of H. What we actually want to show is that the derived group $[H_0, H_0]$ (or universal cover of the derived group $[\widetilde{H_0, H_0}]$) of H_0, is actually $SU(m)$. The proof proceeds as follows.

Sketch of proof. Here all braid generators σ_i are conjugate and, in nontrivial cases, the eigenvalue ratio is not ± 1. Using the Jones skein relation $q^{-1/2}\rho(\sigma_i) - q^{1/2}\rho(\sigma_i^{-1}) = q^{1/4} - q^{-1/4}$, one can assert that the fundamental representation of $U(m)$ restricted to H, $\varphi|_H$, has the TEVP. We would like to show that $V|_H$ is irreducible. This was done by a series of technical lemmas in [5].

Using TEVP, one first shows that the further restriction to the identity component H_0, $\varphi|_{H_0}$, is *isotypic* (i.e. a direct sum of several copies of a single irreducible representation of H) and then *irreducible*. This implies that H_0 is *reductive* ($H_0 = H_0^{Der} Z(H_0)$, with $Z(H_0)$ the centre of H_0), so its derived group $H_0^{Der} := [H_0, H_0]$ is semisimple and, it can be argued, $\varphi|_{H_0^{Der}}$ still satisfies the TEVP and is still irreducible.

A final (harmless) variation on H is to pass to the universal cover $H_0^{uc} := [\widetilde{H_0, H_0}]$. The pulled back representation $\varphi|_{H_0^{uc}}$ still has the TEVP and one finally arrives at the irreducible representations of semisimple Lie groups of bounded dimension, where one can apply the classification of such representations [19] to show that the mysterious H_0^{uc} is none other than $SU(m)$. If this is so, then it follows that the sequence $H \to H_0 \to [H_0, H_0] \to [\widetilde{H_0, H_0}]$ did nothing (beyond the first arrow, which may have eliminated some components of H on which the determinant is a nontrivial root of unity).

To complete the proof, let us summarise our situation: we have shown the existence of a nontrivial semisimple group H_0^{uc} with an irreducible unitary representation $\varphi|_{H_0^{uc}}$. Furthermore, it has a special element x whose image under the representation has exactly two distinct eigenvalues whose ratio is not ± 1. The remaining work[12] is to search for this irreducible representation.

[12] In general, looking for which Jones representations are projectively dense, out of the classification [19], requires some tricky combinatorics and rank-level duality [15].

The closed image of $\rho_{[3,3]}$ is $H \subset U(5)$, so our irreducible representation $\varphi|_{H_0^{uc}}$ of H_0^{uc}, coming from $U(5)$'s fundamental, is exactly 5-dimensional (we don't yet know the dimension of H_0^{uc}). From McKay and Patera, 1981 [19], there are four 5-dimensional irreducible representations, which we list by rank:

1. rank = 1: $(SU(2), 4\varpi_1)$,
2. rank = 2: $(Sp(4), \varpi_2)$,
3. rank = 4: $(SU(5), \varpi_i),\ i = 1, 4$,

where ϖ_i is the fundamental weight. By examining the possible eigenvalues, we can exclude the first two cases as follows.

In case (1), suppose $x \in SU(2)$ has eigenvalues α and β in ϖ_1. Then under $4\varpi_1$, it will have $\alpha^i\beta^j,\ i+j=4\ (i,j \geq 0)$ as eigenvalues, which are too many (unless $\frac{\alpha}{\beta} = \pm 1$). In case (2), since 5 is odd, every element in the image has at least one real eigenvalue, with the others coming in reciprocal pairs. Again, there is no solution (unless there are two eigenvalues whose ratio is ± 1). Therefore, by the TEVP, the only possible pair is case (3), viz. $H_0^{uc} \cong SU(5)$. Since φ is a faithful representation of H_0^{Der}, the image of H_0^{Der} is the same as that of H_0^{uc} which is $SU(5)$. From this we get the desired conclusion: $SU(5) \subset H \subset U(5)$.

The same eigenvalue analysis can be done for the 8-dimensional case for $\rho_{[4,2]}$, which one will get the irreducible representation $(SU(8), \varpi_i),\ i = 1, 7$; details are in [5]. This completes the proof of our density theorem. □

Example. *For the (2,5) Young diagram $\lambda = [3,3]$, the representation $\rho_{[3,3]}$ is 5-dimensional. With an appropriate ordering of the basis, $\rho_{[3,3]}$ takes the braid generators σ_i (projectively) to these operators:*

$$\rho_{[3,3]}(\sigma_1) = \begin{pmatrix} -1 & & & & \\ & q & & & \\ & & -1 & & \\ & & & q & \\ & & & & q \end{pmatrix}, \quad \rho_{[3,3]}(\sigma_2) = \begin{pmatrix} \frac{q^2}{q+1} & -\frac{q\sqrt{[3]}}{q+1} & & & \\ -\frac{q\sqrt{[3]}}{q+1} & -\frac{1}{q+1} & & & \\ & & \frac{q^2}{q+1} & -\frac{q\sqrt{[3]}}{q+1} & \\ & & -\frac{q\sqrt{[3]}}{q+1} & -\frac{1}{q+1} & \\ & & & & q \end{pmatrix}, \tag{3.1}$$

where $[3] = q + q^{-1} + 1$, and σ_i for $i = 3, 4, 5$ are similar; details can be found in [16]. It is clear that the positive braid generators are sufficient for the Fibonacci anyons to support a universal topological quantum computation.

References

[1] E. H. Rezayi and N. Read, "Non-abelian quantized hall states of electrons at filling factors 12/5 and 13/5 in the first excited landau level," *Physical Review B* **79** no. 7, (Feb, 2009) 5. http://dx.doi.org/10.1103/PhysRevB.79.075306.

[2] J. S. Xia, W. Pan, C. L. Vicente, E. D. Adams, N. S. Sullivan, H. L. Stormer, D. C. Tsui, L. N. Pfeiffer, K. W. Baldwin, and K. W. West, "Electron correlation in the second landau level: A competition between many nearly degenerate quantum phases," *Physical Review Letters* **93** no. 17, (Oct, 2004) 5. http://dx.doi.org/10.1103/PhysRevLett.93.176809.

[3] L. Hormozi, G. Zikos, N. E. Bonesteel, and S. H. Simon, "Topological quantum compiling," *Physical Review B* **75** no. 16, (Apr, 2007) 20. http://dx.doi.org/10.1103/PhysRevB.75.165310.

[4] N. E. Bonesteel, L. Hormozi, G. Zikos, and S. H. Simon, "Braid topologies for quantum computation," *Physical Review Letters* **95** no. 14, (Sep, 2005) 4. http://dx.doi.org/10.1103/PhysRevLett.95.140503.

[5] M. Freedman, M. Larsen, and Z. Wang, "A modular functor which is universal for quantum computation," *arXiv e-prints* (Jan., 2000) 23, arXiv:quant-ph/0001108 [quant-ph].

[6] J. Preskill, "Lecture notes for physics 219:quantum computation," 2004. http://theory.caltech.edu/~preskill/ph219/topological.pdf.

[7] J. Fuchs, *Affine Lie algebras and quantum groups: An Introduction, with applications in conformal field theory.* Cambridge University Press, 3, 1995.

[8] C. Gómez, M. Ruiz-Altaba, and G. Sierra, *Quantum groups in two-dimensional physics.* Cambridge University Press, 2005.

[9] G. Moore and N. Seiberg, "Polynomial equations for rational conformal field theories," *Physics Letters B* **212** no. 4, (1988) 451–460.

[10] G. Moore and N. Seiberg, "Classical and quantum conformal field theory," *Communications in Mathematical Physics* **123** no. 2, (1989) 177–254.

[11] M. J. Bremner, C. M. Dawson, J. L. Dodd, A. Gilchrist, A. W. Harrow, D. Mortimer, M. A. Nielsen, and T. J. Osborne, "Practical scheme for quantum computation with any two-qubit entangling gate," *Physical Review Letters* **89** no. 24, (Nov, 2002) 3. http://dx.doi.org/10.1103/PhysRevLett.89.247902.

[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[13] S. H. Simon, N. E. Bonesteel, M. H. Freedman, N. Petrovic, and L. Hormozi, "Topological quantum computing with only one mobile quasiparticle," *Physical Review Letters* **96** no. 7, (Feb, 2006) 4. http://dx.doi.org/10.1103/PhysRevLett.96.070503.

[14] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, "Non-abelian anyons and topological quantum computation," *Reviews of Modern Physics* **80** no. 3, (Sep, 2008) 1083–1159. http://dx.doi.org/10.1103/RevModPhys.80.1083.

[15] M. H. Freedman, M. J. Larsen, and Z. Wang, "The two-eigenvalue problem and density of jones representation of braid groups," *Communications in Mathematical Physics* **228** no. 1, (Jun, 2002) 177–199. http://dx.doi.org/10.1007/s002200200636.

[16] L. Funar, "On the tqft representations of the mapping class groups," *Pacific journal of mathematics* **188** no. 2, (1999) 251–274.

[17] V. G. Turaev, *Quantum invariants of knots and 3-manifolds*. de Gruyter, 2016.

[18] K. Walker, "On witten's 3-manifold invariants," *preprint* **116** (1991) 133.

[19] W. G. McKay and J. Patera, *Tables of dimensions, indices, and branching rules for representations of simple Lie algebras*. Dekker, 1981.