The Search For Leakage-free Entangling Fibonacci Braiding Gates

Shawn X. Cui,1,2 Kevin T. Tian,3 Jennifer F. Vasquez,4 Zhenghan Wang,3,5 Helen M. Wong6

1 Stanford Institute for Theoretical Physics, Stanford University, Stanford, CA 94305
2 Department of Mathematics, Virginia Tech, Blacksburg, VA, 24061
3 Department of Mathematics, University of California, Santa Barbara, CA 93106
4 Department of Mathematics, University of Scranton, Scranton, PA 18510
5 Microsoft Station Q, Santa Barbara, CA 93106
6 Department of Mathematical Sciences, Claremont McKenna College, Claremont, CA 91711

cuixsh@gmail.com, ktian@math.ucsb.edu, jennifer.vasquez@scranton.edu, zhenghwa@microsoft.com, hwong@cmc.edu

Abstract

It is an open question if there are leakage-free entangling Fibonacci braiding gates. We provide evidence to the conjecture for the negative in this paper. We also found a much simpler protocol to generate approximately leakage-free entangling Fibonacci braiding gates than existing algorithms in the literature.
1 Introduction

Fibonacci anyons are universal for quantum computing by braidings alone \cite{5}. They are conjectured to exist in fractional quantum Hall liquids at $\nu = \frac{12}{5}$ \cite{11}, superconductor networks \cite{9}, and Majorana networks \cite{7}. Quantum algorithms such as Shor’s factoring algorithm written for the quantum circuit model are not convenient for implementation using Fibonacci anyons because explicit qubit structure is required. Moreover, the universality proof of Fibonacci anyons only guarantees efficient approximations of two-qubit entangling gates, though this is probably adequate for all practical purposes. It has long been an interesting open question if there are leakage-free entangling Fibonacci braiding gates\footnote{We are not going to touch on any other variations of the question such as using measurements and/or ancillary states.}.

In this paper, we focus on two complementary questions: proving the non-existence of leakage-free Fibonacci entangling gates, and finding protocols to generate good approximations adequate for the experimental construction of a Fibonacci quantum computer. On the first question, we found a systematic construction of leakage-free braiding gates, which are then proved to be non-entangling. We also set up a computer search with up-to-date computing technology and found no leakage-free entangling gates either. These two results provide evidence that such leakage-free Fibonacci braiding gates do not exist. On the second question, we discovered a much simpler protocol to generate approximately leakage-free entangling Fibonacci braiding gates than algorithms in the existing literature \cite{12,2}. The time complexity of our approximation algorithm for a leakage-free entangling gate is comparable to the standard Solovay-Kitaev algorithm; however, our algorithm performs worse for the length of words. The gain in simplicity and geometric intuition justifies such a sacrifice.

After recalling some basic background on Fibonacci anyons in Sec. 2, we search for leakage-free braiding gates in Sec. 3 both analytically and numerically. In Sec. 4 we adapt the magical iteration from \cite{12} to a more general situation in order to find approximate 2-qubit leakage-free braiding gates. In the last section, we conjecture that our approximation algorithm should work for more general anyons such as those in $SU(2)_k$. We also provide a precise formulation of the tension between universality and entangling leakage-free braiding gates for anyons.

2 Background

2.1 Fibonacci Anyons

There are numerous references on topological quantum computation. See, for instance, \cite{14} among others. In particular, see \cite{4} for an explicit setup, encoding, and calculations with anyons. An anyon system, or a unitary modular tensor category, is characterized by fusion rules, $F$-matrices, $R$-matrices, topological twists, etc.
The Fibonacci anyon system is one of the most important and also the most elegant theories for topological quantum computation [5,10]. It consists of two anyon types, \(1\) and \(\tau\), where \(1\) represents the vacuum and \(\tau\) is a non-Abelian anyon\(^2\). The only nontrivial fusion rule is \(\tau \otimes \tau = 1 \oplus \tau\). For anyons \(a, b, c, d\), \((a, b, c; d)\) is called admissible if \(d\) is a total type of \(a \otimes b \otimes c\); that is, \(d\) is an outcome of fusing \(a, b,\) and \(c\). If \((a, b, c; d)\) is admissible, then the \(F\)-matrix \(F^{abc}_d\) is the \(1 \times 1\) identity matrix whenever \(a, b, c,\) or \(d\) is \(1\), and,

\[
F := F^{\tau \tau \tau}_\tau = \left( \begin{array}{cc} \phi^{-1} & \sqrt{\phi^{-1}} \\ \sqrt{\phi^{-1}} & -\phi^{-1} \end{array} \right),
\]

where \(\phi = \frac{1+\sqrt{5}}{2}\) is the golden ratio. Note that \(F\) is a real symmetric and involutary matrix. For \(R\)-symbols, we have \(R^1_a = R^{a1}_a = 1\), \(R^\tau_\tau = e^{-\frac{2\pi i}{\sqrt{5}}}\), and \(R^\tau_\tau = e^{\frac{2\pi i}{\sqrt{5}}}\). Denote by \(R = \text{diag}(R^1_\tau, R^\tau_\tau)\).

### 2.2 Encoding of a Qubit

To encode one qubit, we take three \(\tau\) particles with total type \(\tau\). The corresponding Hilbert space \(V^\tau_\tau\) (or \(\text{Hom}(\tau, \tau \otimes \tau \otimes \tau)\)) has dimension 2. We will describe two bases for \(V^\tau_\tau\) using splitting/fusion trees.

The first (splitting/fusion tree) basis for \(V^\tau_\tau\) is denoted by \(B_L\) and can be described as follows. We first split a \(\tau\) into a pair of anyons \((x, \tau)\), and then continue to split \(x\) into a pair \((\tau, \tau)\). The splitting/fusion tree for this basis is illustrated on the lefthand side of Figure 1. One can also think of the fusion process in reverse, namely, one fuses the first two \(\tau\)'s into \(x\), and then fuses \(x\) and the third \(\tau\) into \(\tau\). According to the fusion rules, \(x\) could be either \(1\) or \(\tau\). Denote by \(|x\rangle_L\) the basis element corresponding to the splitting/fusion process mentioned above. Then \(B_L := \{|1\rangle_L, |\tau\rangle_L\}\) is an orthonormal basis for \(V^\tau_\tau\).

We can encode a qubit \(\mathbb{C}^2\) in \(V^\tau_\tau\) by the map, \(|0\rangle \mapsto |1\rangle_L, |1\rangle \mapsto |\tau\rangle_L\).

Similarly, there is a different basis \(B_R\), shown on the righthand side of Figure 1 where one splits \(\tau\) into \((\tau, y)\) followed by splitting \(y\) into \((\tau, \tau)\). Again, \(y\) can be either \(1\) or \(\tau\). Denote by \(|y\rangle_R\) the corresponding the basis element and \(B_R := \{|1\rangle_R, |\tau\rangle_R\}\). Both \(B_L\) and \(B_R\) are called the computational bases for the one-qubit space \(V^\tau_\tau\). They are related by the matrix \(F\):

\[
|y\rangle_L = \sum_{x=1,\tau} F_{xy} |x\rangle_R
\]

for \(y = 1, \tau\), and where it is understood that \(F_{11} = F_{1\tau}, F_{1\tau} = F_{12}, F_{\tau 1} = F_{21},\) and \(F_{\tau \tau} = F_{22}\).

We next describe the action of the braid group. Recall that the \(n\)-strand braid group \(B_n\) has the presentation,

\[
B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \sigma_i \sigma_j = \sigma_j \sigma_i, |i - j| > 1 \rangle,
\]

\(^2\)Strictly speaking, we need to distinguish anyon types vs anyons or (quasi)-particles [17]. But for Fibonacci anyons, this difference can be safely ignored.
\[ x_L := \left\{ \begin{array}{c|c} t & t \\ \hline \hline 1 & x = 1, r \end{array} \right\} \quad \text{and} \quad y_R := \left\{ \begin{array}{c|c} t & t \\ \hline \hline 1 & y = 1, r \end{array} \right\} \]

Figure 1: Two splitting/fusion tree bases for \( V_{\tau \tau \tau} \).

\[ \sigma_{i,n} \]

Figure 2: Braid generator \( \sigma_{i,n} \)

where the convention is that \( \sigma_i \) corresponds to the braid diagram such that the \( i \)-th strand goes over the \( (i + 1) \)-th strand, as illustrated in Figure 2.

The encoding of the three \( \tau \) particles described above leads to a unitary representation of the three-strand braid group, \( \rho_3: B_3 \rightarrow U(V_{\tau \tau \tau}) \).

Denote by \( \rho_3^L(\sigma) \) (resp. \( \rho_3^R(\sigma) \)) the matrix of a braid \( \sigma \) under the basis \( B_L \) (resp. \( B_R \)). Then,

\[ \rho_3^L(\sigma_1) = \rho_3^R(\sigma_2) = R = \text{diag}(R_1^{\tau}, R_2^{\tau}), \]

\[ \rho_3^L(\sigma_2) = \rho_3^R(\sigma_1) = FRF = \begin{pmatrix} e^{\frac{2\pi i}{5}} & e^{-\frac{3\pi i}{5}} \\ e^{-\frac{3\pi i}{5}} & e^{\frac{2\pi i}{5}} \end{pmatrix} \]

Thus, under the two bases \( B_L, B_R \), the matrices of \( \sigma_1 \) and \( \sigma_2 \) are swapped. They generate the same group under either basis, so that there is essentially no difference between \( B_L \) and \( B_R \). As a default convention, by computational basis, we will take to mean \( B_L \) unless explicitly stated otherwise. The matrices \( \rho_3(\sigma) := \rho_3^L(\sigma) \) are called 1-qubit quantum gates.

It is well-known that \( \rho_3(\sigma_1) \) and \( \rho_3(\sigma_2) \) generate a dense subgroup of \( U(2) \) up to phases [5]. Interestingly, in the \( F \)-matrix of the Fibonacci theory lies in the image. Explicitly, it follows from the identities \( (RF)^3 = R_1^{\tau} I_2 \) and \( F^2 = I_2 \) that

\[ \rho_3(\sigma_1 \sigma_2 \sigma_1) = R_1^{\tau} F. \]

Moreover, [8] provides an asymptotically optimal algorithm which approximates an arbitrary unitary matrix using products of the generators \( \rho_3(\sigma_1) \) and \( \rho_3(\sigma_2) \) and characterizes the exact image of \( B_3 \) from the Fibonacci theory.

### 2.3 Encoding of 2-qubits

Let \( \text{SWAP} \in U(C^2 \otimes C^2) \) be the 2-qubit gate mapping \( |i, j\rangle \) to \( |j, i\rangle \), \( i, j = 0, 1 \). Alternatively, \( \text{SWAP} \) is the \( 4 \times 4 \) permutation matrix obtained by exchanging the second and third rows of a \( 4 \times 4 \) identity matrix.
Recall that a 2-qubit gate $U \in \mathbf{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is called non-entangling if one of the following conditions is satisfied (and the other condition will hold as a consequence).

1. $U$ is of the form $A \otimes B$ or $\text{SWAP} \circ (A \otimes B)$ for some 1-qubit gates $A, B \in \mathbf{U}(\mathbb{C}^2)$.

2. $U$ maps product states to product states. That is, for any $|x\rangle, |y\rangle \in \mathbb{C}^2$, there exist $|u\rangle, |v\rangle \in \mathbb{C}^2$ such that $U(|x\rangle \otimes |y\rangle) = |u\rangle \otimes |v\rangle$.

$U$ is called entangling otherwise. Note that the non-entangling gates form a subgroup.

All 1-qubit gates together with any entangling 2-qubit gate is universal. Hence any universal gate set for 1-qubit gates plus an entangling 2-qubit gate is a universal gate set for all qubits. This shows that entangling gates are essential for quantum computing, and in this paper, we investigate whether such entangling 2-qubit gates can arise from the Fibonacci theory.

In particular, we are concerned with the encoding of 2-qubits obtained from six $\tau$ particles from the Fibonacci theory with total type trivial. Explicitly, we group the first three $\tau$ particles to form the first qubit and group the last three to form the second qubit. We further require the total type of each group of anyons to be trivial. The resulting Hilbert space $V^\otimes_\text{6} \tau$ of six $\tau$ particles with total type trivial has dimension five. The four in Figure 3 are denoted by $|1\rangle, |1\tau\rangle, |	au1\rangle, |	au\tau\rangle$ and span the computational subspace $V^\tau_\text{C} \otimes V^\tau_\text{C}$. The element $|NC\rangle$ in Figure 4 we call the non-computational state. Thus $V^\otimes_\text{6} \tau = \text{span} \{ |NC\rangle \} \oplus V^\tau_\text{C}$.

The computational subspace $V^\tau_\text{C}$ encodes 2-qubits in the way described in Figure 3. Note that the basis $B_L$ is used for the first qubit, while $B_R$ for the second qubit. As mentioned in the previous subsection, there is essentially no difference between the two bases. The particular choice here is simply for notational convenience. To emphasize this encoding of two qubits, we will write $V^\tau_\text{C} = V^\tau_\text{C} \otimes V^\tau_\text{C}$. By braiding, we obtain a unitary representation of the six-strand braid group,

$$
\rho_6 : B_6 \rightarrow \mathbf{U}(V^\otimes_\text{6} \tau).
$$

Let $P_{14}$ be the permutation matrix obtained by exchanging the first and fourth rows of a $5 \times 5$ identity matrix. Recall that $I_2$ is the $2 \times 2$ identity matrix. By convention, the tensor product $A \otimes B$ is the matrix of the form $(a_{ij}B)$.

Direct calculation shows that the matrices of the braid group generators under the basis $\{|NC\rangle, |11\rangle, |1\tau\rangle, |	au1\rangle, |	au\tau\rangle\}$ are represented by,

$$
\rho_6(\sigma_1) = (R^T \otimes (R \otimes I_2))
$$

$$
\rho_6(\sigma_2) = (R^T \otimes (FRF \otimes I_2))
$$

$$
\rho_6(\sigma_3) = P_{14} ((R^T \otimes R \oplus FRF) P_{14})
$$

$$
\rho_6(\sigma_4) = (R^T \otimes (I_2 \otimes FRF))
$$

$$
\rho_6(\sigma_5) = (R^T \otimes (I_2 \otimes R)).
$$
Figure 3: The encoding of two qubits where $x, y = 1, \tau$.

Figure 4: The non-computational basis element.
Note that the formula for $\rho_6(\sigma_3)$ means that when restricting to the subspace $\text{span}\{|NC\rangle, |\tau\rangle\}$ it is equal to $\rho_3(\sigma_2) = FRF$. We will use this fact later in Section 4.

**Definition 2.1.** A unitary acting on $V^{\otimes 6}_\tau$ is called leakage-free if it preserves the 4-dimensional computational subspace $V_C$.

Equivalently, a unitary is leakage-free if its $(1,1)$-entry has norm equal to 1. To perform quantum computing, we need to have leakage-free gates to avoid information leakage. We also allow the states to go out of the computational subspace temporarily if they are performed in a controlled way.

In the Fibonacci 2-qubit model, if a braiding gate $\rho_6(\sigma)$ is leakage-free, then we say it is entangling if the restriction of $\rho_6(\sigma)$ on $V_C$ is entangling with respect to the decomposition $V_C = V^{\otimes 6}_\tau \otimes V^{\otimes 6}_\tau$. For example, we see from Equation [8] for the first braid generator $\sigma_1$ produces a leakage-free gate. However, it is not entangling since $\rho_6(\sigma_1)|_{V_C} = R \otimes I_2$.

It has been long suspected that, in the Fibonacci model, there are no braids that realize exactly leakage-free entangling gates. Our results in the next section support such a possibility.

### 3 Leakage-free gates

The formulas from Section 2 for the gates $\rho_6(\sigma_1)$, $\rho_6(\sigma_2)$, $\rho_6(\sigma_4)$, and $\rho_6(\sigma_5)$ immediately imply that they are leakage-free and non-entangling on $V_C$. Thus, because the non-entangling gates form a closed subgroup, any word in the braid group generators $\sigma_1, \sigma_2, \sigma_4$ and $\sigma_5$ will also be leakage-free and non-entangling. In this section we will consider two other braids, $\Delta$ and $\Sigma$, that also produce leakage-free, non-entangling gates.

![Diagram](image)

Figure 5: The half-twist $\Delta$ applied to a splitting/fusion tree.

**Lemma 3.1.** Let $\Delta = \sigma_1(\sigma_2 \sigma_1)(\sigma_3 \sigma_2 \sigma_1)(\sigma_4 \sigma_3 \sigma_2 \sigma_1)(\sigma_5 \sigma_4 \sigma_3 \sigma_2 \sigma_1)$. Then $\rho_6(\Delta) = (R_1^{\tau \tau})^3 \cdot (I_1 \oplus \text{SWAP})$

**Proof.** $\Delta$ is the half-twist, as illustrated on the left hand side in Figure 5. Isotope $\Delta$ as in the ride hand side and rewrite it as the product

$$\Delta = (\sigma_1 \sigma_2 \sigma_1) \cdot (\sigma_5 \sigma_4 \sigma_5) \cdot (\sigma_3 \sigma_2 \sigma_1)(\sigma_4 \sigma_3 \sigma_2)(\sigma_5 \sigma_4 \sigma_3).$$
Recall from Section 2 that $\rho_6(\sigma_1\sigma_2\sigma_1) = (R_{1}^{+})^3 \oplus (R_{1}^{-} F \otimes I_2)$, and $\rho_6(\sigma_5\sigma_4\sigma_3) = (R_{1}^{-})^3 \oplus (I_2 \otimes R_{1}^{+} F)$. Furthermore,

$$\rho_6(\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1) = I_1 \oplus (R_{1}^{+} (F \otimes F) SWAP)$$

With $(R_{1}^{-})^2 = R_{1}^{+}$, the formula for $\rho_6(\Delta)$ then follows immediately.

Next, we explain the topological procedure that led us to the pure braid $\Sigma = (\sigma_3\sigma_2\sigma_1)(\sigma_1\sigma_2\sigma_3)$, which yields a leakage-free gate. Start with a braid on four strands which returns the first strand to its leftmost position. Such a braid belongs in the annular braid group, which is generated by $\sigma_1^2$, $\sigma_2$, and $\sigma_3$ in $B_4$ [1]. Now replace the first strand by three parallel strands to obtain a braid on six strands, which is a product of $\Sigma$, $\sigma_4$, and $\sigma_5$ in $B_6$. Any braid obtained in this way preserves $V_C$. $\Sigma$ is illustrated in Figure 6 and a computation yields the following lemma, from which it is also easy to see that $\Sigma$ produces a non-entangling gate.

Figure 6: The pure braid $\Sigma$

**Lemma 3.2.** Let $\Sigma = (\sigma_3\sigma_2\sigma_1)(\sigma_1\sigma_2\sigma_3)$. Then $\rho_6(\Sigma) = I_1 \oplus (I_2 \otimes R^2)$

We remark that we could instead have arrived at the pure braid $\Sigma$ by starting with a braid on four strands which moves the first strand to the rightmost position, and then replacing the first strand with three parallel strands. In that case, we produce a braid on six strands that is a product of $\Sigma$, $\sigma_1$, $\sigma_5$, and $(\sigma_3\sigma_2\sigma_1)(\sigma_1\sigma_2\sigma_3)(\sigma_5\sigma_4\sigma_3)$ in $B_6$. Recall from our proof of Lemma 3.1 that $(\sigma_3\sigma_2\sigma_1)(\sigma_4\sigma_3\sigma_2)(\sigma_5\sigma_4\sigma_3)$ can be written as a product of $\Delta$, $\sigma_1$, $\sigma_2$, $\sigma_4$, and $\sigma_5$. Thus, while the resulting braid will also yield a leakage-free gate, it is one that we’ve seen already.

We summarize the above results in the following theorem.

**Theorem 3.3.** Any word $w$ in $\sigma_1, \sigma_2, \sigma_4, \sigma_5, \Delta$, and $\Sigma$ produces a gate that is leakage-free and non-entangling on the computational subspace $V_C$.

**Remark 3.4.** Topological constructions similar to used in Theorem 3.3 may be used to obtain braids which preserve subspaces other than $V_C$. Often, the braids turn out to be entangling on the complement of the preserved subspace.

In particular, to find an infinite family of braids which fixes subspace spanned by $|11\rangle$, we may start with a pure braid on three strands and double every strand. We may further take products with $\sigma_1, \sigma_2, \sigma_4, \sigma_5$, and $\Delta$, and still obtain...
gates which fix $|11\rangle$ up to a phase. Interestingly, unlike the situation with the non-computational $|NC\rangle$, many of the gates that fix $|11\rangle$ up to a phase are entangling on the complementary 4-dimensional subspace. For example, it can be shown that $\rho_6((\sigma_2\sigma_3)^3)$ fixes $|11\rangle$ up to a phase, does not fix $|NC\rangle$, and is entangling on the basis elements $|NC\rangle$, $|1\tau\rangle$, $|\tau 1\rangle$ and $|\tau \tau\rangle$.

To obtain braids that fix $|1\tau\rangle$ and $|\tau 1\rangle$, choose a annular braid on five strands and double the first or last. As above, many of the resulting gates are entangling on the complementary 4-dimensional subspace. For example, $\rho_6((\sigma_2\sigma_3)^3)$ fixes $|1\tau\rangle$ up to a phase, does not fix $|NC\rangle$, and is entangling on the basis elements $|NC\rangle$, $|11\rangle$, $|1\tau\rangle$ and $|\tau \tau\rangle$.

Although it is easy to find braids that fix $|11\rangle$, $|1\tau\rangle$ and $|\tau 1\rangle$, we do not know of any gate which fixes $|\tau \tau\rangle$ up to a phase, except for $\rho_6(\Delta)$.

### 3.1 Systematic computer search

To help find leakage-free entangling gates, we performed a computer search by enumerating elements of the braid group and computing their corresponding matrices in the representation given in Section 2. Then we checked whether it was leakage-free, and whether it was entangling.

We enumerated the elements of the braid group $B_6$ by taking words consisting of the generators and their inverses. We excluded trivial cases of a generator appearing adjacent to its inverse.

Due to exponential growth rate of the number of words of a given length, our search only reached words of length 7, and no leakage-free entangling gates were found.

### 4 Approximate Leakage-free Entangling Braid- ing Gates

In this section, we provide a simple procedure which approximates certain leakage-free entangling gates with braidings to arbitrary precision.

#### 4.1 Braiding gates preserving $\text{span}\{|NC\rangle, |\tau \tau\rangle\}$

For the 6-anyon encoding of two qubits as shown in Figures 3 and 4, we consider braiding gates that preserve the subspace $V := \text{span}\{|NC\rangle, |\tau \tau\rangle\}$. Let $V^\perp = \text{span}\{|11\rangle, |1\tau\rangle, |\tau 1\rangle\}$.

First, consider the braid $\sigma_2\sigma_1\sigma_2$, which is represented as in Figure 7, where the equality is obtained by isotopy of braids. Then direct computation shows that with respect to the decomposition $V \oplus V^\perp$,

$$\rho_6(\sigma_2\sigma_1\sigma_2) = \rho_3(\sigma_1^2) \oplus \text{diag}(1, 1, (R_\tau^\tau)^2).$$

Similarly,

$$\rho_6(\sigma_4\sigma_5\sigma_4) = \rho_3(\sigma_1^2) \oplus \text{diag}(1, (R_\tau^\tau)^2, 1).$$
Figure 7: The braid $\sigma_2 \sigma_1 \sigma_2$ applied to a splitting/fusion tree

It can also be verified that $\rho_6(\sigma_3)$ preserves the decomposition $V \oplus V^\perp$, where

$$\rho_6(\sigma_3) = \rho_3(\sigma_2) \oplus \text{diag}(R_1^\tau, R_2^\tau, R_3^\tau).$$  \hspace{1cm} (15)

Hence, through braidings from the 6-anyon encoding of two qubits, we can obtain all of the group of gates generated by $\{\rho_3(\sigma_1^2), \rho_3(\sigma_2)\}$ on $V$. We do not know if this group contains all the possible braiding gates on $V$. However, Proposition 4.1 below implies that $\{\rho_3(\sigma_1^2), \rho_3(\sigma_2)\}$ is already a universal gate set on $V$.

In particular, recall the well-known result that $\{\rho_3(\sigma_1), \rho_3(\sigma_2)\}$ generates a dense subgroup of $\text{SU}(2)$ up to phases [5]. We prove a stronger result in the following proposition.

**Proposition 4.1.** Let $\rho_3(\sigma_1) = \rho_3^L(\sigma_1)$, $\rho_3(\sigma_2) = \rho_3^L(\sigma_2)$ be the 1-qubit gates given in Equations 5, 6. Then $\{\rho_3(\sigma_1^2), \rho_3(\sigma_2)\}$ generate a dense subgroup of $\text{SU}(2)$ up to global phases.

**Proof.** Let $U_1, U_2 \in \text{SU}(2)$. By the classification of subgroups of $\text{SU}(2)$, if $U_1$ and $U_2$ have infinite order and they do not commute up to phases, then $\{U_1, U_2\}$ generate a dense subgroup of $\text{SU}(2)$. Take $U_1 = \rho_3(\sigma_1^2\sigma_2^4)$, $U_2 = \rho_3^{-1}(\sigma_1^2\sigma_2^6)$. Then it is straightforward to check $U_1$ and $U_2$ do not commute.

To show that they have infinite order, we show that their eigenvalues are not $m$-th roots of unity for any integer $m$, or equivalently that their real parts are not the cosine of a rational multiple of $\pi$. Normalizing determinants to equal 1, the real part of the eigenvalues of $e^{i\pi/10} \rho_3(\sigma_1^2\sigma_2^4)$ and $e^{i\pi/10} \rho_3^{-1}(\sigma_1^2\sigma_2^6)$ are given (respectively) by:

$$\frac{-2 + \sqrt{5}}{2} \text{ and } \frac{-3 + \sqrt{5}}{2}$$

Neither real part given above is the value of cosine at a rational multiple of $\pi$, and thus it follows from [15] that both elements are infinite order. \hfill $\Box$

In Section 4.3, we will combine the fact that $\{\rho_3(\sigma_1^2), \rho_3(\sigma_2)\}$ is a universal gate set on $V$ together with some techniques developed in Section 4.2 to provide a simple scheme to approximate certain 2-qubit leakage-free, entangling gates using braidings.
4.2 Iteration to diagonal gates

Let $D \in U(2)$ be any diagonal gate and write it as $D = \gamma \text{diag}(e^{-i\frac{\theta}{2}}, e^{i\frac{\theta}{2}})$ for $-\pi \leq \theta \leq \pi$ and $\gamma \in U(1)$. The phase $\gamma$ will not play a role below, so we also write $D = D(\theta)$. Let $U_0 \in U(2)$ be any 1-qubit gate. Consider the sequence $\{U_k\}_{k=0}^{\infty}$ defined inductively by the formula:

$$U_{k+1} = U_k \cdot D(\theta) \cdot U_k^{-1} \cdot D(\theta) \cdot U_k \cdot D(\theta)^{-2} \quad (16)$$

Obviously, $U_k$ does not depend on the phase $\gamma$. For $\theta = 0$, then $U_k = U_0$ for all $k$.

**Lemma 4.2.** If $-\frac{\pi}{2} < \theta < \frac{\pi}{2}$, $\theta \neq 0$, and $|(U_0)_{12}| < 1$, then the sequence $\{U_k\}$ defined in Equation (16) converges to a diagonal gate.

**Proof.** It suffices to consider the case $U_0 \in SU(2)$ since by Equation (16), if $U_k$ has a global phase, then $U_{k+1}$ has the same global phase.

Let $\lambda = e^{i\bar{\theta}}$, $\delta = |(U_0)_{12}| < 1$, and

$$U_k = \left( \begin{array}{cc} a_k & -\bar{b}_k \\ b_k & \bar{a}_k \end{array} \right). \quad (17)$$

We first show that there exists $\epsilon = \epsilon(\theta, \delta) < 1$ such that $|b_{k+1}| \leq \epsilon|b_k|$, which implies that $\{|b_k|\}$ converges to 0. By direct calculation,

$$|b_{k+1}| = |b_k|y_k,$$

where

$$y_k = |(1 - |b_k|^2)(1 - \lambda + \lambda^2) + |b_k|^2\lambda| \quad (18)$$

$$= |(\lambda + \bar{\lambda} - 2)(1 - |b_k|^2) + 1| \quad (19)$$

$$= |(2 - 2\cos(\theta))(1 - |b_k|^2) - 1|. \quad (20)$$

It is clear that $y_k \leq 1$. Hence $|b_{k+1}| \leq |b_k| \leq \delta$. In turn, setting $\epsilon := \max\{|1 - 2\cos(\theta)|, (2 - 2\cos(\theta))(1 - \delta^2) - 1\}$, we have $y_k \leq \epsilon$. By our assumption on $\theta$, both of the two expressions in max{·,·} are strictly less than one, and hence $\epsilon < 1$.

That $|b_{k+1}| \leq \epsilon|b_k|$ implies the statement in the lemma. Intuitively, when $k$ gets large, $U_k$ is close to a diagonal gate, and hence approximately commutes with $D(\theta)$. By Equation (16), $U_{k+1}$ would be approximately equal to $U_k$. The following is a more elementary argument. Again by direct calculations,

$$a_{k+1} = a_k(1 - |b_k|^2)(\lambda - 1)^2). \quad (21)$$

Hence,

$$|a_{k+1} - a_k| = |a_k| \cdot |\lambda - 1|^2 \cdot |b_k|^2 \leq c\epsilon^{2k} \quad (22)$$

for some constant $c > 0$, which implies that the sequence $\{a_k\}$ converges. □
A few remarks are in order.

**Remark 4.3.** For \( \theta = \frac{\pi}{3} \), by Equation 18, we have \( y_k = |b_k|^2 \) and hence \( |b_{k+1}| = |b_k|^3 \). In this case, the sequence \( \{b_k\} \) converges to 0 exponentially faster than it does for a general \( \theta \) as in the proof of Lemma 4.2. The formula in Equation 16 for \( \theta = \frac{\pi}{2} \) was used in [13] as a scheme to approximate certain diagonal gates. To be precise, the formula in [13] does not have the \( 'D^{-2} \) factor as in Equation 16. This does not change the fact that the off-diagonal entries of \( U_k \) converges to zero. However, without the \( 'D^{-2} \) factor, the \( \{U_k\} \) sequence does not converge to a diagonal gate, but rather fluctuates among several diagonal gates which differ by some powers of \( D \) from each other.

**Remark 4.4.** In [12, 2], a formula different from that in Equation 16 was provided to give rise to a sequence \( \{U_k\} \) which converges at an even higher rate: \( |(U_{k+1})_{1,2}| = |(U_k)_{1,2}|^5 \) for \( \theta = \frac{\pi}{2} \). However, their formula does not apply here. This is because \( D\left(\frac{\pi}{2}\right) = \rho(\sigma_1)^3 \) up to phases, and as will be seen in Section 4.3, we will give a scheme to approximate 2-qubit entangling gates with braids that preserve the subspace \( V := \text{span}\{\{NC\}, |\tau\tau\}\} \). However, the braids that preserve the subspace \( V \) do not seem to realize the gate \( \rho(\sigma_1)^3 \) on \( V \), but only \( \rho(\sigma_1)^2 \) instead.

**Remark 4.5.** There is a geometric interpretation of the formula in Equation 16. If we think of a 1-qubit gate \( U \in \text{SU}(2) \) as a rotation in \( \mathbb{R}^3 \), then \( D(\theta) \) is a rotation around the \( z \)-axis by the angle \( \theta \). A unitary \( U \) has an axis in the \( xy \)-plane if and only if its \((1, 2)\)-entry has norm one. Then by Lemma 4.2, as long as \( \theta \) has absolute value strictly between 0 and \( \frac{\pi}{2} \) and the axis of \( U_0 \) is not in the \( xy \)-plane, then each iteration in Equation 16 brings the axis of \( U_k \) closer to the \( z \)-axis. In the limit, \( U_k \) becomes a rotation around the \( z \)-axis.

### 4.3 Approximation of 2-qubit Leakage-free Entangling Braiding Gates

We provide a scheme to approximate certain 2-qubit leakage-free entangling gates with braiding. Of course, since the Fibonacci model is universal, one can in principle approximate arbitrary \( n \)-qubit gates using (for instance) the Solovay-Kitaev algorithm. However, the procedure we give is more explicit and simpler.

We use the braiding gates from \( G := \langle \rho_0(\sigma_2\sigma_1\sigma_1\sigma_2), \rho_0(\sigma_3) \rangle \) for the approximation. Recall that \( V = \text{span}\{\{NC\}, |\tau\tau\}\} \), \( V^\perp = \text{span}\{\{11\}, |\tau\rangle, |\tau1\}\} \), and that gates in \( G \) all preserve \( V \). Choose any gate \( \tilde{U}_0 \) and a diagonal gate \( \tilde{D} \in G \) such that \( \tilde{D} := \tilde{D}|_V \) and \( \tilde{U}_0 := \tilde{U}_0|_V \) satisfy the conditions in Lemma 4.2. We then obtain a sequence of gates \( \{\tilde{U}_k\} \) by the formula in Equation 16 starting from \( \tilde{U}_0 \) and \( \tilde{D} \). Note that \( \tilde{U}_k = \tilde{U}_0 \) on \( V^\perp \) for all \( k \)'s. By Lemma 4.2, \( \{\tilde{U}_k\} \) converges to some \( \tilde{U} \) such that \( \tilde{U}|_V \) is a diagonal gate and \( \tilde{U}|_{V^\perp} = \tilde{U}_0|_{V^\perp} \) is also a diagonal gate. Hence \( \tilde{U} \) is a leakage-free diagonal gate. In general it is straightforward to check whether \( \tilde{U} \) is entangling for each particular choice of \( \tilde{D} \) and \( \tilde{U}_0 \) since \( \tilde{U} \) agrees with \( \tilde{U}_0 \) on \( V^\perp \). If \( \tilde{U} = \text{diag}(\lambda_{-1}, \lambda_0, \lambda_1, \lambda_2, \lambda_3) \)
under the basis \{|NC\rangle, |11\rangle, |1\tau\rangle, |\tau 1\rangle\}, then \(\tilde{U}\) is entangling if and only if \(\lambda_3 \neq \lambda_1 \lambda_2 \lambda_0^{-1}\).

**Theorem 4.6.** Let \(\tilde{D} = \rho_0(\sigma_2 \sigma_1 \sigma_1 \sigma_2)^3\), \(\tilde{U}_0 = \rho_0(\sigma_3)\). Then the limit of the sequence \(\{\tilde{U}_k\}\) defined by Equation (16) exists and its limit \(\tilde{U}\) is a leakage-free entangling 2-qubit gate.

**Proof.** With respect to the decomposition \(V \oplus V^\perp\), we have

\[
\tilde{D} = e^{-\frac{2\pi i}{5}} \left( \begin{array}{cc} e^{-\frac{\pi i}{2}} & 0 \\ 0 & e^{\frac{\pi i}{2}} \end{array} \right) \oplus \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{-\frac{2\pi i}{5}} \end{array} \right)
\]

\[
\tilde{U}_0 = \left( \begin{array}{ccc} e^{\frac{2\pi i}{5} \phi^{-1}} & e^{-\frac{2\pi i}{5} \sqrt{\phi^{-1}}} & 0 \\ e^{-\frac{2\pi i}{5} \sqrt{\phi^{-1}}} & e^{\frac{2\pi i}{5} \phi^{-1}} & 0 \\ 0 & 0 & e^{\frac{2\pi i}{5}} \end{array} \right) \oplus \left( \begin{array}{ccc} 0 & 0 & 0 \\ 0 & e^{\frac{2\pi i}{5}} & 0 \\ e^{-\frac{2\pi i}{5}} & 0 & 0 \end{array} \right)
\]

The angle of \(\tilde{D}|_V\) is \(\theta = \frac{2\pi}{5} < \frac{\pi}{2}\), and the \((1,2)\)-entry of \(\tilde{U}_0|_V\) (that is, the \((1,5)\)-entry of \(\tilde{U}_0\)) has absolute value \(\sqrt{\phi^{-1}} \approx 0.786 < 1\). Hence the conditions in Lemma 4.2 are satisfied. \(\tilde{U}\) is entangling if and only if \(\tilde{U}_{5,5} \neq 1\), which can be checked numerically. \(\square\)

## 5 SU(2)_k anyons

As a modular tensor category, the Fibonacci theory Fib is a sub category of the anyon theory \(\text{SU}(2)_3\) whose anyon types are given by \{0, 1, 2, 3\}. Explicitly, the correspondence is \(1 \leftrightarrow 0\), \(\tau \leftrightarrow 2\). Moreover, \{0, 3\} forms the semion theory \(S\) and \(\text{SU}(2)_3 = \text{Fib} \otimes S\). Also note that semion \(S\) is an Abelian theory and \(1 = 2 \otimes 3 = 2 \otimes 3\). Then an important observation is as follows. In the encoding of one- and two-qubit models (Section 2.3), if we replace all the anyons of type \(\tau\) (i.e., type 2) by anyons of type 1, then the braiding gates remain the same up to (irrelevant) global phases which are contributed by the semion theory. This means that for anyons of type 1, all the results discussed in the paper still hold.

Now for the sequence of anyon theories \(\text{SU}(2)_k\), for \(k \geq 2\) with anyon types \{0, 1, \cdots, k\}, exactly the same models of one and two qubits (and more generally \(n\)-qubits) as in Section 2 can be defined with type 1 anyons. It is known that the type 1 anyon in \(\text{SU}(2)_k\) is braiding universal if and only if \(k = 3\) or \(k \geq 5\). We believe that the results presented in this paper still hold for \(k \geq 5\). For instance, \(\{\rho_3(\sigma_2^2), \rho_3(\sigma_2^2)\}\) generates a dense subgroup of \(\text{SU}(2)\). Also, the method for approximating entangling leakage-free 2-qubit gates in earlier sections also applies.

### 5.1 A Conjecture

Let \(C\) be an anyon theory, namely, a unitary modular tensor category, and \(a, b, c \in C\) be anyon types. Assume \(c\) is a total type of \((b, b)\). Consider the
embedding $V_b^a \otimes V_b^a \subset V_c^a \otimes 2^n$ for some $n > 1$. See Figure 8. We treat each $V_b^a$ as a qudit space. We call an anyon type $a$ to have the property of entangling leakage-free if for some $n > 1$ and anyon types $b, c$, there exists a braid $\sigma \in B_{2n}$ such that the representation of $\sigma$ on $V_c^a \otimes 2^n$ preserves, and is entangling on, the subspace $V_b^a \otimes V_b^a$.

By the results in this paper, we believe that the Fibonacci anyon (or the type 1 anyon$^3$ in SU$_2(2)$) does not have the property of entangling leakage-free. On the other hand, the type 1 anyon in SU$_2(2)_k$ does have the property of entangling leakage-free for $k = 2$ and $k = 4$ [17, 3]. Thus there seems to be a tension between braiding universality and the property of entangling leakage-free.

Conjecture 5.1. An anyon type has the property of entangling leakage-free if and only if the braid group representations of $B_n$ associated with it have finite images for all $n \geq 1$.

The anyon of type 1 of SU$_2(2)_8$ has finite images for $B_3$ and $B_4$, but infinite images for all $B_n, n \geq 5$ [6].

By the Property F conjecture [10], we can also formulate the above as:

Conjecture 5.2. An anyon type has the property of entangling leakage-free if and only if its quantum dimension is the square root of an integer.

Acknowledgement: K.T. and Z.W. are partially supported by NSF grant FRG-1664351, and H.W. by DMS-1841221. S.C. acknowledges the support from the Simons Foundation. All authors thank the IAS School of Mathematics for their support during Summer 2018, where the project started and most of the results were obtained.

References

[1] Joan S Birman. Braids, Links, and Mapping Class Groups. (AM-82), volume 82. Princeton University Press, 2016.

$^3$spin 1/2 in physics parlance.
[2] Caitlin Carnahan, Daniel Zeuch, and NE Bonesteel. Systematically generated two-qubit anyon braids. Physical Review A, 93(5):052328, 2016.

[3] Shawn X Cui and Zhenghan Wang. Universal quantum computation with metaplectic anyons. Journal of Mathematical Physics, 56(3):032202, 2015.

[4] Colleen Delaney, Eric C Rowell, and Zhenghan Wang. Local unitary representations of the braid group and their applications to quantum computing. Revista Colombiana de Matemáticas, 50(2):211–276, 2016.

[5] Michael H Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. Communications in Mathematical Physics, 227(3):605–622, 2002.

[6] Michael H Freedman, Michael J Larsen, and Zhenghan Wang. The two-eigenvalue problem and density of Jones representation of braid groups. Communications in mathematical physics, 228(1):177–199, 2002.

[7] Yichen Hu and CL Kane. Fibonacci topological superconductor. Physical review letters, 120(6):066801, 2018.

[8] Vadym Kliuchnikov, Alex Bocharov, and Krysta M Svore. Asymptotically optimal topological quantum compiling. Physical review letters, 112(14):140504, 2014.

[9] Roger SK Mong, David J Clarke, Jason Alicea, Netanel H Lindner, Paul Fendley, Chetan Nayak, Yuval Oreg, Ady Stern, Erez Berg, Kirill Shtengel, et al. Universal topological quantum computation from a superconductor-abelian quantum Hall heterostructure. Physical Review X, 4(1):011036, 2014.

[10] Deepak Naidu and Eric C Rowell. A finiteness property for braided fusion categories. Algebras and representation theory, 14(5):837–855, 2011.

[11] Nicholas Read and E Rezayi. Beyond paired quantum Hall states: Parafermions and incompressible states in the first excited Landau level. Physical Review B, 59(12):8084, 1999.

[12] Ben W Reichardt. Systematic distillation of composite fibonacci anyons using one mobile quasiparticle. Quantum Information & Computation, 12(9-10):876–892, 2012.

[13] Ben W Reichardt and Lov K Grover. Quantum error correction of systematic errors using a quantum search framework. Physical Review A, 72(4):042326, 2005.

[14] Eric Rowell and Zhenghan Wang. Mathematics of topological quantum computing. Bulletin of the American Mathematical Society, 55(2):183–238, 2018.
[15] Pinthira Tangsupphathawat. Algebraic trigonometric values at rational multipliers of $\pi$. *Acta et Commentationes Universitatis Tartuensis de Mathematica*, 18(1):9–18, 2014.

[16] Simon Trebst, Matthias Troyer, Zhenghan Wang, and Andreas WW Ludwig. A short introduction to fibonacci anyon models. *Progress of Theoretical Physics Supplement*, 176:384–407, 2008.

[17] Zhenghan Wang. *Topological quantum computation*. Number 112. American Mathematical Soc., 2010.