Journal of Physics A: Mathematical and Theoretical

PAPER

The search for leakage-free entangling Fibonacci braiding gates

To cite this article: Shawn X Cui *et al* 2019 *J. Phys. A: Math. Theor.* **52** 455301

View the article online for updates and enhancements.

IOP | ebooks™

Bringing together innovative digital publishing with leading authors from the global scientific community.

Start exploring the collection–download the first chapter of every title for free.

This content was downloaded from IP address 128.210.126.199 on 13/09/2020 at 04:42

IOP Publishing Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. **52** (2019) 455301 (14pp) https://doi.org/10.1088/1751-8121/ab488e

The search for leakage-free entangling Fibonacci braiding gates

Shawn X Cui[1,2,7], Kevin T Tian[3], Jennifer F Vasquez[4], Zhenghan Wang[3,5] and Helen M Wong[6]

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

E-mail: cui177@purdue.edu, ktian@math.ucsb.edu, jennifer.vasquez@scranton.edu, zhenghwa@microsoft.com and hwong@cmc.edu

Received 2 April 2019, revised 16 August 2019
Accepted for publication 27 September 2019
Published 11 October 2019

Abstract

It is an open question if there are leakage-free entangling Fibonacci braiding gates. In this article, we give a construction of a large family of leakage-free braiding gates which are then proved to be non-entangling. We also conducted brute-force numerical searches for braids with a word-length up to seven and found no leakage-free entangling gates. These suggest the negative for the conjecture. On the other hand, we provide a much simpler protocol to generate approximately leakage-free entangling Fibonacci braiding gates than existing algorithms in the literature.

Keywords: Fibonacci anyon, braiding gate, leakage free, entangling

1. Introduction

Fibonacci anyons are universal for quantum computing by braidings alone [7]. They are conjectured to exist in fractional quantum Hall liquids at $\nu = \frac{12}{5}$ [14], superconductor networks [12], and Majorana networks [9]. Quantum algorithms such as Shor's factoing algorithm written

[7] Present affiliation: Department of Mathematics and Department of Physics and Astronomy, Purdue University, West Lafayette, IN 47906

1751-8121/19/455301+14$33.00 © 2019 IOP Publishing Ltd Printed in the UK

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[8].

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 and found no leakage-free entangling gates either. These two results suggest 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 [2, 15]. 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.

Leakage-free entangling gates are known to exist in several models such the Ising theory (or its cousin $\mathbf{SU}(2)_2$), $\mathbf{SU}(2)_4$ [3], and the quantum double of $\mathrm{Rep}(S_3)$ [4], all of which are not braiding universal. In particular, the Ising theory is currently the most promising model that can be realized experimentally such as the Majorana Zero Mode in semiconductor-superconductor heterostructures (see for instance [11] and references therein). However, the more powerful Fibonacci anyons do not seem to support leakage-free entangling gates. This suggests a tension between braiding universality and the existence of leakage-free entangling gates. See conjecture 5.1.

After recalling some basic background on Fibonacci anyons in section 2, we search for leakage-free braiding gates in section 2 both analytically and numerically. In section 3, we adapt the magical iteration from [15] to a more general situation in order to find approximate two-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 $\mathbf{SU}(2)_k$. 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, [17] among others. In particular, see [6] 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 [7, 19]. It consists of two anyon types, $\mathbf{1}$ and τ, where $\mathbf{1}$ represents the vacuum and τ is a non-Abelian anyon[9]. The only nontrivial fusion rule is $\tau \otimes \tau = \mathbf{1} \oplus \tau$. For anyons $a,\ b,\ c,\ d$, $(a, b, c; d)$ is called admissible if d is a total type of

[8] We are not going to touch on any other variations of the question such as using measurements and/or ancillary states.

[9] Strictly speaking, we need to distinguish anyon types versus anyons or (quasi)-particles [20]. But for Fibonacci anyons, this difference can be safely ignored.

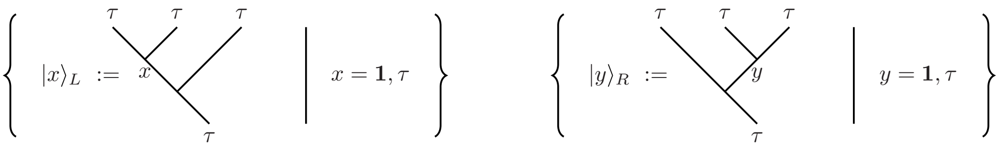

Figure 1. Two splitting/fusion tree bases for $V_\tau^{\tau\tau\tau}$.

$a \otimes b \otimes c$; that is, d is an outcome of fusing a, b, and c. If $(a, b, c; d)$ is admissible, then the F-matrix F_d^{abc} is the 1×1 identity matrix whenever $a,\ b,\ c$, or d is $\mathbf{1}$, and,

$$F := F_\tau^{\tau\tau\tau} = \begin{pmatrix} \phi^{-1} & \sqrt{\phi^{-1}} \\ \sqrt{\phi^{-1}} & -\phi^{-1} \end{pmatrix}, \tag{1}$$

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 $R_a^{\mathbf{1}a} = R_a^{a\mathbf{1}} = 1,\ R_{\mathbf{1}}^{\tau\tau} = \mathrm{e}^{-\frac{4\pi\mathrm{i}}{5}}$, and $R_\tau^{\tau\tau} = \mathrm{e}^{\frac{3\pi\mathrm{i}}{5}}$. Denote by $R = \mathrm{diag}(R_{\mathbf{1}}^{\tau\tau}, R_\tau^{\tau\tau})$.

2.2. Encoding of a qubit

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

The first (splitting/fusion tree) basis for $V_\tau^{\tau\tau\tau}$ is denoted by $\mathcal{B}_L$ and can be described as follows. We first split a τ into a pair of anyons (x, τ), and then continue to split x into a pair (τ, τ). 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 τ 's into x, and then fuses x and the third τ into τ. According to the fusion rules, x could be either $\mathbf{1}$ or τ. Denote by $|x\rangle_L$ the basis element corresponding to the splitting/fusion process mentioned above. Then $\mathcal{B}_L := \{|\mathbf{1}\rangle_L, |\tau\rangle_L\}$ is an orthonormal basis for $V_\tau^{\tau\tau\tau}$. We can encode a qubit $\mathbb{C}^2$ in $V_\tau^{\tau\tau\tau}$ by the map, $|0\rangle \mapsto |\mathbf{1}\rangle_L, |1\rangle \mapsto |\tau\rangle_L$.

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

$$|y\rangle_L = \sum_{x=\mathbf{1},\tau} F_{xy} |x\rangle_R \tag{2}$$

for $y = \mathbf{1}, \tau$, and where it is understood that $F_{\mathbf{1}\mathbf{1}} = F_{11}$, $F_{\mathbf{1}\tau} = F_{12}$,$F_{\tau\mathbf{1}} = F_{21}$, 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,

$$B_n = \langle \sigma_1, \cdots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i, |i-j| > 1\rangle, \tag{3}$$

where the convention is that σ_i corresponds to the braid diagram such that the ith strand goes over the $(i+1)$th strand, as illustrated in figure 2.

The encoding of the three τ particles described above leads to a unitary representation of the three-strand braid group,

$$\rho_3\colon B_3 \longrightarrow \mathbf{U}(V_\tau^{\tau\tau\tau}). \tag{4}$$

Denote by $\rho_3^L(\sigma)$ (resp. $\rho_3^R(\sigma)$) the matrix of a braid σ under the basis $\mathcal{B}_L$ (resp. $\mathcal{B}_R$). Then,

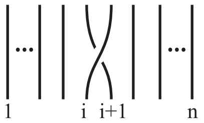

Figure 2. Braid generator $\sigma_{i,n}$.

$$\rho_3^L(\sigma_1) = \rho_3^R(\sigma_2) = R = \mathrm{diag}(R_{\mathbf{1}}^{\tau\tau}, R_{\tau}^{\tau\tau}), \tag{5}$$

$$\rho_3^L(\sigma_2) = \rho_3^R(\sigma_1) = FRF = \begin{pmatrix} \mathrm{e}^{\frac{4\pi\mathrm{i}}{5}}\phi^{-1} & \mathrm{e}^{-\frac{3\pi\mathrm{i}}{5}}\sqrt{\phi^{-1}} \\ \mathrm{e}^{-\frac{3\pi\mathrm{i}}{5}}\sqrt{\phi^{-1}} & -\phi^{-1} \end{pmatrix}. \tag{6}$$

Thus, under the two bases $\mathcal{B}_L, \mathcal{B}_R$, the matrices of σ_1 and σ_2 are swapped. They generate the same group under either basis, so that there is essentially no difference between $\mathcal{B}_L$ and $\mathcal{B}_R$. As a default convention, by computational basis, we will take to mean $\mathcal{B}_L$ unless explicitly stated otherwise. The matrices $\rho_3(\sigma) := \rho_3^L(\sigma)$ are called one-qubit quantum gates.

It is well-known that the $\rho_3(\sigma_1)$ and $\rho_3(\sigma_2)$ generate a dense subgroup of $\mathbf{U}(2)$ up to phases [7]. Interestingly, in the F-matrix of the Fibonacci theory lies in the image. Explicitly, it follows from the identities $(RF)^3 = R_{\mathbf{1}}^{\tau\tau} I_2$ and $F^2 = I_2$ that

$$\rho_3(\sigma_1\sigma_2\sigma_1) = R_{\mathbf{1}}^{\tau\tau} F.$$

Moreover, [10] 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 two-qubits

Let SWAP $\in \mathbf{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be the two-qubit gate mapping $|i, j\rangle$ to $|j, i\rangle$, $i, j = 0, 1$. Alternatively, SWAP is the 4×4 permutation matrix obtained by exchanging the second and third rows of a 4×4 identity matrix.

Recall that a two-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 SWAP $\circ$ $(A \otimes B)$ for some one-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 one-qubit gates together with any entangling two-qubit gate is universal. Hence any universal gate set for one-qubit gates plus an entangling two-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 two-qubit gates can arise from the Fibonacci theory.

In particular, we are concerned with the encoding of two-qubits obtained from six τ particles from the Fibonacci theory with total type trivial. Explicitly, we group the first three τ 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 $V_{\mathbf{1}}^{\tau^{\otimes 6}}$ of six τ particles with total type trivial has dimension five. The four in figure 3 are denoted by

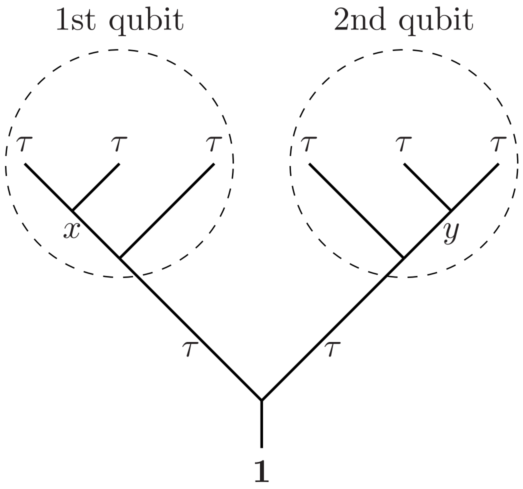

Figure 3. The encoding of two qubits where $x, y = \mathbf{1}, \tau$.

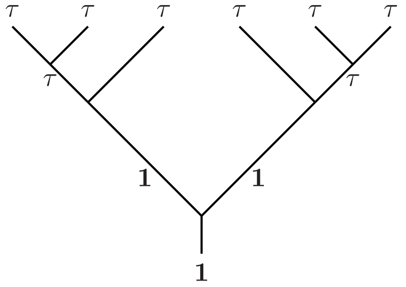

Figure 4. The non-computational basis element.

$|\mathbf{11}\rangle, |\mathbf{1}\tau\rangle, |\tau\mathbf{1}\rangle, |\tau\tau\rangle$ and span the *computational subspace* V_C. The element $|NC\rangle$ in figure 4 we call the *non-computational state*. Thus $V_{\mathbf{1}}^{\tau^{\otimes 6}} = \text{span}\{|NC\rangle\} \oplus V_C$.

The computational subspace V_C encodes two-qubits in the way described in figure 3. Note that the basis $\mathcal{B}_L$ is used for the first qubit, while $\mathcal{B}_R$ 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 $V_C = V_\tau^{\tau\tau\tau} \otimes V_\tau^{\tau\tau\tau}$.

By braiding, we obtain a unitary representation of the six-strand braid group,

$$\rho_6 \colon B_6 \longrightarrow \mathbf{U}(V_\tau^{\tau^{\otimes 6}}). \tag{7}$$

Let P_{14} be the permutation matrix obtained by exchanging the first and fourth rows of a 5×5 identity matrix. Recall that I_2 is the 2×2 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 $\{|NC\rangle, |\mathbf{11}\rangle, |\mathbf{1}\tau\rangle, |\tau\mathbf{1}\rangle, |\tau\tau\rangle\}$ are represented by,

$$\rho_6(\sigma_1) = (R_\tau^{\tau\tau}) \oplus (R \otimes I_2) \tag{8}$$

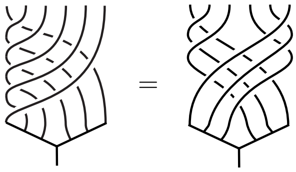

Figure 5. The half-twist Δ applied to a splitting/fusion tree.

$$\rho_6(\sigma_2) = (R_{\tau}^{\tau\tau}) \oplus (FRF \otimes I_2) \tag{9}$$

$$\rho_6(\sigma_3) = P_{14}\,((R_{\tau}^{\tau\tau}) \oplus R \oplus FRF)\,P_{14} \tag{10}$$

$$\rho_6(\sigma_4) = (R_{\tau}^{\tau\tau}) \oplus (I_2 \otimes FRF) \tag{11}$$

$$\rho_6(\sigma_5) = (R_{\tau}^{\tau\tau}) \oplus (I_2 \otimes R). \tag{12}$$

Note that the formula for $\rho_6(\sigma_3)$ means that when restricting to the subspace span$\{|NC\rangle, |\tau\tau\rangle\}$ 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 $V_{\tau}^{\tau^{\otimes 6}}$ is called *leakage-free* if it preserves the 4-dimensional (4D) 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 two-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 $V_C = V_{\tau}^{\tau\tau\tau} \otimes V_{\tau}^{\tau\tau\tau}$. For example, we see from equation (8) for the first braid generator σ_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 σ_5 will also be leakage-free and non-entangling. In this section we will consider two other braids, Δ and Σ, that also produce leakage-free, non-entangling gates.

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*

$$\rho_6(\Delta) = (R_{\mathbf{1}}^{\tau\tau})^3 \cdot (I_1 \oplus \mathrm{SWAP}).$$

Proof. Δ is the half-twist, as illustrated on the left hand side in figure 5. Isotope Δ as in the ride hand side and rewrite it as the product

$$\Delta = (\sigma_1\sigma_2\sigma_1) \cdot (\sigma_5\sigma_4\sigma_5) \cdot (\sigma_3\sigma_2\sigma_1)(\sigma_4\sigma_3\sigma_2)(\sigma_5\sigma_4\sigma_3).$$

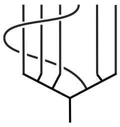

Figure 6. The pure braid Σ.

Recall from section 2 that $\rho_6(\sigma_1\sigma_2\sigma_1) = (R^{\tau\tau}_\tau)^3 \oplus (R^{\tau\tau}_{\mathbf{1}} F \otimes I_2)$, and $\rho_6(\sigma_5\sigma_4\sigma_5) = (R^{\tau\tau}_\tau)^3 \oplus (I_2 \otimes R^{\tau\tau}_{\mathbf{1}} F)$. Furthermore,

$$\rho_6((\sigma_3\sigma_2\sigma_1)(\sigma_4\sigma_3\sigma_2)(\sigma_5\sigma_4\sigma_3)) = I_1 \oplus (R^{\tau\tau}_{\mathbf{1}}(F \otimes F)\mathrm{SWAP}).$$

With $(R^{\tau\tau}_\tau)^2 = R^{\tau\tau}_{\mathbf{1}}$, 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 σ_1^2, σ_2, and σ_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 Σ, σ_4, and σ_5 in B_6. Any braid obtained in this way preserves V_C. Σ is illustrated in figure 6, and a computation yields the following lemma, from which it is also easy to see that Σ produces a non-entangling gate.

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 Σ 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 Σ, σ_4, σ_5, and $(\sigma_3\sigma_2\sigma_1)(\sigma_4\sigma_3\sigma_2)(\sigma_5\sigma_4\sigma_3)$ 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 Δ, σ_1, σ_2, σ_4, and σ_5. Thus, while the resulting braid will also yield a leakage-free gate, it is one that we have 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* Σ *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 $|\mathbf{11}\rangle$, 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 Δ, and still obtain gates which fix $|\mathbf{11}\rangle$ up to a phase. Interestingly, unlike the situation with the non-computational $|NC\rangle$, many of the gates that fix $|\mathbf{11}\rangle$ up to a phase are entangling on the complementary 4D subspace. For example, it can be shown that $\rho_6((\sigma_2\sigma_3)^3)$ fixes $|\mathbf{11}\rangle$ up to a phase, does not fix $|NC\rangle$, and is entangling on the basis elements $|NC\rangle$, $|\mathbf{1}\tau\rangle$, $|\tau\mathbf{1}\rangle$ and $|\tau\tau\rangle$.

To obtain braids that fix $|\mathbf{1}\tau\rangle$ and $|\tau\mathbf{1}\rangle$, 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 4D subspace. For example, $\rho_6((\sigma_2\sigma_3)^3)$ fixes $|\tau\mathbf{1}\rangle$ up to a phase, does not fix $|NC\rangle$, and is entangling on the basis elements $|NC\rangle$, $|\mathbf{11}\rangle$, $|\mathbf{1}\tau\rangle$ and $|\tau\tau\rangle$.

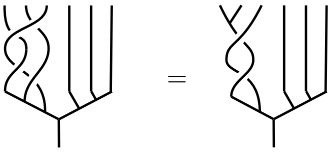

Figure 7. The braid $\sigma_2\sigma_1\sigma_1\sigma_2$ applied to a splitting/fusion tree.

Although it is easy to find braids that fix $|\mathbf{11}\rangle$, $|\mathbf{1}\tau\rangle$ and $|\tau\mathbf{1}\rangle$, 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. Our search enumerated all words up to length seven. Note that a braid word of length n involves multiplying n 5×5 matrices, and that there are 10^7 braid words of length seven on six strands before simplification. In our limited search, no leakage-free entangling gates were found.

It is possible to enlarge the scope of the search by optimizing braid words and utilizing larger computing units. However, the increase in braid word length is very limited due to the exponential growth rate of the number of words with respect to word length.

4. Approximate leakage-free entangling braiding 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 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 $V^{\perp} = \text{span}\{|\mathbf{11}\rangle, |\mathbf{1}\tau\rangle, |\tau\mathbf{1}\rangle\}$.

First, consider the braid $\sigma_2\sigma_1\sigma_1\sigma_2$, 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 $V \oplus V^{\perp}$,

$$\rho_6(\sigma_2\sigma_1\sigma_1\sigma_2) = \rho_3(\sigma_1^2) \oplus \text{diag}(1, 1, (R_{\tau}^{\tau\tau})^2). \tag{13}$$

Similarly,

$$\rho_6(\sigma_4\sigma_5\sigma_5\sigma_4) = \rho_3(\sigma_1^2) \oplus \text{diag}(1, (R_{\tau}^{\tau\tau})^2, 1). \tag{14}$$

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

$$\rho_6(\sigma_3) = \rho_3(\sigma_2) \oplus \text{diag}(R_{\mathbf{1}}^{\tau\tau}, R_{\tau}^{\tau\tau}, R_{\tau}^{\tau\tau}). \tag{15}$$

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 $\mathbf{SU}(2)$ up to phases [7]. 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 one-qubit gates given in equations (5) and (6). Then $\{\rho_3(\sigma_1^2), \rho_3(\sigma_2^2)\}$ generate a dense subgroup of $\mathbf{SU}(2)$ up to global phases.*

Proof. Let $U_1, U_2 \in \mathbf{SU}(2)$. By the classification of subgroups of $\mathbf{SU}(2)$, 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 $\mathbf{SU}(2)$. Take $U_1 = \rho_3(\sigma_1^2\sigma_2^4), U_2 = \rho_3(\sigma_1^2\sigma_2^6)$. 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 mth roots of unity for any integer m, or equivalently that their real parts are not the cosine of a rational multiple of π. Normalizing determinants to equal 1, the real part of the eigenvalues of $\mathrm{e}^{\frac{\mathrm{i}\pi}{10}}\rho_3(\sigma_1^2\sigma_2^4)$ and $\mathrm{e}^{\frac{\mathrm{i}\pi}{10}}\rho_3(\sigma_1^2\sigma_2^6)$ 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 π by theorem 2.3 of [18]. Hence both of the two eigenvalues are of infinite order. □

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 two-qubit leakage-free, entangling gates using braidings.

4.2. Iteration to diagonal gates

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

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

Obviously, U_k does not depend on the phase γ. 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 $U_0 \in \mathbf{SU}(2)$ since by equation (16), if U_k has a global phase, then U_{k+1} has the same global phase.

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

$$U_k = \begin{pmatrix} a_k & -\overline{b_k} \\ b_k & \overline{a_k} \end{pmatrix}. \tag{17}$$

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

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

where

$$y_k = |(1 - |b_k|^2)(1 - \lambda + \lambda^2) + |b_k|^2 \lambda| \tag{18}$$

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

$$= |(2 - 2\cos(\theta))(1 - |b_k|^2) - 1|. \tag{20}$$

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

That $|b_{k+1}| \leqslant \epsilon |b_k|$ 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,

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

Hence,

$$|a_{k+1} - a_k| \;=\; |a_k| \cdot |\lambda - 1|^2 \cdot |b_k|^2 \;\leqslant\; c\epsilon^{2k} \tag{22}$$

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 θ as in the proof of lemma 4.2. The formula in equation (16) for $\theta = \frac{\pi}{3}$ was used in [16] as a scheme to approximate certain diagonal gates. To be precise, the formula in [16] 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 [2, 15], 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 $\theta = \frac{\pi}{5}$. However, their formula does not apply here. This is because $D(\frac{\pi}{5}) = \rho(\sigma_1)^3$ up to phases, and as will be seen in section 4.3, we will give a scheme to approximate two-qubit entangling gates with braids that preserve the subspace $V := \mathrm{span}\{|NC\rangle, |\tau\tau\rangle\}$. 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 one-qubit gate $U \in \mathbf{SU}(2)$ as a rotation in $\mathbb{R}^3$, then $D(\theta)$ is a rotation around the z-axis by the angle θ. 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 θ 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 two-qubit leakage-free entangling braiding gates

We provide a scheme to approximate certain two-qubit leakage-free entangling gates with braidings. Of course, since the Fibonacci model is universal, one can in principle approximate arbitrary n-qubit gates using (for instance) the Solovay–Kitaev algorithm. See [5] for a review of the Solovay–Kitaev algorithm. However, the procedure we give is more explicit and simpler.

Before going into details, let us describe briefly some characteristics of our procedure. First of all, it is designed specially for the six-strand two-qubit model in the Fibonacci theory as defined in section 2.3. Secondly, it does not (at least not directly) approximate an arbitrary two-qubit gate. Rather, it takes certain six-strand braids as input and outputs a leakage-free diagonal two-qubit gate. It is not known to us whether there is an efficient way to determine the input braids so that the procedure with that input will produce a given two-qubit gate. Instead, we choose certain braids as input and prove that the resulting two-qubit is entangling, which together with the one-qubit gates forms a universal gate set. Lastly, the procedure only consists of iterative applications of the formula in equation (16). Furthermore, given a precise $\epsilon > 0$, the number of iterations needed to output the gate with error ϵ is upper bounded by $O(\log(\frac{1}{\epsilon}))$. This can be obtained from the proof of lemma 4.2 that the sequence $\{U_k\}$ in equation (16) converges exponentially fast. However, the length of the braid words in the output is $O(\text{poly}(\frac{1}{\epsilon}))$ which is an easy calculation. In comparison, the Solovay–Kitaev algorithm produces the output both in time and space complexity $O(\text{poly}(\log(\frac{1}{\epsilon})))$.

We use the braiding gates from $\mathcal{G} := \langle \rho_6(\sigma_2\sigma_1\sigma_1\sigma_2), \rho_6(\sigma_3)\rangle$ for the approximation. Recall that $V = \text{span}\{|NC\rangle, |\tau\tau\rangle\}$, $V^{\perp} = \text{span}\{|\mathbf{11}\rangle, |\mathbf{1}\tau\rangle, |\tau\mathbf{1}\rangle\}$, and that gates in $\mathcal{G}$ all preserve V. Choose any gate $\tilde{U}_0$ and a diagonal gate $\tilde{D}$ in $\mathcal{G}$ such that $D := \tilde{D}|_V$ and $U_0 := \tilde{U}_0|_V$ 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 $\{|NC\rangle, |\mathbf{11}\rangle, |\mathbf{1}\tau\rangle, |\tau\mathbf{1}\rangle, |\tau\tau\rangle\}$, then $\tilde{U}$ is entangling if and only if $\lambda_3 \neq \lambda_1\lambda_2\lambda_0^{-1}$.

Theorem 4.6. *Let $\tilde{D} = \rho_6(\sigma_2\sigma_1\sigma_1\sigma_2)^3, \tilde{U}_0 = \rho_6(\sigma_3)$. Then the limit of the sequence $\{\tilde{U}_k\}$ defined by equation (16) exists and its limit $\tilde{U}$ is a leakage-free entangling two-qubit gate.*

Proof. With respect to the decomposition $V \oplus V^{\perp}$, we have

$$\tilde{D} = \begin{pmatrix} e^{-\frac{\pi i}{5}} & 0 \\ 0 & e^{\frac{\pi i}{5}} \end{pmatrix} \oplus \begin{pmatrix} e^{\frac{3\pi i}{5}} & 0 & 0 \\ 0 & e^{\frac{3\pi i}{5}} & 0 \\ 0 & 0 & e^{\frac{\pi i}{5}} \end{pmatrix} \tag{23}$$

$$\tilde{U}_0 = \begin{pmatrix} -\mathrm{e}^{-\frac{\pi \mathrm{i}}{10}}\phi^{-1} & -\mathrm{i}\sqrt{\phi^{-1}} \\ -\mathrm{i}\sqrt{\phi^{-1}} & -\mathrm{e}^{\frac{\pi \mathrm{i}}{10}}\phi^{-1} \end{pmatrix} \oplus \begin{pmatrix} \mathrm{e}^{-\frac{7\pi \mathrm{i}}{10}} & 0 & 0 \\ 0 & \mathrm{e}^{\frac{7\pi \mathrm{i}}{10}} & 0 \\ 0 & 0 & \mathrm{e}^{\frac{7\pi \mathrm{i}}{10}} \end{pmatrix}. \tag{24}$$

We have normalized the above two matrices such that their restriction on V are in $\mathbf{SU}(2)$. 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 $\tilde{U}_{5,5} \neq \mathrm{e}^{\frac{7\pi \mathrm{i}}{10}}\mathrm{e}^{\frac{7\pi \mathrm{i}}{10}}/\mathrm{e}^{\frac{-7\pi \mathrm{i}}{10}} = \mathrm{e}^{\frac{\pi \mathrm{i}}{10}}$. We prove below that $\tilde{U}_{5,5} \neq \mathrm{e}^{\frac{\pi \mathrm{i}}{10}}$.

Denote by $D = \tilde{D}|_V, U_k = \tilde{U}_k|_V, U = \tilde{U}|_V$, where $U = \mathrm{diag}(\ \tilde{U}_{5,5}, \tilde{U}_{5,5}\ )$ is the limit of $\{U_k\}$. We use notations from the proof of lemma 4.2. We have $\theta = \frac{2\pi}{5}$, $\lambda = \mathrm{e}^{\mathrm{i}\theta}$, $\delta = |b_0| = \sqrt{\phi^{-1}}$, $a_0 = -\mathrm{e}^{-\frac{\pi \mathrm{i}}{10}}\phi^{-1}$. By direct calculations, $\epsilon = |(2 - 2\cos(\theta))(1 - \delta^2) - 1| \approx 0.472$.

By equation (22),

$$|a_{k+1} - a_k| \leqslant |1 - \lambda|^2 |b_0|^2 \epsilon^{2k}. \tag{25}$$

Hence,

$$|a_{k+1} - a_0| \leqslant |1 - \lambda|^2 |b_0|^2 \frac{1}{1 - \epsilon^2} < 1.1. \tag{26}$$

Noting that the limit of $\{\overline{a_k}\}$ is precisely $\tilde{U}_{5,5}$, we have

$$|\tilde{U}_{5,5} - \overline{a_0}| \leqslant 1.1. \tag{27}$$

On the other hand, $|\mathrm{e}^{\frac{\pi \mathrm{i}}{10}} - \overline{a_0}| > 1.6$ again by direct calculations. We conclude that $\tilde{U}_{5,5} \neq \mathrm{e}^{\frac{\pi \mathrm{i}}{10}}$. □

5. Conjectures and conclusion

5.1. $\mathbf{SU}(2)_k$ *anyons*

As a modular tensor category, the Fibonacci theory Fib is a sub category of the anyon theory $\mathbf{SU}(2)_3$ whose anyon types are given by $\{0, 1, 2, 3\}$. Explicitly, the correspondence is $\mathbf{1} \leftrightarrow 0$, $\tau \leftrightarrow 2$. Moreover, $\{0, 3\}$ forms the semion theory $\mathcal{S}$ and $\mathbf{SU}(2)_3 = \mathrm{Fib} \boxtimes \mathcal{S}$. Also note that semion $\mathcal{S}$ is an Abelian theory and $1 = 2 \otimes 3 = 2 \boxtimes 3$. 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 τ (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 $\mathbf{SU}(2)_k$, for $k \geqslant 2$ 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 $\mathbf{SU}(2)_k$ is braiding universal if and only if $k = 3$ or $k \geqslant 5$ [8]. We believe that the results presented in this paper still hold for $k \geqslant 5$. For instance, $\{\rho_3(\sigma_1^2), \rho_3(\sigma_2^2)\}$ generates a dense subgroup of $\mathbf{SU}(2)$. Also, the method for approximating entangling leakage-free two-qubit gates in earlier sections also applies.

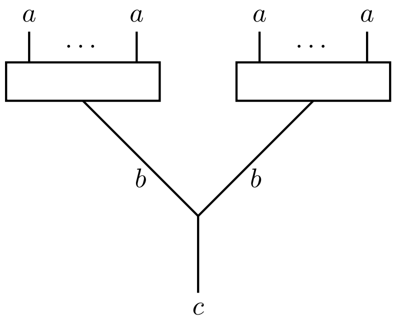

Figure 8. Two qudits.

5.2. Conjectures

Let $\mathcal{C}$ be an anyon theory, namely, a unitary modular tensor category, and $a, b, c \in \mathcal{C}$ be anyon types. Assume c is a total type of (b, b). Consider the embedding $V_b^{a^{\otimes n}} \otimes V_b^{a^{\otimes n}} \subset V_c^{a^{\otimes 2n}}$ for some $n > 1$. See figure 8. We treat each $V_b^{a^{\otimes n}}$ 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 σ on $V_c^{a^{\otimes 2n}}$ preserves, and is entangling on, the subspace $V_b^{a^{\otimes n}} \otimes V_b^{a^{\otimes n}}$.

By the results in this paper, we believe that the Fibonacci anyon (or the type 1 anyon[10] in $\mathbf{SU}(2)_3$) does not have the property of *entangling leakage-free*. On the other hand, the type 1 anyon in $\mathbf{SU}(2)_k$ does have the property of *entangling leakage-free* for $k = 2$ and $k = 4$ [3, 20]. Moreover, the anyon of type D with quantum dimension three in the quantum double of $\mathrm{Rep}(S_3)$ also has the property of *entangling leakage-free*. See [4]. All the examples known to have the property of *entangling leakage-free* are not braiding universal. Thus there seems to be a tension between braiding universality and the property of *entangling leakage-free*, which motivates the following conjecture.

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 $n \geqslant 1$.

The anyon of type 1 of $\mathbf{SU}(2)_8$ has finite images for B_3 and B_4, but infinite images for all $B_n, n \geqslant 5$ [8].

By the property $\mathbf{F}$ conjecture [13], 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.

5.3. Conclusion

In this short note, we tried to address the question whether there exist leakage-free entangling two-qubit gates by braiding Fibonacci anyons. We constructed a large class of leakage-free braiding gates and then proved that all of them are actually non-entangling. We also performed brute-force search for braid words of length less than or equal to seven and did not find any leakage-free entangling gates. This suggests that leakage-free entangling braiding gates may not exist. On the other hand, we provide a protocol specifically designed for the six-strand

[10] Spin 1/2 in physics parlance.

two-qubit model to approximate certain leakage-free entangling gates. The protocol is simple in that it only consists of choosing some intial braids and iteratively applying certain explicit formula. By combining numerical calculations and theoretical work on other anyon models, we speculate that there is a tension between braiding universality and the existence of leakage-free entangling gates. Specifically, we conjecture that there exist leakage-free entangling gates if and only if the theory is not braiding universal.

Acknowledgment

KT and ZW are partially supported by NSF Grant FRG-1664351, and HW by DMS-1841221. SC 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] Birman J S 1976 Braids, links and mapping class groups *Bull. Amer. Math. Soc.* **82** 42–5

[2] Carnahan C, Zeuch D and Bonesteel N 2016 Systematically generated two-qubit anyon braids *Phys. Rev.* A **93** 052328

[3] Cui S X and Wang Z 2015 Universal quantum computation with metaplectic anyons *J. Math. Phys.* **56** 032202

[4] Cui S X, Hong S M and Wang Z 2015 Universal quantum computation with weakly integral anyons *Quantum Inf. Process.* **14** 2687–727

[5] Dawson C M and Nielsen M A 2006 The Solovay–Kitaev algorithm *Quantum Inf. Comput.* **6** 81–95

[6] Delaney C, Rowell E C and Wang Z 2016 Local unitary representations of the braid group and their applications to quantum computing *Rev. Colomb. Mat.* **50** 211–76

[7] Freedman M H, Larsen M and Wang Z 2002 A modular functor which is universal for quantum computation *Commun. Math. Phys.* **227** 605–22

[8] Freedman M H, Larsen M J and Wang Z 2002 The two-eigenvalue problem and density of jones representation of braid groups *Commun. Math. Phys.* **228** 177–99

[9] Hu Y and Kane C 2018 Fibonacci topological superconductor *Phys. Rev. Lett.* **120** 066801

[10] Kliuchnikov V, Bocharov A and Svore K M 2014 Asymptotically optimal topological quantum compiling *Phys. Rev. Lett.* **112** 140504

[11] Lutchyn R, Bakkers E, Kouwenhoven L P, Krogstrup P, Marcus C and Oreg Y 2018 Majorana zero modes in superconductor–semiconductor heterostructures *Nat. Rev. Mater.* **3** 52–68

[12] Mong R S *et al* 2014 Universal topological quantum computation from a superconductor-abelian quantum Hall heterostructure *Phys. Rev.* X **4** 011036

[13] Naidu D and Rowell E C 2011 A finiteness property for braided fusion categories *Algebras Represent. Theory* **14** 837–55

[14] Read N and Rezayi E 1999 Beyond paired quantum Hall states: parafermions and incompressible states in the first excited Landau level *Phys. Rev.* B **59** 8084

[15] Reichardt B W 2012 Systematic distillation of composite Fibonacci anyons using one mobile quasiparticle *Quantum Inf. Comput.* **12** 876–92

[16] Reichardt B W and Grover L K 2005 Quantum error correction of systematic errors using a quantum search framework *Phys. Rev.* A **72** 042326

[17] Rowell E and Wang Z 2018 Mathematics of topological quantum computing *Bull. Am. Math. Soc.* **55** 183–238

[18] Tangsupphathawat P 2014 Algebraic trigonometric values at rational multipliers of π *Acta Comment. Univ. Tartuensis Math.* **18** 9–18

[19] Trebst S, Troyer M, Wang Z and Ludwig A W 2008 A short introduction to fibonacci anyon models *Prog. Theor. Phys. Suppl.* **176** 384–407

[20] Wang Z 2010 *Topological Quantum Computation* vol 112 (Providence, RI: American Mathematical Society)