Quantum Information Processing (2025) 24:14
https://doi.org/10.1007/s11128-024-04633-1

Universal topological quantum computing via double-braiding in SU(2) Witten–Chern–Simons theory

Adrian L. Kaufmann[1] · **Shawn X. Cui**[2]

Received: 2 February 2024 / Accepted: 23 December 2024 / Published online: 6 January 2025

Abstract
We study the problem of universality in the anyon model described by the $SU(2)$ Witten–Chern–Simons theory at level k. A classic theorem of Freedman–Larsen–Wang states that for $k \geq 3,\ k \neq 4$, braiding of the anyons of topological charge $1/2$ is universal for topological quantum computing. For the case of one qubit, we prove a stronger result that double-braiding of such anyons alone is already universal.

Keywords Topological quantum computing · Double braiding · Witten-Chern-Simons theory · Universal quantum computing

1 Introduction

Topological quantum computing is an approach to building a fault-tolerant quantum computer using certain quasi-particles, called anyons, in two dimensions. The physical systems hosting anyons are two-dimensional topological phases of matter. Topological phases are gapped quantum phases which go beyond Landau's theory of symmetry breaking and local order parameters; instead, they obey a new order called topological quantum order [1]. Such phases exhibit several remarkable properties including robust ground state degeneracy, depending on the topology of the underlying system, long-range entanglement, protected gapless edge modes, fractionalized quasi-particle excitations, and exotic exchange statistics. The robustness of the ground/excited state space provides an ideal place to store quantum information as logical qubits. Braiding of anyons, a process of adiabatically interchanging anyons, induces a unitary transformation on the state space. These unitary transformations remain unchanged under

✉ Shawn X. Cui
cui177@purdue.edu

Adrian L. Kaufmann
kaufmannadi25@gmail.com

[1] West Lafayette Junior/Senior High School, West Lafayette, IN 47906, USA

[2] Department of Mathematics, Department of Physics and Astronomy, Purdue University, West Lafayette, IN 47907, USA

local deformations of the braiding world lines, and hence serve as logical quantum gates. This method of encoding and manipulating information in global degrees of anyons is called topological quantum computing [2, 3], and it has the advantage of achieving fault tolerance at the 'hardware' level. This is an active area of research both theoretically and experimentally. See [4, 5] for a comprehensive review. For some more recent progress on this area, see, for instance [6–12], and references therein.

An important family of topological phases is described by the Witten–Chern–Simons theory associated with the Lie group $SU(2)$ and a level $k \in \mathbb{Z}_{\geq 0}$ [13]. Denote the theory by $\mathbf{SU}(2)_k$. It is among the earliest studied anyon models. By a classic result of [14], except for a few values of k, the model is universal for topological quantum computing, i.e., it is equivalent to the standard circuit model. Furthermore, the theory has various potential realizations in fractional quantum Hall (FQH) systems. For example, $\mathbf{SU}(2)_2$ contains the Ising anyon expected to exist in FQH with filling factor $\nu = 5/2$, and $\mathbf{SU}(2)_3$ contains the Fibonacci anyon expected to exist in $\nu = 12/5$ FQH.

We elaborate a bit more on the universality of $\mathbf{SU}(2)_k$. It contains an anyon type, which we denote by τ, with topological charge $1/2$. Fusing two type-τ anyons produces either the ground state or a type-τ anyon. By iteratively fusing τ with itself, every anyon type in this model can be produced. In this sense, τ is the most critical anyon type in $\mathbf{SU}(2)_k$. Denote by $V_\tau^{\tau^{\otimes 3}}$ the space of three τ anyons with total type equal to τ, or equivalently, the space of four type-τ anyons (with total type trivial). This space has dimension two, and hence is a qubit. Braiding of the τ anyons induces a unitary representation of the braid group B_3 on the qubit. The theorem of [14] states that, for all $k \geq 3$, $k \neq 4,\ 8$, this representation has a dense image in $U(V_\tau^{\tau^{\otimes 3}})$, implying universal quantum computing on one qubit by braiding. In fact, [14] shows that for the above values of k and for any $n \geq 3$, the image of the braid group representation is dense in $V_\tau^{\tau^{\otimes n}}$.[1] These results set the theoretical foundation for universal topological quantum computing.

In this paper, we focus on the qubit $V_\tau^{\tau\tau\tau}$ and study the representation from braiding,

$$\rho_k \colon B_3 \to U(V_\tau^{\tau\tau\tau}). \tag{1}$$

Recall that the braid group on n strands B_n has the standard generators $\sigma_1, \ldots, \sigma_{n-1}$ (see Sec. 2). B_n acts on the space of n identical anyons of certain type where σ_i corresponds to a counterclockwise braiding the i-th and $(i+1)$-th anyon. We call σ_i^2 a *double-braiding*, and it corresponds to moving the i-th anyon counterclockwise around the $(i+1)$-th anyon and returning to its original position in the end. See Fig. 1. More generally, any braid in the group generated by the σ_i^2's is also called a double-braiding. Specializing to the case of one qubit $V_\tau^{\tau\tau\tau}$ in $\mathbf{SU}(2)_k$ with $k \geq 3$, $k \neq 4,\ 8$, while [14] states that the image of B_3 under ρ_k is dense in $U(V_\tau^{\tau\tau\tau})$, we prove that the image of the subgroup of double-braidings alone is dense in $U(V_\tau^{\tau\tau\tau})$.

Our result is of significance in several aspects. Firstly, it is mathematically stronger than the theorem of [14] adapted to one qubit, and may reveal some hidden structure in the representations of the braid group. Secondly, although our result is stated only

[1] This result also holds for $k = 8$, but n needs to be at least 5.

Fig. 1 (Left) A counterclockwise braiding of two anyons; (Right) A counterclockwise double-braiding of two anyons

for one qubit, it is not too much restricted, as any entangling 2-qubit gate plus 1-qubit gates are universal for quantum computing. Thirdly, our result generalizes the work of [15] where the Fibonacci anyon was shown to be universal by double-braidings, which corresponds to the case $k = 3$ here. Moreover, using the double-braiding-universality of the Fibonacci anyon, the authors in [15] provided an elegant, exponentially fast algorithm to produce entangling leakage-free 2-qubit gates which are necessary for universal quantum computing on multi-qubits. With the result in the current paper, the algorithm of [15] can be straightforwardly adapted to other $\mathbf{SU}(2)_k$. Fourthly, from a physical point of view, double-braidings have the advantage that at each step only one anyon needs to move, it needs to move at most to the vicinity of its nearest neighbor, and it returns to its own position immediately after the move. Hence, there is no need to track the positions of the involved anyons. This approach mitigates the errors associated with the control of anyons, and simplifies the operations on them, thereby potentially reducing the experimental challenges in realizing topological quantum computing. It should be noted that the group of double-braidings is strictly smaller than the pure braid group consisting of braids where anyons return to their positions *eventually*.

It is now a well-established dictionary that two-dimensional topological phases of matter are characterized by the structure of a unitary modular tensor category which is a braided category satisfying additional conditions. A double-braiding is also called a *twine* structure in the braided category introduced by [16]. The twine structure can be formalized and defined on non-braided categories. There exist monoidal categories without a braiding structure, but with a twine structure. An example of this is the fermionic Moore–Read fusion category [17]. While most FQH states are expected to fit in the framework of modular tensor categories, some do not seem so. Instead, they might be described by twine fusion categories [17, 18]. Our work on double-braidings could provide insight into exploring the power of quantum computing in those systems.

We conjecture that our result on the universality of double-braidings also holds for the case of multi-qubits, i.e., the space of more than three anyons. For that generalization, the techniques utilized in this paper may not apply. Instead, it is possible to make use of the Lie-theoretical tools on the two-eigenvalue problem in [14]. We leave this as a future direction.

After the first version of the manuscript was posted, we were made aware[2] that Theorem 3.5 follows from a result in [19], which proved that if braiding of n identical anyons is universal, then universality is also achieved by moving only one anyon around the other $n - 1$ anyons. Specializing to $n = 3$, the group of braids in which only the second anyon moves is precisely the group of double braids. Then, combining the braiding universality of $\mathbf{SU}(2)_k$ of [14] and result of [19] for $n = 3$, we arrive at

[2] S.X.C would like to thank Sachin Valera for pointing out the result in [19]

Theorem 3.5. However, it should be noted that both [14] and [19] replied heavily on abstract Lie-theoretical results such as the characterization of normal subgroups of Lie groups. In contrast, our proof for Theorem 3.5 is explicit and only involves elementary tools. We hope the proof itself is interesting to readers who might want to extend it to other anyon theories.

The rest of the paper is organized as follows. Section 2 gives a brief overview on the algebraic theory of anyons and the setup in topological quantum computing, with a more detailed explanation in Appendix A. In Sects. 3.1–3.2, we provide data for $\mathbf{SU}(2)_k$ and explicit calculations of the braid group representations. Section 3.3 contains the main result.

2 Topological quantum computing with anyons

In this section, we provide a very brief introduction to topological quantum computing (TQC). There are many references with more comprehensive discussions on this subject, such as [4, 5, 20, 21].

Mathematically, an anyon model is characterized by the structure of a unitary modular tensor category (MTC). An MTC can be described either in terms of abstract categorical language or by a set of concrete data. We take the second approach and provide a partial set of data for the purpose of fixing the convention. See Appendix A for a more detailed discussion of MTCs.

An anyon model has a finite set

$$L = \{a, b, c, \ldots\} \tag{2}$$

consisting of all the possible anyon types in a topological phase. Each anyon type a has a dual anyon type $\bar{a}$. The ground state is considered as a special trivial anyon type, usually denoted by $\mathbf{1}$. The fusion rule describes the possible outcomes when fusing two anyons. Given $a, b \in L$, we formally write,

$$a \otimes b = \bigoplus_{c \in L} N_{ab}^{c}\, c, \tag{3}$$

where N_{ab}^{c} denotes the number of different channels of fusing a and b to result in the output c. If there is no way to obtain c from the fusion, then $N_{ab}^{c} = 0$. If $N_{ab}^{c} > 0$, we say c is a *total type* or *total charge* of a and b, and call the triple $(a, b; c)$ *admissible*. For simplicity, in the following discussions **we will assume N_{ab}^{c} is either** 0 **or** 1, i.e., the anyon model is multiplicity-free.

For anyon types $c, a_1, \ldots, a_n$, denote by $V_c^{a_1 a_2 \cdots a_n}$ the space of states representing n anyons $a_1, \ldots, a_n$ with total charge c. A basis for such a space can be described as follows. Choose an upward-growing binary tree with one root at the bottom and n leaves at the top. See Fig. 2 for an illustration. Label the root by c and the leaves, from left to right, by $a_1, a_2, \ldots, a_n$. Now label each internal edge e by an anyon type b_e such that at each fork, the relevant triple of labels are admissible. Then, the binary tree with all possible labels $\{b_e\}$ of internal edges forms a basis of $V_c^{a_1 a_2 \cdots a_n}$, called a *splitting-*

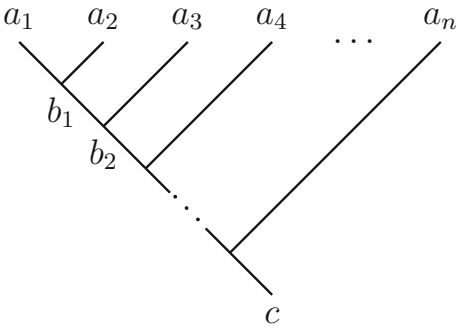
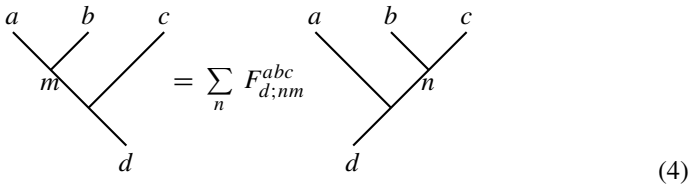


Fig. 2 A basis of $V_c^{a_1 a_2 \cdots a_n}$ corresponding to a binary tree

tree basis. For each labeled binary tree, one can interpret the state it represents as a splitting process, where and throughout the context, the time direction is from bottom to top. For example, the state represented by the tree in Fig. 2 is obtained by splitting c into b_{n-2} and a_n, followed by splitting b_{n-2} into b_{n-3} and a_{n-1}, …, followed by splitting b_1 into $b_0 = a_1$ and a_2.

For $n = 3$, there are two splitting trees, with one internal edge, as shown on both sides of the equation below. The basis corresponding to the tree on the left side of the equation consists of all possible labelings m of the internal edge so that $(a, b; m)$ and $(m, c; d)$ are both admissible. Similarly, the basis for the tree on the right side consists of labelings n of the internal edge so that $(b, c; n)$ and $(a, n; d)$ are both admissible. Denote the matrix change between the two bases by F_d^{abc}. More explicitly,



(4)

where $F_{d;nm}^{abc}$ is the (n, m)-entry of F_d^{abc}, and the sum is over all labelings n as described above. Note that, here the anyon types n and m are used as the indices of the entries of F_d^{abc}. We call F_d^{abc} an F-matrix, its entries F-symbols or $6j$-symbols, and the identity in the above equation an F-move.

The process of swapping positions of anyons is called a braiding. A braiding induces a unitary transformation on the state space. Consider two anyons a and b with total type c. A counterclockwise braiding of a and b maps a state in V_c^{ab} to one in V_c^{ba}. Since both spaces have dimension one, there exists a phase R_c^{ba} such that the following equality holds,

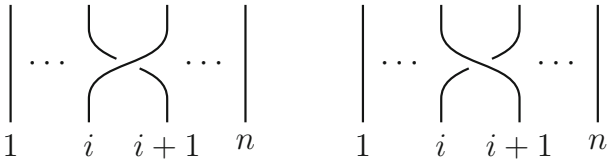
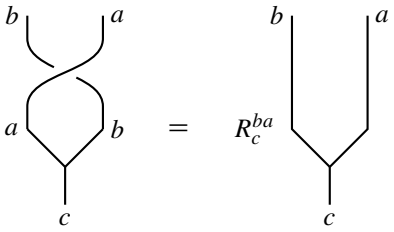


Fig. 3 (Left) the braid diagram σ_i; (Right) the braid diagram σ_i^{-1}



(5)

The above equality is called an R-move, and R_c^{ba} is called an R-symbol. The set of F- and R-symbols is crucial for calculations in the anyon model.

Now, we discuss how to perform quantum computing with anyons. The state space of multi-anyons is the logical space to store information. Typically, one chooses multiple identical anyons, say n type-a anyons with total type c for some n. Denote this space by $V_c^{a^{\otimes n}} := V_c^{aa\cdots a}$. The type a needs to be non-Abelian so that the dimension of $V_c^{a^{\otimes n}}$ approaches to infinity as $n \to \infty$. In general, $V_c^{a^{\otimes n}}$ does not have a natural tensor product structure, and we need to choose a subspace which does have a tensor product structure as multi-qubits or multi-qudits. The computational basis for the qudits can be chosen to be any splitting-tree basis.

Braiding of anyons induces a representation of the braid group and acts as quantum gates on the logical space $V_c^{a^{\otimes n}}$. Recall that the n-strand braid group B_n has a presentation as

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \,|\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \\ \sigma_i\sigma_j = \sigma_j\sigma_i, |i-j| > 1 \rangle, \tag{6}$$

where σ_i (resp. σ_i^{-1}) corresponds to the braid diagram in Fig. 3(Left) (resp. (Right)).

We have a representation,

$$\rho\colon B_n \to U(V_c^{a^{\otimes n}}), \tag{7}$$

where σ_i (resp. σ_i^{-1}) acts on $V_c^{a^{\otimes n}}$ by counterclockwise (resp. clockwise) braiding of the i-th with the $(i+1)$-th anyon. With a chosen splitting-tree basis, a matrix for each braid generator can be computed using F- and R-symbols. The set of quantum gates obtained from braiding is the image of this braid group representation.

3 Universality in $\mathbf{SU}(2)_k$ anyons

3.1 $\mathbf{SU}(2)_k$ anyons

Recall that the $SU(2)$ Witten–Chern–Simons theory at level $k \in \mathbb{Z}_{\geq 0}$ is denoted by $\mathbf{SU}(2)_k$. The MTC corresponding to $\mathbf{SU}(2)_k$ is constructed from finite-dimensional representations of the quantum group $U_q(\mathrm{sl}_2)$ for $q = e^{\frac{2\pi i}{k+2}}$. It also describes the Wess–Zumino–Witten conformal field theory [22, 23].

Below we describe the data of the $\mathbf{SU}(2)_k$ MTC obtained from Sec. 5.4 of [18], though the data also appeared in earlier literature in different forms. The MTC has $k+1$ anyon types (i.e., simple objects) labeled by half-integers $0, \frac{1}{2}, \frac{2}{2}, \ldots, \frac{k}{2}$, where 0 denotes the trivial anyon type. The fusion rule is given by,

$$j_1 \otimes j_2 = \bigoplus_{j=|j_1-j_2|}^{\min\{j_1+j_2,\, k-j_1-j_2\}} j, \tag{8}$$

where j has an increment of 1 in the above sum, implying that for admissible $(j_1, j_2; j)$, $j_1 + j_2 + j$ is always an integer. Throughout the context, fix $q = e^{\frac{2\pi i}{k+2}}$, and denote by $q^x := e^{\frac{2\pi i x}{k+2}}$. For $n \in \mathbb{Z}_{\geq 0}$, the quantum integer $[n]$ and the quantum factorial are defined by,

$$[n]_q := \frac{q^{\frac{n}{2}} - q^{-\frac{n}{2}}}{q^{\frac{1}{2}} - q^{-\frac{1}{2}}}, \qquad [n]_q! = ([n-1]_q!)\,[n], \qquad [0]_q! = 1. \tag{9}$$

The R-symbols are given by,

$$R_j^{j_1,j_2} = (-1)^{j-j_1-j_2} q^{\frac{1}{2}(j(j+1)-j_1(j_1+1)-j_2(j_2+1))}. \tag{10}$$

The F-symbols are given by,

$$F^{j_1,j_2,j_3}_{j;\,j_{12},j_{23}} = [F_j^{j_1,j_2,j_3}]_{j_{12},j_{23}} = (-1)^{j_1+j_2+j_3+j} \sqrt{[2j_{12}+1]_q [2j_{23}+1]_q} \begin{Bmatrix} j_1 & j_2 & j_{12} \\ j_3 & j & j_{23} \end{Bmatrix}_q, \tag{11}$$

where

$$\begin{Bmatrix} j_1 & j_2 & j_{12} \\ j_3 & j & j_{23} \end{Bmatrix}_q = \Delta(j_1, j_2, j_{12})\Delta(j_{12}, j_3, j)\Delta(j_2, j_3, j_{23})\Delta(j_1, j_{23}, j) \times$$
$$\sum_z \left\{ \frac{(-1)^z [z+1]_q!}{[z-j_1-j_2-j_{12}]_q![z-j_{12}-j_3-j]_q![z-j_2-j_3-j_{23}]_q![z-j_1-j_{23}-j]_q!} \right.$$
$$\left. \times \frac{1}{[j_1+j_2+j_3+j-z]_q![j_1+j_{12}+j_3+j_{23}-z]_q![j_2+j_{12}+j+j_{23}-z]} \right\},$$

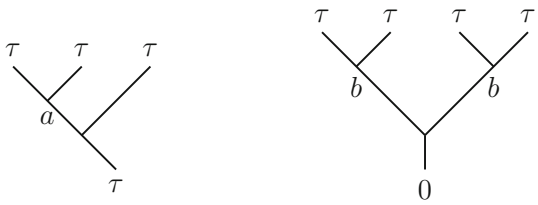


Fig. 4 (Left) A splitting-tree basis for $V_\tau^{\tau\tau\tau}$; (Right) A splitting-tree basis for $V_0^{\tau\tau\tau\tau}$, where τ is the anyon of type $\frac{1}{2}$. $a, b = 0, 1$

(12)

where the sum is over z with an increment of 1 for which all the $[\cdot]_q!$ in the sum are defined, and

$$\Delta(j_1, j_2, j_3) = \sqrt{\frac{[-j_1 + j_2 + j_3]_q![j_1 - j_2 + j_3]_q![j_1 + j_2 - j_3]}{[j_1 + j_2 + j_3 + 1]_q!}}. \tag{13}$$

A fact that will not be used in this paper is that a close cousin of the $\mathbf{SU}(2)_k$ MTC is the Temperley–Lieb–Jones MTC obtained from skein theory [24]. Under a proper translation between the level k and the Kauffman variable A in the skein theory, the $\mathbf{SU}(2)_k$ MTC and the Temperley–Lieb–Jones MTC are equivalent as braided fusion categories, but differ by a ribbon twist.

3.2 The 1-qubit model

For $k \geq 2$, we consider the anyon type labeled by $\tau := \frac{1}{2}$ in the $\mathbf{SU}(2)_k$ model. For $k = 2$, τ is the Ising anyon, while for $k = 3$, τ is closely related to the Fibonacci anyon.[3]

There are two standard ways to obtain a qubit using τ anyons. They are the dense encoding and the sparse encoding corresponding to the spaces $V_\tau^{\tau\tau\tau}$ and $V_0^{\tau\tau\tau\tau}$, respectively. That is, the dense encoding takes, as a qubit, the space of three τ anyons with total type τ, while the sparse encoding takes the space of four τ anyons with total type 0. From the fusion rule,

$$\frac{1}{2} \otimes \frac{1}{2} = 0 \oplus 1, \quad \frac{1}{2} \otimes 1 = \frac{1}{2} \oplus \frac{3}{2}, \quad 0 \otimes j = j, \tag{14}$$

both $V_\tau^{\tau\tau\tau}$ and $V_0^{\tau\tau\tau\tau}$ are of two dimensions with a splitting-tree basis given in Fig. 4. Denote the splitting-tree basis in Fig. 4 (Left) by $\{|x\rangle : x = 0, 1\}$ and the one in Fig. 4 (Right) by $\{|x\rangle' : x = 0, 1\}$.

The braiding of the τ anyons induces representations of the braid groups with the action of the generator σ_i given by the counterclockwise swap of the i-th and the $(i + 1)$-th anyon,

$$\rho_k : B_3 \to U(V_\tau^{\tau\tau\tau}), \tag{15}$$

[3] The anyon of type $\frac{1}{2}$ in $\mathbf{SU}(2)_3$ is the composite of the Fibonacci anyon with a semion [18].

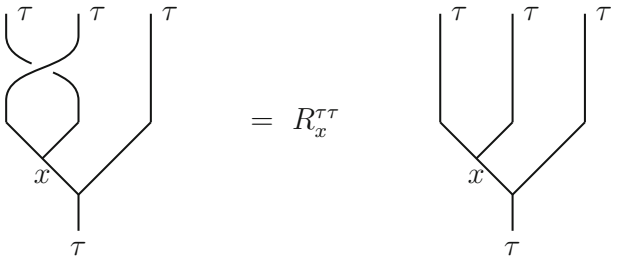


Fig. 5 The action of σ_1 on $V_\tau^{\tau\tau\tau}$

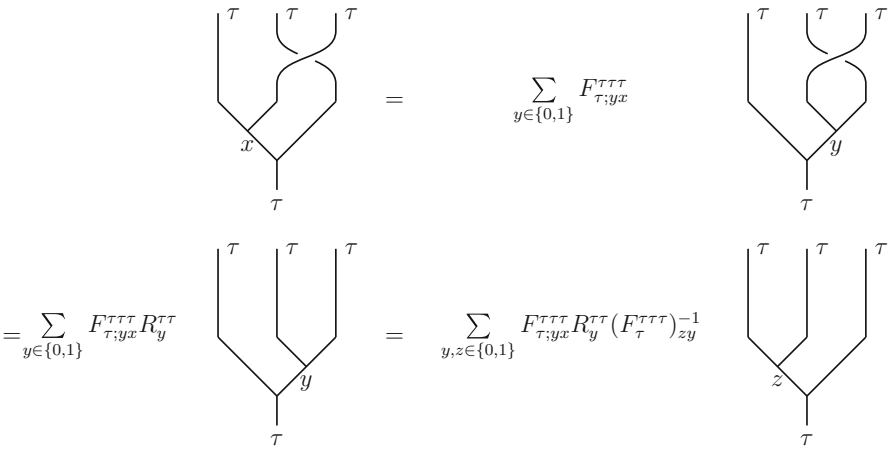


Fig. 6 The action of σ_2 on $V_\tau^{\tau\tau\tau}$. The first and the third equalities are due to an F-move and an inverse F-move, respectively. The second equality is due to an R-move

$$\rho'_k \colon B_4 \to U(V_0^{\tau\tau\tau\tau}). \tag{16}$$

For the dense encoding, under the basis $\{|x\rangle : x = 0, 1\}$ of $V_\tau^{\tau\tau\tau}$, the action of the generators σ_1 and σ_2 are computed in Fig. 5 and Fig. 6, respectively.

Hence,

$$\rho_k(\sigma_1)|x\rangle = R_x^{\tau\tau}|x\rangle \tag{17}$$

$$\rho_k(\sigma_2)|x\rangle = \sum_{y,z\in\{0,1\}} F_{\tau;yx}^{\tau\tau\tau}\, R_y^{\tau\tau}\, (F_\tau^{\tau\tau\tau})_{zy}^{-1}\, |z\rangle. \tag{18}$$

Denote by,

$$R = \begin{pmatrix} R_0^{\tau\tau} & 0 \\ 0 & R_1^{\tau\tau} \end{pmatrix}, \qquad F = F_\tau^{\tau\tau\tau} = \begin{pmatrix} F_{\tau;00}^{\tau\tau\tau} & F_{\tau;01}^{\tau\tau\tau} \\ F_{\tau;10}^{\tau\tau\tau} & F_{\tau;11}^{\tau\tau\tau} \end{pmatrix}. \tag{19}$$

From the data in Sect. 3.1,

$$R = \begin{pmatrix} -q^{-\frac{3}{4}} & 0 \\ 0 & q^{\frac{1}{4}} \end{pmatrix}, \qquad F = F_\tau^{\tau\tau\tau} = \frac{\sqrt{q}}{q+1} \begin{pmatrix} -1 & \sqrt{q+\frac{1}{q}+1} \\ \sqrt{q+\frac{1}{q}+1} & 1 \end{pmatrix}. \tag{20}$$

Note that F is a symmetric, real, involutory matrix. Then, we have

$$\rho_k(\sigma_1) = R = \begin{pmatrix} -q^{-\frac{3}{4}} & 0 \\ 0 & q^{\frac{1}{4}} \end{pmatrix}, \tag{21}$$

$$\rho_k(\sigma_2) = F^{-1}RF = \frac{q^{\frac{1}{4}}}{1+q} \begin{pmatrix} q & \sqrt{q+\frac{1}{q}+1} \\ \sqrt{q+\frac{1}{q}+1} & -\frac{1}{q} \end{pmatrix}. \tag{22}$$

For the sparse encoding, we show in fact the image $\rho_k'(B_4)$ is the same as $\rho_k(B_3)$ if we identify $|x\rangle' \in V_0^{\tau\tau\tau\tau}$ with $|x\rangle \in V_\tau^{\tau\tau\tau}$. Under this identification, it is clear that $\rho_k'(\sigma_1) = \rho_k'(\sigma_3) = \rho_k(\sigma_1)$, while $\rho_k'(\sigma_2)$ can be computed, similar to $\rho_k(\sigma_2)$ in Fig. 6, as,

$$\rho_k'(\sigma_2)|x\rangle' = (F_0^{x\tau\tau})_{\tau x}^{-1} \left(\sum_{y,z\in\{0,1\}} F_{\tau;yx}^{\tau\tau\tau}\, R_y^{\tau\tau}\, (F_\tau^{\tau\tau\tau})_{zy}^{-1} \right) F_{0;z\tau}^{z\tau\tau}\, |z\rangle'. \tag{23}$$

From the F-symbols of $\mathbf{SU}(2)_k$ in Sect. 3.1, it can be checked that $F_{j;j_{23}j_{12}}^{j_1 j_2 j_3} = 1$ whenever $j = 0$ and the involved labels are admissible. Hence, we have $\rho_k'(\sigma_2) = \rho_k(\sigma_2)$. This shows the equality of $\rho_k'(B_4)$ and $\rho_k(B_3)$.

Therefore, from now on, we will focus on the dense encoding only. A logical qubit is given by the space $V_\tau^{\tau\tau\tau}$ whose computational basis is $\{|0\rangle, |1\rangle\}$ as shown in Fig. 4 (Left). The set of 1-qubit logical gates obtained from anyon braidings corresponds to elements in the image $\rho_k(B_3)$. Since quantum gates are well defined only up to global $U(1)$ phases, the gates in $\rho_k(B_3)$ can be multiplied by any phase, or they should be considered as elements of the projective unitary group $PU(V_\tau^{\tau\tau\tau})$.

Definition 3.1 Let V be a Hilbert space, and $\mathcal{G}$ be a subset of the unitary group $U(V)$. $\mathcal{G}$ is said to be universal on V if $\mathcal{G} \cup U(1)$ generate a dense subgroup of $U(V)$.

To study the universality of the braiding gates, it is convenient to normalize the generators of B_3 so that the image of ρ_k lies in $SU(V_\tau^{\tau\tau\tau})$. Explicitly, multiplying $-iq^{1/4}$ to the generators, we obtain the normalized representation $\tilde{\rho}_k : B_3 \to SU(V_\tau^{\tau\tau\tau})$,

$$\tilde{\rho}_k(\sigma_1) = \tilde{R} = \begin{pmatrix} i\, q^{-\frac{1}{2}} & 0 \\ 0 & -i\, q^{\frac{1}{2}} \end{pmatrix}, \tag{24}$$

$$\tilde{\rho}_k(\sigma_2) = F^{-1}\tilde{R}F = \frac{i\sqrt{q}}{q+1} \begin{pmatrix} -q & -\sqrt{q+\frac{1}{q}+1} \\ -\sqrt{q+\frac{1}{q}+1} & \frac{1}{q} \end{pmatrix}. \tag{25}$$

Since ρ_k equals $\tilde{\rho}_k$ up to a global phase, we will use ρ_k and $\tilde{\rho}_k$ interchangeably.

As an example, when $k = 2$, $\tilde{\rho}_2(\sigma_1)$ and $\tilde{\rho}_k(\sigma_2)$ are given, respectively, by,

$$e^{\frac{\pi i}{4}} \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}, \tag{26}$$

which, together with $U(1)$ phases, generate the 1-qubit Clifford group.

The multi-qubit models can be obtained by increasing the number of anyons utilized. We will not discuss that direction. The universality of braiding the τ anyons is a classic problem settled in [14]. We rephrase Theorem 4.1 of [14] in the setup of one qubit.

Theorem 3.2 *([14]) For any integer $k \geq 3, k \neq 4, 8$, let $V_\tau^{\tau\tau\tau}$ be the 1-qubit space in the $\mathbf{SU}(2)_k$ model. Then, set of braiding gates corresponding to the image of the representation $\tilde{\rho}_k$ defined in Eqs. 24 and rm 25 is universal on $V_\tau^{\tau\tau\tau}$.*

3.3 Universality of double-braiding in $\mathbf{SU}(2)_k$

In this section, we prove a stronger result than Theorem 3.2. That is, for those values of k in Theorem 3.2, we show that the set of double-braiding gates on $V_\tau^{\tau\tau\tau}$ is universal in the $\mathbf{SU}(2)_k$ model. By a double-braiding is meant a braid generated by even powers of the standard generators σ_i's of the braid group. We will rely on two critical results. The content of Lemma 3.3 below first appeared in the work of Kitaev [25] where he used the lemma to prove the universality of certain gate sets. The lemma can also be found in Section 6 of [26].

Lemma 3.3 *([25]) Let A and B be two non-commuting elements of $SU(2)$ both of which are of infinite order. Then, A and B generate a dense subgroup of $SU(2)$.*

Proof (*sketch.*) Let G be the closure of the subgroup generated by A and B. By the assumption in the lemma, G is a closed connected noncommutative Lie subgroup of $SU(2)$. Hence, the Lie algebra $\mathfrak{g}$ of G is a noncommutative Lie subalgebra of $\mathfrak{su}(2)$. The only such Lie subalgebra of $\mathfrak{su}(2)$ is itself. Therefore, $G = SU(2)$. □

Theorem 3.4 *(*Theorem 7, [27]*) Suppose we have at most four distinct rational multiples of π lying strictly between 0 and $\frac{\pi}{2}$ for which some rational linear combination of their cosines is rational but no proper subset has this property. Then, the appropriate linear combination is proportional to one from the following list:*

- $\cos \pi/3 = \frac{1}{3}$,
- $-\cos\phi + \cos(\pi/3 - \phi) + \cos(\pi/3 + \phi) = 0$ $(0 < \phi < \pi/6)$,
- $\cos \pi/5 - \cos 2\pi/5 = \frac{1}{2}$,
- $\cos \pi/7 - \cos 2\pi/7 + \cos 3\pi/7 = \frac{1}{2}$,
- $\cos \pi/5 - \cos \pi/15 + \cos 4\pi/15 = \frac{1}{2}$,
- $-\cos 2\pi/5 + \cos 2\pi/15 - \cos 7\pi/15 = \frac{1}{2}$,
- $\cos \pi/7 + \cos 3\pi/7 - \cos \pi/21 + \cos 8\pi/21 = \frac{1}{2}$,
- $\cos \pi/7 - \cos 2\pi/7 + \cos 2\pi/21 - \cos 5\pi/21 = \frac{1}{2}$,
- $-\cos 2\pi/7 + \cos 3\pi/7 + \cos 4\pi/21 + \cos 10\pi/21 = \frac{1}{2}$,
- $-\cos \pi/15 + \cos 2\pi/15 + \cos 4\pi/15 - \cos 7\pi/15 = \frac{1}{2}$.

The following is the main result of the paper.

Theorem 3.5 *For any integer $k \geq 3, k \neq 4, 8$, let τ be the anyon of type $\frac{1}{2}$ in the anyon model $\boldsymbol{SU}(2)_k$, and $\rho_k : B_3 \to U(V_\tau^{\tau\tau\tau})$ be the representation of B_3 on the dense-encoding 1-qubit $V_\tau^{\tau\tau\tau}$. Then, the images of σ_1^2 and σ_2^2 under ρ_k, together with phases, generate a dense subgroup of $U(V_\tau^{\tau\tau\tau})$. That is, the double-braiding gates alone are universal.*

Proof It suffices to show, for the normalized $\tilde{\rho}_k : B_3 \to U(V_\tau^{\tau\tau\tau})$ defined in Eqs. 24 25, $\tilde{\rho}_k(\sigma_1^2)$ and $\tilde{\rho}_k(\sigma_2^2)$ generate a dense subgroup of $SU(V_\tau^{\tau\tau\tau})$. Let

$$A := \tilde{\rho}_k(\sigma_1^2\sigma_2^4) = \tilde{R}^2 F^{-1} \tilde{R}^4 F, \quad B := \tilde{\rho}_k(\sigma_1^2\sigma_2^6) = \tilde{R}^2 F^{-1} \tilde{R}^6 F. \tag{27}$$

From the expressions of $\tilde{R}$ (Eq. 24) and F (Eq. 20), the matrices of A, B, and $W := ABA^{-1}B^{-1}$ can be calculated as (See Appendix B for a Mathematica implementation),

$$A = \begin{pmatrix} -\frac{q^4+q^2-q+1}{q^3+q^2} & -\frac{\sqrt{q+\frac{1}{q}+1}(q^3-q^2+q-1)}{q^2(q+1)} \\ -\frac{\sqrt{q+\frac{1}{q}+1}(q^3-q^2+q-1)}{q+1} & -\frac{q^5+q^2+q+1}{q(q+1)^2} \end{pmatrix} \tag{28}$$

$$B = \begin{pmatrix} \frac{q^7+q^6+q^5+1}{q^3(q+1)^2} & \frac{\sqrt{q+\frac{1}{q}+1}(q^5-q^4+q^3-q^2+q-1)}{q^3(q+1)} \\ \frac{\sqrt{q+\frac{1}{q}+1}(q^5-q^4+q^3-q^2+q-1)}{q(q+1)} & \frac{q^6+q+\frac{1}{q}+1}{q(q+1)^2} \end{pmatrix} \tag{29}$$

$$W_{11} = \frac{q^{13}-3q^{12}+6q^{11}-11q^{10}+16q^9-19q^8+22q^7-21q^6+19q^5-14q^4+10q^3-6q^2+3q-1}{q^6(q+1)} \tag{30}$$

$$W_{12} = -\frac{(q-1)^2\sqrt{q+\frac{1}{q}+1}\left(q^{10}-q^9+3q^8-4q^7+5q^6-6q^5+6q^4-5q^3+4q^2-2q+1\right)}{q^7(q+1)} \tag{31}$$

$$W_{21} = \frac{(q-1)^2\sqrt{q+\frac{1}{q}+1}\left(q^{10}-2q^9+4q^8-5q^7+6q^6-6q^5+5q^4-4q^3+3q^2-q+1\right)}{q^4(q+1)} \tag{32}$$

$$W_{22} = \frac{-q^{13}+3q^{12}-6q^{11}+10q^{10}-14q^9+19q^8-21q^7+22q^6-19q^5+16q^4-11q^3+6q^2-3q+1}{q^7+q^6} \tag{33}$$

We will show that, for the values of k in the statement of the theorem, A and B are both of infinite order and they do not commute. Then by Lemma 3.3, A and B generate a dense subgroup of $SU(2)$, implying the validity of the theorem. The rest of the proof is devoted to verifying the assumptions on A and B mentioned above.

Proving A has infinite order.

Denote the eigenvalues of A by $e^{\pm\theta_k i}$, $0 \le \theta_k \le \pi$. It suffices to show that θ_k is not a rational multiple of π. Recall that $q = e^{\frac{2\pi i}{k+2}}$. We have,

$$2\cos\theta_k = \mathrm{tr}(A) = -\frac{((q-1)q+1)\left(q^2+1\right)}{q^2} \tag{34}$$

$$= -2 - \left(q^2+\frac{1}{q^2}\right) + \left(q+\frac{1}{q}\right) \tag{35}$$

$$= -2 - 2\cos\frac{4\pi}{k+2} + 2\cos\frac{2\pi}{k+2}. \tag{36}$$

That is,

$$\cos\frac{4\pi}{k+2} - \cos\frac{2\pi}{k+2} + \cos\theta_k = -1. \tag{37}$$

We wish to show the above identity is not equivalent to any of the identities in Theorem 3.4, and hence θ_k cannot be a rational multiple of π. But we need to first verify the assumptions in that theorem.

We make four statements which can be verified by checking small values of k and applying Theorem 3.4, noting that when $k > 6$, $\frac{2\pi}{k+2}$ and $\frac{4\pi}{k+2}$ lie strictly between 0 and $\frac{\pi}{2}$. Assume $k \ge 3$.

(A) The only k for which $\cos\frac{2\pi}{k+2}$ is rational is $k = 4$,

$$\cos\frac{2\pi}{4+2} = \frac{1}{2}. \tag{38}$$

(B) The only k's for which $\cos\frac{4\pi}{k+2}$ is rational are $k = 4, 6, 10$,

$$\cos\frac{4\pi}{4+2} = -\frac{1}{2}, \quad \cos\frac{4\pi}{6+2} = 0, \quad \cos\frac{4\pi}{10+2} = \frac{1}{2}. \tag{39}$$

(C) The only k's for which neither $\cos\frac{2\pi}{k+2}$ nor $\cos\frac{4\pi}{k+2}$ is rational but certain nontrivial rational combinations of them is rational are $k = 3, 8$,

$$-\cos\frac{2\pi}{3+2} - \cos\frac{4\pi}{3+2} = \frac{1}{2}, \qquad \cos\frac{2\pi}{8+2} - \cos\frac{4\pi}{8+2} = \frac{1}{2}. \tag{40}$$

(D) Furthermore, the only k's for which $\cos\theta_k$ is rational are $k = 4, 8$,

$$\cos\theta_4 = 0, \quad \cos\theta_8 = -\frac{1}{2}. \tag{41}$$

Statement *D*) implies that for $k = 4, 8$, θ_k is a rational multiple of π. For all other k's, θ_k is not a rational multiple of π and in particular $\theta_k \neq 0, \frac{\pi}{2}, \pi$.

The above statements also imply for $k \geq 7$, $k \neq 8, 10$, none of $\cos\frac{4\pi}{k+2}$, $\cos\frac{2\pi}{k+2}$, or $\cos\theta_k$ is rational. Furthermore, for those values of k, for any two elements from $\{\cos\frac{4\pi}{k+2}, \cos\frac{2\pi}{k+2}, \cos\theta_k\}$, they cannot have a nontrivial rational combination which is rational. The above claim for the pair $\{\cos\frac{4\pi}{k+2}, \cos\frac{4\pi}{k+2}\}$ is clear from Statement *C*). For the other two pairs, say, $\{\cos\frac{4\pi}{k+2}, \cos\theta_k\}$, if they do not satisfy the claim, then one can substitute $\cos\theta_k$ with an expression of $\cos\frac{4\pi}{k+2}$ in Eq. 37, yielding a rational combination of $\cos\frac{4\pi}{k+2}$ and $\cos\frac{2\pi}{k+2}$ which is rational. That is a contradiction.

Then for $k \geq 7$, $k \neq 8, 10$, if θ_k is a rational multiple of π strictly between 0 and $\frac{\pi}{2}$, then Eq. 37 is an identity concerning a rational combination of the cosine of three distinct angles satisfying the conditions in Theorem 3.4. However, this identity is not equivalent to any of those in that theorem, a contradiction.

If θ_k is a rational multiple of π strictly between $\frac{\pi}{2}$ and π, then Eq. 37 can be written as,

$$\cos\frac{4\pi}{k+2} - \cos\frac{2\pi}{k+2} - \cos(\pi - \theta_k) = -1. \tag{42}$$

Applying the same argument to the new equation leads to a similar contradiction. This shows that for $k \geq 7$, $k \neq 8, 10$, θ_k is not a rational multiple of π.

The remaining cases to check are $k = 3, 5, 6, 10$. The corresponding identity of Eq. 37 for these values of k can be simplified below.

$$\cos\theta_3 = \frac{\sqrt{5}-2}{2}, \ \cos\theta_5 = \cos\frac{3\pi}{7} + \cos\frac{2\pi}{7} - 1, \ \cos\theta_6 = \frac{\sqrt{2}-2}{2},$$
$$\cos\theta_{10} = \frac{\sqrt{3}-3}{2}. \tag{43}$$

It can be checked directly by a computer program or by applying Theorem 3.4 that the above θ_k's are not rational multiple of pi. This completes the proof that the eigenvalues of A are of infinite order for $k \geq 3$, $k \neq 4, 8$.

Proving B has infinite order.

Denote the eigenvalues of B by $e^{\pm\theta_k i}$, $0 \le \theta_k \le \pi$.

$$2\cos\theta_k = \mathrm{tr}(B) = \frac{\left(q^2+1\right)\left((q-1)q\left(q^2+1\right)+1\right)}{q^3} \tag{44}$$

$$= -2 + (q^3 + \frac{1}{q^3}) - \left(q^2 + \frac{1}{q^2}\right) + 2\left(q + \frac{1}{q}\right) \tag{45}$$

$$= -2 + 2\cos\frac{6\pi}{k+2} - 2\cos\frac{4\pi}{k+2} + 4\cos\frac{2\pi}{k+2}. \tag{46}$$

That is,

$$2\cos\frac{2\pi}{k+2} - \cos\frac{4\pi}{k+2} + \cos\frac{6\pi}{k+2} - \cos\theta_k = 1. \tag{47}$$

The rest of the proof is completely similar to the case of the matrix A by repeatedly applying Theorem 3.4. We leave the details as an exercise for curious readers.

Proving $\mathbf{W \neq I}$.

Note that $W \neq I$ if and only if $\mathrm{Tr}(W) \neq 2$. Assume $\mathrm{Tr}(W) = 2$. Then,

$$2 = -\frac{((q-1)q+1)\left(q^4 - 2q^3 - 2q + 1\right)}{q^3} \tag{48}$$

$$= 4 - \left(q^3 + \frac{1}{q^3}\right) + 3\left(q^2 + \frac{1}{q^2}\right) - 3\left(q + \frac{1}{q}\right) \tag{49}$$

$$= 4 - 2\cos\frac{6\pi}{k+2} + 6\cos\frac{4\pi}{k+2} - 6\cos\frac{2\pi}{k+2}. \tag{50}$$

That is,

$$\cos\frac{6\pi}{k+2} - 3\cos\frac{4\pi}{k+2} + 3\cos\frac{2\pi}{k+2} = 1. \tag{51}$$

That the above identity is fake can be checked directly for small values $k \le 10$ and by Theorem 3.4 for $k \ge 11$. □

Appendix A Anyon models

Mathematically, an anyon model is characterized by the structure of a unitary modular tensor category (MTC). To avoid abstract categorical language, we describe an MTC with a set of concrete data. The content and figures contained in this section are adapted from the second named author's lecture notes [28].

Label set. Associated with each anyon model is a finite set

$$L = \{a, b, c, \ldots\} \tag{52}$$

consisting of all the possible anyon types in a topological phase. The ground state is considered as a special trivial anyon type, and is usually denoted by $\mathbf{1} \in L$. For each anyon type $x \in L$, there exists $\bar{x} \in L$ corresponding to the anti-particle (i.e., the dual anyon type) of x. We require that $\bar{\mathbf{1}} = \mathbf{1}$ and $\bar{\bar{x}} = x$.

Fusion rule. For $a, b \in L$, fusing a and b produces different possible anyon types. Formally, it is written as,

$$a \otimes b = \bigoplus_{c \in L} N_{ab}^{c}\, c, \tag{53}$$

where N_{ab}^{c} denotes the number of different channels of fusing a and b to result in the output c. If there is no way to obtain c from the fusion, then $N_{ab}^{c} = 0$. One can also view the equality in the above equation from an alternative perspective. Namely, the composite type of a and b is a superposition of all possible anyon types with each type c appearing in N_{ab}^{c} copies. If $N_{ab}^{c} > 0$, we say c is a *total type* or *total charge* of a and b, and call the triple $(a, b; c)$ *admissible*. The collection of the integers $\{N_{ab}^{c} \mid a, b, c \in L\}$ is called the fusion rule. The fusion rule should satisfy the following requirements.

(A) The fusion rule is commutative, i.e., $a \otimes b = b \otimes a$, implying

$$N_{ab}^{c} = N_{ba}^{c}, \quad \forall a, b, c. \tag{54}$$

(B) The dual of $a \otimes b$ as a composite equals $\bar{b} \otimes \bar{a}$, implying

$$N_{ab}^{c} = N_{\bar{b}\bar{a}}^{\bar{c}}, \quad \forall a, b, c. \tag{55}$$

(C) $\mathbf{1} \otimes a = a$, implying

$$N_{\mathbf{1}a}^{b} = \delta_{a,b}, \quad \forall a, b. \tag{56}$$

(D) $\mathbf{1}$ is a total type of a and b if and only if $a = \bar{b}$, implying

$$N_{ab}^{\mathbf{1}} = \delta_{a,\bar{b}}, \quad \forall a, b. \tag{57}$$

(E) The fusion rule is associative, i.e., $(a \otimes b) \otimes c = a \otimes (b \otimes c)$, implying

$$\sum_{p \in L} N_{ab}^{p} N_{pc}^{d} = \sum_{q \in L} N_{aq}^{d} N_{bc}^{q}, \quad \forall a, b, c, d, \tag{58}$$

For simplicity, in the following discussions **we will assume N_{ab}^{c} is either** 0 **or** 1, i.e., the anyon model is multiplicity-free. This already covers a large family of anyon models including the ones considered in the current paper.

State space. For anyon types $c, a_1, \ldots, a_n$, denote by $V_c^{a_1 a_2 \cdots a_n}$ the space of states representing n anyons $a_1, \ldots, a_n$ with total charge c. The dimension and bases of these spaces are described inductively as follows.

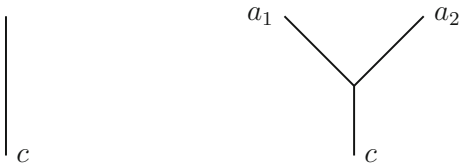


Fig. 7 (Left) A canonical basis of V_c^c; (Right) A (noncanonical) basis of $V_c^{a_1 a_2}$

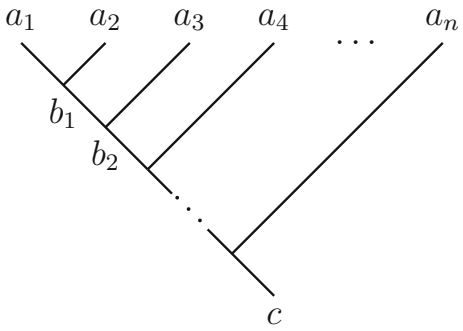


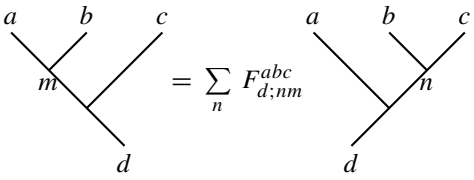
Fig. 8 A basis of $V_c^{a_1 a_2 \cdots a_n}$ corresponding to a binary tree

For $n = 1$, $V_c^{a_1} = 0$ if $c \neq a_1$, and V_c^c is one-dimensional with a canonical basis denoted by the left diagram of Fig. 7. One can think of the diagram representing the state obtained by 'doing nothing' to an existent anyon c.

For $n = 2$, $V_c^{a_1 a_2} = 0$ if $N_{a_1 a_2}^c = 0$, and $V_c^{a_1 a_2}$ is one-dimensional otherwise, with a noncanonical basis denoted by the right diagram in Fig. 7. One can then think of the diagram representing the state obtained from the process of splitting c into the pair a and b, where and throughout the context, the time direction for physical processes is assumed to be from bottom to top. This choice of basis is not canonical as one can multiply an arbitrary phase to it. We will use the diagrams in Fig. 7 as building blocks to describe bases of multi-anyon spaces.

For $n \geq 3$, take an upward-growing binary tree with one root at the bottom and n leaves at the top. See Fig. 8 for an illustration. It is to be understood that the tree is constructed using the two diagrams in Fig. 7. Label the root by c and the leaves, from left to right, by $a_1, a_2, \ldots, a_n$. Now label each internal edge e by an anyon type b_e such that at each fork, the relevant labels are admissible. Then, the binary tree with all possible labels $\{b_e\}$ of internal edges forms a basis of $V_c^{a_1 a_2 \cdots a_n}$. For each labeled binary tree, one can similarly interpret the state it represents as a splitting process. For example, the state represented by the tree in Fig. 8 is obtained by splitting c into b_{n-2} and a_n, followed by splitting b_{n-2} into b_{n-3} and a_{n-1}, …, followed by splitting b_1 into $b_0 = a_1$ and a_2. Such a basis is called a *splitting-tree basis*.

For the case of $n = 3$, there are exactly two such binary trees as shown on both sides of Equation (59), each of which provides a basis of V_d^{abc}. Each tree has one internal edge. The basis corresponding to the tree on the left side of the equation consists of all possible labelings m of the internal edge so that $(a, b; m)$ and $(m, c; d)$ are both admissible. Similarly, the basis for the tree on the right side consists of labelings n of the internal edge so that $(b, c; n)$ and $(a, n; d)$ are both admissible. Denote the matrix change between the two bases by F_d^{abc}. More explicitly,



(59)

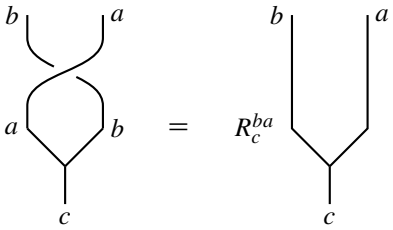
where $F^{abc}_{d;nm}$ is the (n, m)-entry of F^{abc}_{d}, and the sum is over all labelings n as described above. Note that, here the anyon types n and m are used as the indices of the entries of F^{abc}_{d}. We call F^{abc}_{d} an F-matrix, its entries F-symbols or $6j$-symbols, and the identity in Equation (59) an F-move.

Using the F-move or its inverse, we can relate any two splitting-tree bases of $V_c^{a_1 a_2 \cdots a_n}$. For V_e^{abcd}, there are exactly five splitting-tree bases, and Fig. 9 shows the F-moves connecting them. In particular, starting from the basis labeled by ①, there are two ways of performing F-moves to obtain the basis labeled by ③, namely, either via the path ① → ② → ③ or via the path ① → ⑤ → ④ → ③. Since both ways induce a basis change between ① and ③, this introduces some constraints on the F-symbols, namely,

$$F^{mcd}_{e;zn} F^{abz}_{e;ym} = \sum_{x \in L} F^{abc}_{n;xm} F^{axd}_{e;yn} F^{bcd}_{y;zx}, \quad \forall a, b, c, d, e, m, n, y, z. \tag{60}$$

Equation 60 is known as the Pentagon equations. It is a nontrivial fact that the Pentagon equations guarantee that the change between splitting-tree bases via F-moves for an arbitrary state space is consistent.

Braiding. The process of swapping positions of anyons is called a braiding. Since anyons live in two-dimensional space, a counterclockwise braiding has a different world line from that of a clockwise braiding. The world line of a sequence of braidings of multi-anyons is a braid diagram, and hence the naming of the process. A braiding induces a unitary transformation on the state space. Consider two anyons a and b with total type c. A counterclockwise braiding of a and b maps a state in V_c^{ab} to one in V_c^{ba}. Since both spaces have dimension one, there exists a phase R_c^{ba} such that the following equality holds,



(61)

The above equality is called an R-move, and $\{R_c^{ab}\}$ is called an R-symbol. Since a counterclockwise braiding followed by a clockwise braiding is equivalent to the

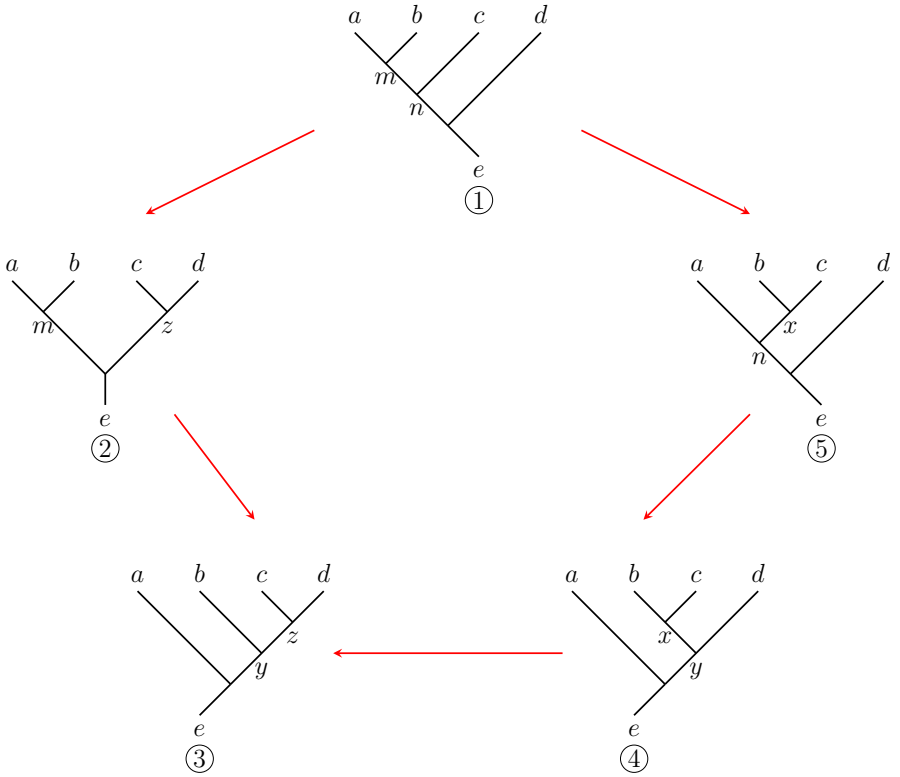
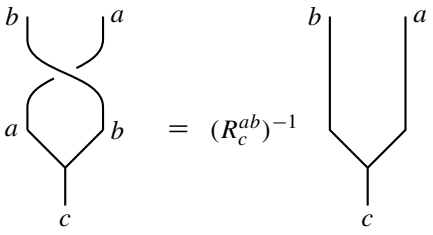


Fig. 9 The five splitting-tree bases of V_e^{abcd} and the F-moves connecting them

identity process, we have,



(62)

Consider the space V_d^{abc}, and braid a with b and c. Each node in Fig. 10 represents a basis of V_d^{bca}, and performing an F-move or R-move change from one basis to another. To change from basis ① to basis ③, one can follow either the path ① → ② → ③ or the path ① → ⑥ → ⑤ → ④ → ③. Consequently, we obtain the hexagon equation,

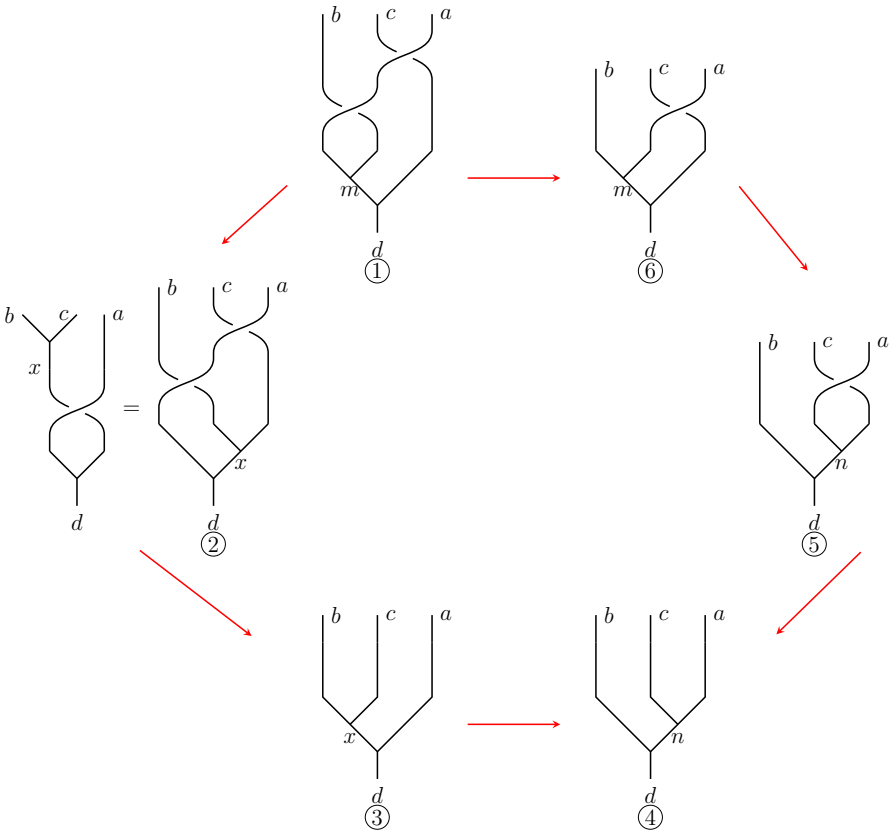


Fig. 10 Consistency conditions for braidings on V_d^{abc}

$$R_m^{ba} F_{d;nm}^{bac} R_n^{ca} = \sum_{x \in L} F_{d;xm}^{abc} R_d^{xa} F_{d;nx}^{bca}. \tag{63}$$

By replacing the counterclockwise braidings in Fig. 10 with clockwise braidings, we obtain another hexagon equation,

$$(R_m^{ab})^{-1} F_{d;nm}^{bac} (R_n^{ac})^{-1} = \sum_{x \in L} F_{d;xm}^{abc} (R_d^{ax})^{-1} F_{d;nx}^{bca}. \tag{64}$$

Topological spin. Each anyon type a has an (intrinsic) topological spin θ_a which is always a root of unity. The type a is said to be bosonic if $\theta_a = 1$, fermionic if $\theta_a = -1$, and semionic if $\theta_a = i$. The topological spins are required to satisfy the following conditions.

(A) The trivial anyon is bosonic,

$$\theta_{\mathbf{1}} = 1. \tag{65}$$

(B) An anyon and its dual have equal topological spin,

$$\theta_a = \theta_{\bar{a}}, \quad \forall a \in L. \tag{66}$$

(C) Whenever c is a total type of a and b, we have

$$\theta_c \theta_a^{-1} \theta_b^{-1} = R_c^{ab} R_c^{ba}. \tag{67}$$

Quantum dimension. For each anyon type a, define an $|L| \times |L|$ matrix N_a whose (b, c)-entry is $N_{ab}^c = N_{ba}^c$. Hence, the entries of N_a are nonnegative integers. By the Perron–Frobenius theorem, N_a has an eigenvalue $\dim(a)$, called the Frobenius–Perron dimension of a, which is greater than or equal to, in absolute value, any other eigenvalues. In the anyon model, we also call $\dim(a)$ the quantum dimension of a. To get a sense of what $\dim(a)$ measures, consider the dimension of the space of n type-a anyons with total type $\mathbf{1}$. We use the splitting-tree basis in Fig. 8 with $a = a_1 = \cdots = a_n$, $\mathbf{1} = c$ to compute the dimension for large n,

$$\sum_{b_1,\ldots,b_{n-2}} N_{aa}^{b_1} N_{b_1 a}^{b_2} \cdots N_{b_{n-3}a}^{b_{n-2}} N_{b_{n-2}a}^{\mathbf{1}} = \sum_{b_1,\ldots,b_{n-3}} N_{aa}^{b_1} N_{b_1 a}^{b_2} \cdots N_{b_{n-3}a}^{\bar{a}} \tag{68}$$

$$= \left((N_a)^{n-2}\right)_{a\bar{a}} \overset{n\to\infty}{\sim} \dim(a)^{n-2}. \tag{69}$$

Thus, $\dim(a)$ measures the asymptotic size of the space of n type-a anyons. Apparently, $\dim(a) \geq 1$. An anyon a is called *Abelian* if $\dim(a) = 1$, and *non-Abelian* otherwise.

***S*-matrix.** Define the $|L| \times |L|$ modular S-matrix with entries,

$$S_{ab} := \theta_a^{-1} \theta_b^{-1} \sum_{c \in L} N_{\bar{a}b}^c \, \theta_c \dim(c). \tag{70}$$

The S-matrix is required to be invertible.

To summarize, an anyon model or a unitary MTC is described by a label set, fusion rule, F-symbols, R-symbols, and topological spins, from which one can derive quantum dimensions and the S-matrix. These data should satisfy various compatibility conditions as listed in this section.

Appendix B Mathematica code

Below we list the Mathematica code to compute some of the matrices used in Sect. 3.2 and 3.3 including F, $\tilde{R}$, A, B, and W.

```
1
2 Clear[q];
```

```
QuantumInteger[n_] := (q^(n/2) - q^(-n/2))/(q^(1/2) - q
    ^(-1/2));
F = FullSimplify[{{-1,
Sqrt[QuantumInteger[3]]}, {Sqrt[QuantumInteger[3]], 1}}/
QuantumInteger[2]];
Rtilde = DiagonalMatrix[{q^(-1/2), -q^(1/2)}]*I;
A = Simplify[
MatrixPower[Rtilde, 2] . F . MatrixPower[Rtilde, 4] . F];
B = Simplify[
MatrixPower[Rtilde, 2] . F . MatrixPower[Rtilde, 6] . F];
W = Simplify[A . B . Inverse[A] . Inverse[B]];
```

Acknowledgements S.X.C is partly supported by NSF grant CCF-2006667, Quantum Science Center (led by ORNL), and ARO MURI.

Author contributions S. C. designed the project. A.K. completed the project under the guidance of S.C. A.K and S.C. wrote the manuscript together.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Wen, X.-G.: Topological orders in rigid states. Int. J. Mod. Phys. B **4**(02), 239–271 (1990)
2. Freedman, M.H., Larsen, M., Wang, Z.: A modular functor which is universal for quantum computation. Commun. Math. Phys. **227**, 605–622 (2002)
3. Kitaev, A.Y.: Fault-tolerant quantum computation by anyons. Ann. Phys. **303**(1), 2–30 (2003)
4. Nayak, C., Simon, S.H., Stern, A., Freedman, M., Das Sarma, S.: Non-abelian anyons and topological quantum computation. Rev. Mod. Phys. **80**(3), 1083 (2008)
5. Wang, Z.: Topological Quantum Computation. Number 112. American Mathematical Soc. (2010)
6. Aghaee, M., Ramirez, A.A., Alam, Z., Ali, R., Andrzejczuk, M., Antipov, A., Astafev, M., Barzegar, A., Bauer, B., Becker, J. et al.: Interferometric single-shot parity measurement in an InAs-Al hybrid device. Preprint at arXiv:2401.09549 (2024)
7. Aghaee, M., Akkala, A., Alam, Z., Ali, R., Alcaraz Ramirez, A., Andrzejczuk, M., Antipov, A.E., Aseev, P., Astafev, M., Bauer, B., et al.: InAs-Al hybrid devices passing the topological gap protocol. Phys. Rev. B **107**(24), 245423 (2023)
8. Minev, Z.K., Najafi, K., Majumder, S., Wang, J., Stern, A., Kim, E.A., Jian, C.M., Zhu, G.: Realizing string-net condensation: Fibonacci anyon braiding for universal gates and sampling chromatic polynomials. Preprint at arXiv:2406.12820 (2024)
9. Nakamura, J., Liang, S., Gardner, G.C., Manfra, M.J.: Direct observation of anyonic braiding statistics. Nat. Phys. **16**(9), 931–936 (2020)
10. Shibo, X., Sun, Z.-Z., Wang, K., Li, H., Zhu, Z., Dong, H., Jinfeng Deng, X., Zhang, J.C., Yaozu, W., et al.: Non-abelian braiding of Fibonacci anyons with a superconducting processor. Nat. Phys. **20**(9), 1469–1475 (2024)
11. Wu, Y.-S.: Simulating the hadamard gate in the Fibonacci disk code for universal topological quantum computation. The Innovation **4**(6) (2023)
12. Zhan, Y.-M., Chen, Y.-G., Chen, B., Wang, Z., Yue, Yu., Luo, X.: Universal topological quantum computation with strongly correlated Majorana edge modes. New J. Phys. **24**(4), 043009 (2022)
13. Witten, E.: Quantum field theory and the jones polynomial. Commun. Math. Phys. **121**(3), 351–399 (1989)
14. Freedman, M.H., Larsen, M.J., Wang, Z.: The two-eigenvalue problem and density of Jones representation of braid groups. Commun. Math. Phys. **228**, 177–199 (2002)

15. Cui, S.X., Tian, K.T., Vasquez, J.F., Wang, Z., Wong, H.M.: The search for leakage-free entangling Fibonacci braiding gates. J. Phys. A Math. Theor. **52**(45), 455301 (2019)
16. Bruguières, A.: Double braidings, twists and tangle invariants. J. Pure Appl. Algebra **204**(1), 170–194 (2006)
17. Liptrap, J.: From Hypergroups to Anyonic Twines. PhD thesis, University of California Santa Barbara (2010)
18. Bonderson, P.H.: Non-Abelian Anyons and Interferometry. PhD thesis, California Institute of Technology (2007)
19. Simon, S.H., Bonesteel, N.E., Freedman, M.H., Petrovic, N., Hormozi, L.: Topological quantum computing with only one mobile quasiparticle. Phys. Rev. Lett. **96**(7), 070503 (2006)
20. Cui, S.X., Wang, Z.: Universal quantum computation with metaplectic anyons. J. Math. Phys. **56**(3) (2015)
21. Rowell, E., Wang, Z.: Mathematics of topological quantum computing. Bull. Am. Math. Soc. **55**(2), 183–238 (2018)
22. Wess, J., Zumino, B.: Consequences of anomalous ward identities. Phys. Lett. B **37**(1), 95–97 (1971)
23. Witten, E.: Global aspects of current algebra. Nuclear Phys. B **223**(2), 422–432 (1983)
24. Turaev, V.G.: Quantum Invariants of Knots and 3-Manifolds. de Gruyter (2010)
25. Kitaev, A.Y.: Quantum computations: algorithms and error correction. Russ. Math. Surv. **52**(6), 1191 (1997)
26. Aharonov, D., Ben-Or, M.: Fault-tolerant quantum computation with constant error rate. SIAM J. Comput. **38**(4), 1207 (2008)
27. Conway, J., Jones, A.: Trigonometric diophantine equations (on vanishing sums of roots of unity). Acta Arith. **30**, 229–240 (1976)
28. Cui, S.X.: Topological quantum computation. https://www.math.purdue.edu/~cui177/Lecture_Combined.pdf (2018)