# Fibonacci Anyons Versus Majorana Fermions: A Monte Carlo Approach to the Compilation of Braid Circuits in SU(2)<sub>k</sub> Anyon Models

Emil Génetay Johansen<sup>®</sup> and Tapio Simula<sup>®</sup>

Optical Sciences Centre, Swinburne University of Technology, Melbourne 3122, Australia

(Received 20 August 2020; revised 15 December 2020; accepted 21 January 2021; published 1 March 2021; corrected 6 August 2021)

We study  $SU(2)_k$  anyon models, assessing their prospects for topological quantum computation. In particular, we compare the Ising (k = 2) anyon and Fibonacci (k = 3) anyon models, motivated by their potential for future realizations based on Majorana fermion quasiparticles or exotic fractional quantum Hall states, respectively. The quantum computational performance of the different anyon models is quantified at the single-qubit level by the difference between a target unitary operator and its approximation realized by anyon braiding. To facilitate efficient comparisons, we develop a Monte Carlo enhanced Solovay-Kitaev quantum compiler algorithm that finds near-optimal braid words in polynomial time from the exponentially large search tree. Since universal quantum computation cannot be achieved within the Ising anyon model by braiding alone, we introduce an additional elementary phase gate to model a nontopological measurement process, which restores universality of the anyon model at the cost of breaking the full topological protection. We model conventional kinds of decoherence processes algorithmically by introducing a controllable noise term to all nontopological gate operations. We find that, for reasonable levels of decoherence, even the hybrid Ising anyon model retains a significant topological advantage over a conventional, nontopological, quantum computer. Furthermore, we find that only surprisingly short anyon braids are ever required to be compiled due to the gate noise exceeding the intrinsic error of the braid words already for word lengths of the order of 100 elementary braids. We conclude that the future for hybrid topological quantum computation remains promising.

DOI: 10.1103/PRXQuantum.2.010334

# I. INTRODUCTION

Topological phases of matter have attracted a significant amount of attention in recent times due to the diversity of emerging physical phenomena heralded by them [1-5]. Systems with only two spatial dimensions have proven to be particularly rich as their excitations do not adhere to the spin-statistics theorem that conventionally divides all particles into bosons or fermions. This theorem is one of the great triumphs of (3 + 1)-dimensional quantum field theory, yet its validity breaks down in lower-dimensional systems with far reaching consequences. This was first discovered in 1977 by Myrheim and Leinaas [6], propelling significant new activity in this field. Twenty years later, in 1997, Kitaev conceived the idea that such exotic phases of matter may hold the key to fault tolerant quantum computation [3], frequently referred to as topological quantum computation (TQC). Within the TQC paradigm, error-correcting schemes are not necessary, in principle, as the states used for encoding information possess an intrinsic *topological* protection against decoherence from the conventional types of external noise sources [7–11]. This concept is predicated on the principle of topological equivalence, which ensures that the configurations remain invariant under diffeomorphisms. The quasiparticle excitations in these systems are called *anyons* [6,7,12–15] as they are not restricted to be bosons or fermions and instead realize fractional statistics.

Perhaps the two most celebrated examples of anyon models are the Ising anyon and Fibonacci anyon models. While the Fibonacci model is computationally universal, which means that it is capable of realizing any quantum algorithm, the Ising anyon model is not. Although anyons are elusive, it is believed that they might emerge as quasiparticle excitations in certain specially engineered condensed matter systems. However, current research indicates that Ising anyons may be a far more accessible platform for TQC. The Majorana fermion is an incarnation of the Ising anyon, i.e., it obeys the same braiding and fusion rules. Majorana fermion quasiparticles are expected to be found in chiral p-wave paired Fermi superfluids [16–19], topological superconductors [20–22], semiconducting nanowires [23–26], and certain quantum Hall fluids [27,28] in dimensions d < 3. Recently, quantized vortices

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

[29] have been used for dressing full-shell nanowires [30], combining proximitized-wire and pure vortex schemes as a pathway to realizing Majorana zero modes. Fibonacci anyons, on the other hand, might be out of reach for the time being, although it is thought that they could exist in some very exotic fractional quantum Hall fluids with filling fraction  $\nu = 12/5$  [31–33] and as quasiparticles in Kondo systems [34].

In a topological quantum computer the quantum gates are realized by enacting certain transformations on the anyons that in a braid-based TQC will be implemented in the hardware by braiding the anyon world lines [10]. More recently, measurement-based topological quantum computation protocols [35,36] that avoid the need of having to move the anyons in physical space by using anyonic quantum state teleportation to enact the effective braiding transformations via forced measurements of the topological charge of the anyons have been rapidly advancing [37–39]. Irrespective of the hardware-level implementation details, before any quantum computations can be performed, one must find a mapping between the desired quantum gates and their corresponding braids (or measurement protocols) that must be realized on the anyon hardware. This is the quantum compilation problem. A generic quantum compilation is notoriously hard, which is why various techniques have been developed in order to compile gates with good accuracy. Some methods include hash function techniques [40], algebraic techniques [41,42], and machine learning [43]. The method developed in Ref. [41] is a number theoretic approach in which the ring structure of the set generated by the elementary gates is identified, and from that an approximation to a given target gate is constructed. This method is very powerful but not generic in the sense that it would work for any gate set, since it relies on the structure of the generator set. The algorithm discussed in Ref. [42] is known as the Solovay-Kitaev algorithm (SKA). Contrary to the number theoretic technique due to Kliuchnikov, the Solovay-Kitaev compiler is completely generic although less efficient. A brief review on a range of quantum compilation approaches beyond the brute force method can be found in Ref. [8].

In this paper we develop a Monte Carlo enhanced Solovay-Kitaev algorithm (MCESKA), which inherits its generic structure from the SKA. It is straightforward to modify the MCESKA to implement a variety of constraints such as limiting the number of noisy conventional gates employed in nonuniversal models, which in turn opens up the possibility of finding a better tradeoff between logical compilation error and error due to noise in nontopological gates. From a practical perspective, this is a highly valuable feature in systems where hardware resources are scarce and limited by decoherence. We return to the details of the SKA and the MCESKA in Sec. II B, after a more general discussion on the underlying Monte Carlo techniques. In particular, we demonstrate a clear advantage of using the MCESKA, when compared to the original SKA. Recently, in Ref. [43] a reinforcement learning technique was deployed in the context of the quantum compilation problem, which appears to have a similar braid word length versus error performance as the MCESKA. Since it is also fully generic, it will be interesting to see if it too allows accommodating extra functionality such as suppressing the fraction of noisy gates required in hybrid TQC implementations. In Sec. III, we use the MCESKA for assessing the prospects of various  $SU(2)_k$  anyon models with a particular emphasis on the Ising anyon (k = 2) and Fibonacci anyon (k = 3) models for TQC, including the k = 4, 5, 6, 8 models to provide a basis for more general comparison. The Ising anyon model (k = 2) and the k = 4 model are not computationally universal, which is why we have supplemented their natural set of braid generators with an additional nontopological gate that is prone to cause errors due to the influence of noise. Braid compilation for nonabelian anyons has previously been considered in Refs. [44,45] for single- and double-qubit systems. The compilation was carried out for specific gates and no noise was considered since the fully topologically protected Fibonacci model was used. In our work, we compile braids for arbitrary unitary gates and the computational performance of the various anyon models is compared for varying levels of noise. We conclude this work in Sec. IV with a summary and discussion. For the sake of completeness, in Appendix A we provide a brief theoretical background to anyons and TQC and in Appendix **B** some rudiments of the  $SU(2)_k$  anyon models are outlined.

# **II. QUANTUM COMPILATION**

When a circuit model of computation is carried out in a quantum computer, the state of the system is acted upon by a series of logic gates. These logical operations are induced by physical processes in the system. In order to realize a particular logic gate, we need to know what action it corresponds to in the physical hardware. In TQC, these transformations are realized by braiding the anyons in a very particular way, which raises the question how to deduce what braids should be performed in order to realize the desired computation. A whole research area centered around this problem, known as quantum compiling, exists within the field of quantum computation. The key objective of quantum compiling is to develop an algorithm that, given a target unitary gate, will search for sequences of braid operations that are approximating this gate to the desired accuracy.

Because of the combinatorial nature of the problem, we may represent the search space as a tree structure. In particular, if we consider the braid group on three strands, since there are four generators in the group, this tree is a 4-ary tree shown in Fig. 1. Considering this graphical structure,



FIG. 1. The search space with node labels. The particular path in green corresponds to the braid word  $S = I \sigma_2^{-1} \sigma_1 \cdots \sigma_1^{-1} \sigma_2$ . The braid generators  $\sigma_i$  are defined explicitly in Appendix B 4.

the exponential growth of the number of leaf nodes with the length of the braid word (height h of the tree) becomes evident. More precisely, given a tree height h, there are a total of  $4^h$  leaf nodes. Let us now consider the tree in the context of quantum compilation.

The goal is to find a sequence of elementary braids S, such that the distance d = ||S - T|| to the target unitary matrix T is less than  $\epsilon$ , where  $\epsilon$  is the desired error tolerance. More specifically, in order to compare the various compiler algorithms as well as anyon models, we need to establish a notion of metric in the space of unitary gates. When a unitary matrix U is approaching a unitary target matrix  $U_0$ , the product  $U_0 U^{\dagger}$  approaches identity such that the error distance d goes to 0. Hence, the trace of this product is a number that approaches n, where n is the dimension of the matrix. This motivates the definition of the fidelity measure in the space of  $2 \times 2$  unitary matrices [8,41]

$$d(U_0, U) = \sqrt{1 - \frac{|\mathrm{Tr}(U_0 U^{\dagger})|}{2}}.$$
 (1)

This function has global phase invariance, i.e., the value of the function for a given target matrix  $U_0$  is the same for all matrices U that are equal up to a global phase change. It is also strictly positive, symmetric [i.e., d(V, W) = d(W, V)], and satisfies the triangle inequality  $d(V, W) \le d(V, U) +$ d(U, W). Each sequence of braids corresponds to a unique path in the search tree, so instead of regarding the problem purely as a constrained optimization problem, we are interested in finding the path to a specific leaf node in the tree, such as the path highlighted in green in Fig. 1. Note that, for an arbitrary N-ary tree, given a level l, there are a total of  $N^l$  leaf nodes. Hence, we may express the total number of nodes in the tree as a geometric sum

$$1 + N + N^{2} + \dots + N^{h} = \sum_{l=0}^{h} N^{l} = \frac{N^{h+1} - 1}{N - 1}.$$
 (2)

Clearly, finding the one leaf node that leads to the smallest error distance d is an inherently exponentially complex

problem, which would demand an enormous amount of computational resources. Although performing an exhaustive search is the only known method for finding the unique path to a specific leaf node, good alternative approaches exist. It is possible to reduce the vast size of the search space by considering the algebraic properties of the braid generators and the intrabraid symmetries [8]. Finding redundancies in the search space allows pruning whole branches from the tree.

In Fig. 2 we illustrate the compilation problem on the Bloch sphere using Fibonacci anyons. The exact Hadamard gate takes the initial state (green arrow) to a superposition state (brown arrow). The blue and red arrows are the optimal state approximations reached by braiding the anyons 10 and 15 times, respectively. Although increasing the length of the braid word takes the final state smoothly ever closer to the target state, the intermediate, intrabraid, states (colored markers) are seemingly randomly scattered on the Bloch sphere, meaning that it is not possible to determine the best braid letters locally within the braid word by conventional optimization means. Specifically, adding just a single letter to the end of a braid word may result in all of the letters changing.



FIG. 2. Fibonacci anyon braid word approximations for the Hadamard gate. The initial state  $|0\rangle$  is shown by the green arrow on the Bloch sphere. The exact final state (brown arrow) is shown together with the optimal (obtained via brute force search) braid word approximations of lengths 10 (blue) and 15 (red). The intermediate states for the latter case are shown by numbered markers that indicate the order of the letters in the braid word sequence. Only 14 of the 15 intermediate states are visible because the first two braid letters only apply a phase to the initial state. The braid word used in this demonstration is  $\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_1\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_1\sigma_2^{-1}\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_1^{-1}$ .

## A. A Monte Carlo approach

Let us consider the 4-ary tree shown in Fig. 1. Each path in the tree corresponds to a particular braid word. Let  $\Sigma$ denote the set of generators and  $|\Sigma|$  the order of that set. This implies that, for a simple random walk, under the condition that the tree is directed, the probability of moving from a parent node  $n_0$  to a specific child node  $n_i$ , where *i* is running from 1 to  $|\Sigma| + 1$  (number of child nodes plus one parent node), is

$$P(n_0 \to n_i) = \begin{cases} \frac{1}{|\Sigma|} & \text{if } n_i = \text{child node,} \\ 0 & \text{if } n_i = \text{parent node.} \end{cases}$$
(3)

With this particular definition we are only considering directed trees as the probability of going backwards is 0. We would then like to find the path from the root  $\mathbb{I}$  to some node *n* at level *l*. Thus, if we simulate a simple random walk according to the probability distribution defined in Eq. (3), the probability of finding this node is

$$P(I \to n) = \underbrace{\frac{1}{|\Sigma|} \frac{1}{|\Sigma|} \cdots \frac{1}{|\Sigma|}}_{l \text{ times}} = \frac{1}{|\Sigma|^{l}}.$$
 (4)

In this model, no move is more favorable than any other, which is obviously a quite simplistic assumption. A better model would be to condition the probability distribution with respect to the present state. Mathematically, we can formulate this as a Markov chain from node  $n_i$  to node  $n_j$  with corresponding states  $s_i$  and  $s_j$ :

$$P(n_{i} \rightarrow n_{j}) = P(a_{k}|s_{j-1})P(s_{j-1})$$
  
=  $P(a_{k}|s_{j-1})P(a_{q}|s_{j-2})P(s_{j-2})$   
=  $P(a_{k}|s_{j-1})P(a_{q}|s_{j-2})P(a_{p}|s_{j-3})\cdots P(s_{0}).$   
(5)

Here we have used the Bayesian property P(A) = P(A|B)P(B). The probabilities  $P(a_i|s_j)$  can be interpreted as the probability of taking action  $a_i$ , given the present state  $s_j$ . The remaining problem is how to best model these conditional probabilities.

#### 1. Mapping the problem onto a $\mathbb{Z}_N$ spin chain

The core idea of our approach is that the problem of finding the right path in the tree can be mapped onto a onedimensional spin chain for which we are searching for the ground state (see Fig. 3). First, let us assign to each generator in the set  $\Sigma$  a spin. Here we consider a set of four generators  $\Sigma = \{\sigma_1, \sigma_2, \sigma_2^{-1}, \sigma_1^{-1}\}$ , which generate the tree



FIG. 3. Mapping between a braid word (a) and a spin chain (b).

in Fig. 1. We define the following map  $f: \Sigma \to \mathbb{Z}_4$ :

$$f(\sigma) = \begin{cases} \uparrow & \text{if } \sigma = \sigma_1, \\ \downarrow & \text{if } \sigma = \sigma_1^{-1}, \\ \rightarrow & \text{if } \sigma = \sigma_2, \\ \leftarrow & \text{if } \sigma = \sigma_2^{-1}. \end{cases}$$
(6)

Thus, for a generic anyon model with  $|\Sigma|$  generators, we can map this problem onto a  $\mathbb{Z}_{|\Sigma|}$  lattice model.

#### 2. A thermodynamic picture

Our ultimate goal is to find a path S corresponding to a braid word that, given a metric, minimizes the distance dto the target unitary gate  $U_0$ . We may establish the equivalence  $d \leftrightarrow E$  in the spin chain representation, where E is the energy of the system. Thus, we implicitly define a Hamiltonian H of our spin chain via  $E = \langle H \rangle$ . Instead of trying to find the smallest error we are interested in finding the state vector corresponding to the known ground state energy of the system. In comparison to the standard Ising lattice model, our implicitly defined spin chain Hamiltonian will most likely exhibit other symmetries. The twofold degeneracy of the ground state in the Ising spin model is illustrated in Fig. 4(a) and can be viewed as a two-dimensional version of a Mexican hat function, which is invariant only under the  $\mathbb{Z}_2$  subgroup of the full U(1) symmetry. In our scenario the function will look more like a wrinkled Mexican hat function, Fig. 4(b), which exhibits various discrete symmetries corresponding to a number of local minima. Therefore, in the thermodynamic picture, the error convergence process may be regarded as a series of successive symmetry breaking processes, gradually bringing the system to lower and lower energies.

Ideally, we would like to deduce all of the symmetries as that would allow us to reduce the information entropy, but since these symmetries depend explicitly on the target matrix, it is difficult to derive any generally applicable results. This is where the Monte Carlo approach is useful. From the thermodynamic perspective, we would ideally like to find the global minimum of the system, or at least a local minimum that lies close to the global one. Therefore, when the system gets trapped in a local minimum, we need to be able to repeatedly climb over barriers and roll



FIG. 4. Schematic of the twofold ground state degeneracy of the Ising anyon model (a) and a "wrinkled" Mexican hat potential (b) with several discrete symmetries corresponding to various minima (one highlighted with an orange marker) instead of the full U(1) symmetry.

down toward lower energy local minima, until the global one is found. This leads to the question of how to assign probabilities to the various minima. In a similar way as for a gas of molecules, we want to maximize the number of statistically equivalent microstates, which happens when the entropy takes its maximum value. Therefore, we introduce a notion of entropy in the system. If we denote by  $p_i$ the probability of finding a minimum *i*, the entropy can be expressed as

$$S = -\alpha \sum_{i=0}^{n} p_i \ln(p_i), \tag{7}$$

where  $\alpha$  is a constant. The maximum occurs when  $dS/dp_i = 0$ , and upon imposing stationarity,  $d(\langle E_i \rangle) = d(\sum_{i=0}^{n} p_i E_i) = 0$ , yields the stationary distribution

$$p_i \sim e^{-E_i/T_\alpha},\tag{8}$$

where we have introduced a dimensionless temperature parameter  $T_{\alpha} \propto \alpha$  to retain the connection to thermodynamics and the energy  $E_i$  is associated with the error distance defined in Eq. (1).

#### 3. A Monte Carlo algorithm

Inspired by the Ising spin model, we assign the event of a spin flip, such as  $\uparrow$  flips to  $\downarrow$ , a probability

$$p(\uparrow \text{ to } \downarrow) = e^{-(E_{\uparrow} - E_{\downarrow})/T_{\alpha}},$$
 (9)

where  $E_{\uparrow} > E_{\downarrow}$ . In this particular case, we are dealing with four generators and thus four different possible actions, that is, either stay in the initial state or flip the spin to any of the other three states. To enhance the convergence rate of the algorithm, we let  $T_{\alpha}$  vary as a function of the energy difference  $E_{\uparrow} - E_{\downarrow}$  such that  $T_{\alpha} = \operatorname{ord}(E_{\uparrow} - E_{\downarrow})$ , where  $\operatorname{ord}(x)$  refers to the order of magnitude of x. Note that this parameter can be further calibrated to achieve even better convergence. The Monte Carlo game proceeds via an iterative sequence of attempted and accepted spin flips executed according to the following specific rules.

(i) The process is initiated by performing a simple random walk in the tree according to the probability of Eq. (3), to generate an initial spin configuration (braid word), and then moving to the first site (letter). If we assume that the final low-error configuration is an approximately even mixture of different elementary braids, a randomly generated initial configuration should be a good starting point.

(ii) A new state of the spin is chosen randomly and if the new state of the system after an attempted flip corresponds to a lower energy, that is,  $E_{\text{flip}} < E_{\text{initial}}$ , the flip is accepted and the process moves on to the next adjacent site (letter), towards the leaf node. If the energy of the new attempted state is greater then the flip is accepted only with a probability *p* defined in Eq. (9). If the flip is not accepted then another attempt is made at the same site. This procedure is repeated until a flip is either accepted or all possible flips have been attempted once, after which the algorithm proceeds to the next site.

(iii) Once the end of the chain (a leaf node) is reached, return to the first lattice site (the root node) and continue the iteration until the desired error tolerance is reached.

This basic Monte Carlo method could likely be further optimized by incorporating enhancements such as the worm algorithm [46,47] and other stochastic Hamiltonian approaches [48–50].

#### 4. Performance of the Monte Carlo algorithm

The exhaustive search of braid words is always guaranteed to yield the minimum achievable error between the target unitary and its finite-length braid word approximation. It therefore provides a convenient absolute reference for testing the performance of other algorithms. A comparison of the average time taken by a digital computer to find the best possible braid word approximation using an exhaustive search and a Monte Carlo method is presented in Fig. 5 for a range of braid word lengths within the Fibonacci anyon model. As expected, the search time grows exponentially with the length of the braid word for the exhaustive search method, which simply reflects the structure of the search space. In contrast, the Monte Carlo algorithm clearly outperforms the exhaustive search for braid word lengths exceeding 10.

To understand the convergence properties of the Monte Carlo algorithm, in Fig. 6 we show the achieved absolute error as a function of CPU time for three distinct randomly generated unitary target gates and a braid word length of 50. Occasionally, the algorithm gets stuck in a local minimum corresponding to the plateaus in the figure,



FIG. 5. Search time (CPU) as a function of the braid word length for the exhaustive search method (yellow) and the Monte Carlo algorithm (turquoise). The errors bars represent the standard deviation of the Monte Carlo sample. The braid words are constructed using the braid generators of the Fibonacci anyon model.

but eventually "tunneling" over the barrier is achieved and the convergence proceeds toward another local minimum. An inherent inbuilt feature of the Monte Carlo algorithm is that it efficiently distills out hidden identities and other inefficiencies from the braid words, as can be verified by explicitly monitoring the braid words during the compilation. The Monte Carlo algorithm is particularly useful when compiling braids for computationally nonuniversal models such as the Ising anyon model that require at least one additional elementary gate to be added to the generator set in order to make the model computationally universal. This means that the search space grows as  $5^{l}$  instead of  $4^{l}$ , which makes it even more challenging to perform an exhaustive search. More importantly, the additional gate is not topologically protected and is thus susceptible to ordinary forms of decoherence. It is therefore of great interest to reduce the total number of such nontopological gates required to approximate a predetermined target unitary. As shown in Sec. III C, it is straightforward to implement this within the Monte Carlo algorithm by introducing a phasegate acceptance probability. If we define the probability such that the probability is decreasing with the number of phase gates already accepted, it is possible to reduce the phase-gate count significantly and thus suppress the susceptibility of the computation to conventional forms of decoherence.

#### B. The Solovay-Kitaev algorithm

The SKA can be viewed as an algorithmic implementation of the shrinking lemma that leads to the Solovay-Kitaev theorem. The algorithm plays a significant role in quantum computation as it guarantees that any arbitrary quantum gate can be implemented with arbitrary precision if the gate set at hand is universal.



FIG. 6. The absolute error d as a function of the CPU search time for a Monte Carlo search of a braid word approximation to three randomly chosen unitary matrices. The braid words of length 50 are constructed using the braid generators of the Fibonacci anyon model. Each step change in the graph corresponds to a spin flip in the braid word.

#### 1. The Shrinking lemma and the Solovay-Kitaev theorem

For the sake of completeness, we present the shrinking lemma here followed by the Solovay-Kitaev theorem, which pertains to the mathematical underpinnings of the SKA [42].

**Lemma 1** (The Shrinking Lemma). Let *G* be a set of generators forming a space endowed with a metric d(X, Y), let  $S_{\epsilon} = \{U \in SU(2) \mid d(U,I) < \epsilon\}$ , and let  $\mathcal{G}_{l}$  be the subspace of braid words of length *l*. Furthermore, if we let  $\epsilon_{0}$  be a constant such that we can find a  $g \in \mathcal{G}_{l}$  satisfying  $d(g,s) < \epsilon^{2}$  for any  $s \in S_{\epsilon}$  and  $\epsilon < \epsilon_{0}$ , then we are guaranteed to find a  $g' \in \mathcal{G}_{5l}$  such that  $d(g',s') < C\epsilon^{3}$  for all  $s' \in S_{\sqrt{C\epsilon^{3}}}$  and some constant *C*.

This statement constitutes the basis upon which the Solovay-Kitaev algorithm is founded. In simple terms, the shrinking lemma states that, by recursively expanding the length of the braid word, it is possible to get closer and closer to the target gate.

In order to be able to realize any arbitrary gate, the anyon model must be universal. In terms of the Bloch sphere representation, this implies that it is always possible to find a combination of generators such that their joint action on the state vector maps the initial point on the sphere arbitrarily close to any other point. Algebraically, this entails that SU(2) must be entirely contained in the set, or that each point in SU(2) has a limit point in the set that is arbitrarily close to that point, given that the space is endowed with a metric. It is thus stated that the set is topologically dense in SU(2) or that the set provides a dense cover for SU(2). The Solovay-Kitaev theorem formalizes this statement more concisely. **Theorem 1** (The Solovay-Kitaev Theorem). Let G be a set of generators forming a space endowed with a metric d(X, Y). For any accuracy  $\epsilon > 0$ , there is a constant c and a sequence of generators S of length  $O[\log_c(1/\epsilon)]$ such that the distance to a given target matrix U satisfies  $d(S, U) < \epsilon$  if the set is dense in SU(2).

For a more detailed analysis of the algebraic treatment, see, e.g., Refs. [12,42,51]. The Solovay-Kitaev theorem has important implications to quantum computation as it ensures that universal quantum computation is indeed possible, at least in theory. It was later shown that the bound on the braid word length to error ratio could be improved, leading to a plethora of new adaptations. However, the improvements discussed in the literature are nongeneric, that is, they only hold for specific generator sets [52–57].

# 2. Implementation of the Solovay-Kitaev algorithm

The key step in the Solovay-Kitaev algorithm, and also in the proof of the shrinking lemma, is to perform a group commutator decomposition (GCD) of the quantity  $\Delta =$  $UU_0^{\dagger}$ , into the new elements V and W, such that  $GCD(\Delta) =$  $\widetilde{V}\widetilde{W}\widetilde{V}^{\dagger}\widetilde{W}^{\dagger}$ , with U being the approximation and  $U_0$  the target gate. Then, by finding approximations to the factors in the decomposition, their product yields a better approximation of  $\Delta$  than could be obtained by searching for approximations of  $\Delta$  directly. This fact can be derived from the shrinking lemma. If U is an approximation to  $U_0$ , we have  $\Delta \in \mathcal{S}_{\epsilon}$  for some  $\epsilon$ , to which we can find an approximation  $U' \in \mathcal{G}_l$  with  $d(U', \Delta) < \epsilon^2$ . The lemma thus promises that another braid word  $U'' \in \mathcal{G}_{5l}$  with  $d(U'', \Delta') < C\epsilon^3$  for some  $\Delta' \in S_{\sqrt{C\epsilon^3}}$  can be found. Consequently, by sequential applications, increasingly good approximations can be obtained. When the decomposition is performed, the function calls upon itself recursively with the factors in the decomposition as inputs, and these input matrices are further decomposed to achieve even higher accuracies.

Since  $U = VWV^{\dagger}W^{\dagger}U_0$ , and each one of the factors in the decomposition is of length  $l_0$ , the total length of a braid word that is a level-*n* approximation is given by  $l_n = l_0 5^n$ . The implementation of Algorithm 1 is due to Dawson and Nielsen [42].

#### C. Monte Carlo enhanced Solovay-Kitaev algorithm

The development of the Solovay-Kitaev algorithm was a major step forward in the field of quantum compiling. Nevertheless, it has a few downsides. Probably the most severe is the exponential growth of the braid word length as a function of the level n of the approximation, which due to the group commutator decomposition grows as

$$l_n = l_0 5^n, \tag{10}$$

| $\mathbf{A}$ | lgorithm | 1: | Sol | lovay- | -Kitaev | (U) | , n | ) |
|--------------|----------|----|-----|--------|---------|-----|-----|---|
|--------------|----------|----|-----|--------|---------|-----|-----|---|

| if $n = 0$ then  |
|--|
| braid word = exhaustive search $(U)$ ;   |
| return braid word  |
| else   |
| $\widetilde{U} = $ Solovay-Kitaev $(U, n-1);$  |
| $(V,W) = \operatorname{GCD}(\Delta);$  |
| $\widetilde{V} = $ Solovay–Kitaev $(V, n - 1);$  |
| $\widetilde{W} = $ Solovay-Kitaev $(W, n - 1);$  |
| $U_n = \widetilde{V}\widetilde{W}\widetilde{V}^{\dagger}\widetilde{W}^{\dagger}\widetilde{U}^{\dagger};$ |
| return $U_n$   |
| end  |

where  $l_0$  is the braid word length of the zeroth-order approximation. In order to reach high accuracies, one has to go to great depths (large n) in the algorithm and this results in very long braid words. For instance, to reach an accuracy of  $\epsilon \sim 10^{-4}$  with a base length  $l_0 = 10$ , depth n = 5 may be needed, which means that the length of the resulting braid word is  $l_5 = 10 \times 5^5 = 31250$ , which is unnecessarily long for an error of that magnitude (even though according to the threshold theorem errors below 1% are acceptable in order to perform quantum computation fault tolerantly [58–64]). Another downside is the required computation time. Considering the pseudocode of the previous subsection, we conclude that the algorithm makes three recursive calls per level. This implies that the simulation time increases by a factor of 3 per level according to

$$t_n = t_0 3^n, \tag{11}$$

where  $t_0$  is the time it takes to perform the exhaustive search.

To summarize, while the SKA promises unconstrained accuracy, the accuracy realized for a given braid word length is highly suboptimal. With an ideal algorithm, it should be possible to find braid words of this accuracy that are only a fraction of the length. Moreover, the exponential growth in simulation time makes the process very slow. The simplest way to improve the efficiency of the algorithm is to find a method that enables surpassing the limits of the exhaustive search method. That is, finding better approximations for shorter braid words, in a shorter time. This motivates our introducing the Monte Carlo enhanced Solovay-Kitaev algorithm. By implementing the Monte Carlo method instead of an exhaustive search at the zeroth depth in the Solovay-Kitaev algorithm, it should be possible to enhance the compiler performance significantly. The implementation of this enhancement is very simple. The exhaustive search method at depth n = 0 in Algorithm 1 is simply substituted with the Monte Carlo search, that is, the line braid word = exhaustive search(U) in the algorithm is simply replaced by the line braid word = Monte Carlo search(U).

The graphs presented in Figs. 5 and 6 verify that the Monte Carlo algorithm is indeed significantly faster than the exhaustive search method. While the exhaustive search method is exponential in time, the Monte Carlo one is linear (at least for moderately long braid words), and since it can be easily applied beyond the small search spaces that the brute force method is limited by, it is also possible to find much better zeroth depth, n = 0, approximations.

In addition to the search time, the search space (nary tree) also has to be constructed before performing an exhaustive search. This is an inherently exponential problem in itself as the search space grows as  $m^h$ , where m is the number of child nodes per node and h is the height of the tree. Thus, we may conclude that the advantages of the Monte Carlo-based MCESKA over the exhaustive search-based SKA are twofold: (i) it enables better zerothlevel approximations, and (ii) not only is it searching more efficiently, but also no preparatory work is required prior to the initiation of the search process. Note, however, that the recursive part of the MCESKA is still exponential and that it is the search time  $t_0$  that is significantly improved upon by the Monte Carlo implementation, as it grows exponentially with the braid word length for exhaustive search. Additionally, it is possible to suppress the phasegate count in the nonuniversal models by introducing a phase-gate acceptance probability to the Monte Carlo part of the MCESKA, which makes it particularly powerful for compiling hybrid anyon models. More general constraints on the desired braid words are also straightforward to implement within the MCESKA.

#### **D.** Comparison of compiler algorithms

In Fig. 7 we summarize our quantum compiler benchmark results obtained for the conventional Solovay-Kitaev algorithm and our Monte Carlo enhanced Solovay-Kitaev algorithm using the braid generators of the Fibonacci anyon model. We have used  $l_0 = 10$  and  $l_0 = 15$  as base lengths for the SKA and  $l_0 = 30$  and  $l_0 = 50$  for the MCESKA. The dashed orange line is an extrapolation based on the brute force method data points (red, green, and cyan). This is a useful benchmark for how well our algorithm performs compared to a hypothetical ideal algorithm that would find the best approximation for any braid word length. In particular, the pure Monte Carlo method for  $l_0 = 50$  achieves practically equivalent precision as an estimated brute force method would. The shaded regions correspond to the braid word length intervals for which the specified algorithm is recommended to be used for optimal results.

These recommendations are based on the following observations. The brute force search allows finding the optimal braid word for any given length, but since it is not feasible in practice to search whole trees for braid words longer than around 20, we recommend brute force



FIG. 7. Comparison of the performance of the conventional Solovay-Kitaev quantum compiler algorithm (SKA) with our Monte Carlo enhanced version (MCESKA). The dashed orange line has a slope of -0.0017275 and is an extrapolation based on the three data points  $l_0 = 10, 15, 20$  obtained with the brute force (BF) method and should be viewed as an estimation of the lowest theoretically attainable error for a given braid word length. The results are obtained using the Fibonacci anyon model.

search for braid words shorter than this. The Monte Carlo method can still be used to search efficiently for lengths much greater than 20 but has an upper limit for lengths of magnitude  $10^2$ . If  $l_0 = 50$  is used as the base length (in our experience this seems to be a good length to optimize the benefits of the Monte Carlo method), one reaches  $l_1 = l_0 5^1 = 50 \times 5 = 250$  after one iteration, which we can take as an upper bound of the Monte Carlo part as any length greater than that is obtained by iterating with the Solovay-Kitaev part of the algorithm.

The results in Fig. 7 confirm our conjecture. Invoking the Monte Carlo method at the zeroth depth brings substantial benefits. Note that these results are obtained for particular parameter values in the algorithm, which could be further optimized. For instance, if one succeeds in improving the calibration of the temperature parameter in Eq. (9), a higher convergence rate could be achieved. Also, if we allow for a longer simulation time, the algorithm will be able to settle into a lower local minimum. With this particular set of parameter values we see that the blue curve  $(l_0 = 50)$  reaches an error 2 orders of magnitude lower than the green curve ( $l_0 = 15$ ), after only three MCESKA recursions. Nevertheless, the braid word length corresponding to this error is still roughly one order of magnitude greater than the estimated ideal length obtained from the brute force extrapolation (the dashed orange line). Also, note that these improvements are obtained despite the longer zeroth-order braid word length. For  $l_0 = 50$ , we reach an average just below  $10^{-3}$ , while for the  $l_0 = 15$ , we only reach an average of about 0.03. This gives the  $l_0 = 50$  a head start and skip over the slow convergence rate in the high error region, resulting in a much greater efficiency as high values of *n* are not required.

# **III. NUMERICAL EXPERIMENTS**

#### A. Fibonacci versus Ising anyon models

Here we present MCESKA compilation results for the Fibonacci and Ising anyon models. As mentioned previously, the Fibonacci model is capable of universal quantum computation by only braiding the anyons, whereas the Ising anyon model must be supplemented with an additional unitary operator such as a suitably chosen phase gate. It is thus natural to ask how to choose such an auxiliary gate.

Recall that universality implies that we must be able to arrive arbitrarily close to any point on the Bloch sphere just by combining the generators. In  $\mathbb{R}^2$ , by picking any two vectors  $\bar{v}, \bar{w}$  such that  $\bar{v} \times \bar{w} \neq 0$ , and parameters  $a, b \in$  $\mathbb{R}$ , we may construct a linear combination  $(a\bar{v}, b\bar{w})$  that reaches any point in the plane. Similarly, on the sphere, by choosing a phase gate  $R_{\theta}$  such that it is possible to construct at least two continuous and nonparallel rotations, we should be able to cover the whole sphere. One way to achieve this is to select a phase that generates a dense set in  $S^1$ , since then we can combine this phase with the other generators to form multiple "nonparallel" dense circles that serve as a basis on the sphere. Mathematically, we thus need to select a phase of infinite order, i.e.,  $\phi^n \neq I$  for all  $n \in \mathbb{Z} \setminus \{0\}$ , and find at least two sequences  $s_1, s_2$  containing the corresponding phase gate  $R_{\theta}$  [defined in Eq. (12)] such that  $[s_1, s_2] \neq 0$ . By considering the unit circle in the complex plane, the two phases  $e^{inx2\pi}$ and  $e^{imy2\pi}$ , where  $m, n \in \mathbb{Z}$ , can never be equal if we let  $x, y \in \mathbb{R} \setminus \mathbb{Q}$  (the irrationals), since no such number can be expressed as a fraction, which further implies that  $e^{inx2\pi} \neq$  $e^{imy2\pi}$  for all  $n \neq m$ . Hence, we arrive at the following propositions.

**Proposition 1.** Let  $\phi = e^{ix\pi}$  be a phase on the complex unit circle with corresponding phase gate  $R_{x\pi}$ . Then the set generated by  $\phi^n$ , where  $n \in \mathbb{Z}$ , will form a topologically dense cover in  $S^1$  (in the complex plane) if  $x \in \mathbb{R} \setminus \mathbb{Q}$ .

**Proposition 2.** Let  $\Sigma$  be a set of generators that does not form a topologically dense cover in SU(2). Then, by adding an irrational phase gate  $R_{\theta}$ , it will become dense if at least two sequences  $s_1$  and  $s_2$ , containing  $\phi$ , can be found such that  $[s_1, s_2] \neq 0$ .

Having established that any irrational phase can be used to supplement a nonuniversal anyon model, we only need to find two sequences containing this phase that do not commute, in order to form a basis on the Bloch sphere. This is easily achieved since braid generators do not commute in general. For instance,  $\sigma_1\phi$  will generate a dense circle around one axis and  $\sigma_2\phi$  around another one since  $[\sigma_1\phi, \sigma_2\phi] \neq 0$ . Thus, we may conclude that universality can be achieved in the Ising anyon model by adding an irrational phase gate to the set of generators. An in-depth analysis of the conditions for universality can be found in Ref. [65] and physical implementations of phase gates are discussed in Ref. [66].

In our numerical experiments, we generate a large number of random unitary matrices as target gates that are then compiled using the different anyon models and for a range of braid word lengths. The braid generators for a generic level k anyon model considered are constructed using Eqs. (B13)–(B17).

In Fig. 8 we show a comparison between the universal Fibonacci anyon model and the hybrid Ising anyon model for which a phase gate

$$R_{\theta} = \begin{pmatrix} 1 & 0\\ 0 & e^{i\theta} \end{pmatrix} \tag{12}$$

with a phase angle  $\theta = \sqrt{2\pi}$  is used to achieve universality. Although it is also possible to achieve universality in the Ising anyon model with a phase gate with rational phase angle, such as  $\theta = \pi/4$ , we have chosen to deploy an irrational phase angle to facilitate fair comparison between the two nonuniversal, k = 2 and k = 4, anyon models, which would otherwise not be possible. The data points in Fig. 8 are an average over the sample with one thousand data points and the error bars represent the corresponding standard deviation. This numerical experiment confirms our conjecture that the Ising anyon model becomes computationally universal when enhanced with an irrational phase. The average performance of this hybrid Ising anyon model generally seems slightly better than the Fibonacci model but, since the error bars are overlapping, from a statistical point of view, their performance should be considered to be equal. However, since the additional phase gate cannot be implemented in a topologically protected manner, the hybrid Ising anyon model is not immune to decoherence, which means that, from a practical point of view, the Fibonacci model will always outperform the hybrid Ising anyon model in the presence of environmental noise, as discussed in detail in Sec. III D. Furthermore, if the Ising anyon model is complemented with an auxiliary gate with rational-valued phase angle, the observed difference between the hybrid Ising anyon model and the Fibonacci anyon models is effectively removed.

# B. The k = 4, 5, 6, 8 anyon models

To provide a broader perspective, we extend our analysis of the k = 2 Ising and k = 3 Fibonacci anyon models to the



FIG. 8. Compilation errors as a function of the braid word length evaluated for the Fibonacci and hybrid Ising anyon models. In total about 20% of  $R_{\sqrt{2}\pi}$  phase gates are deployed in the Ising braid words. Each data point comprises  $10^3$  realizations with a corresponding statistical error estimate shown.

k = 4, 5, 6, 8 anyon models. In light of Theorems 2 and 3 in Sec. III B, we conclude that, similar to the k = 2 case, the k = 4 model is nonuniversal and needs to be supplemented with a generator having an irrational phase. We use the fusion product  $(k - 1)/2 \otimes (k - 1)/2 = 0 \oplus 1$  as the qubit for these numerical experiments.

The results of these calculations are summarized in Fig. 9(a), which shows that the data (averaged over  $10^3$  realizations) corresponding to k = 2, 3, 4, 5, 8 are all within one standard deviation from one another. The only one that lies consistently above the others is the k = 6 model. This indicates that the group generated by the k = 6 braid generators may cover the SU(2) at a slower rate than the other models, yielding a slower convergence rate. In order to understand this observation, we construct a heuristic argument based on the structure of the corresponding braid group. We project the rotations onto the complex plane to analyze the cyclicity of the group generators. Letting  $\Sigma_{\sigma_i,k}$  denote the subgroup generated by  $\sigma_i$  for a given k, we may define an isomorphism

$$f: \Sigma_{\sigma_i,k} \to \Sigma'_{\sigma_i,k} \tag{13}$$

such that  $f(\sigma_i^q \sigma_j^p) = f(\sigma_i^q) f(\sigma_j^p)$  for any  $q, p \in \mathbb{Z}$ , where the image forms a group that is identical in terms of rotations but the axis is aligned with the axis of the group we are comparing with. In fact,  $\Sigma_{\sigma_i,k}$  and  $\Sigma'_{\sigma_i,k}$  belong to the same equivalence class. Since the generators  $\sigma_1$  and  $\sigma_2$  in a given SU(2)<sub>k</sub> model are always 2(k + 2) cycles, we can deduce the size of the intersection between two subgroups  $\Sigma'_{\sigma_i,k}$  and  $\Sigma_{\sigma_i,k'}$  (where  $\Sigma'_{\sigma_i,k}$  is the image of f such that the axes are aligned), generated by  $\sigma_i$ . Let us start with the case in which  $k, k' \in 2\mathbb{Z}$  (even) and let k' > k. Then the following statement holds when projected onto the complex plane:

$$\Sigma'_{\sigma_{i},k} \cap \Sigma_{\sigma_{i},k'} = \begin{cases} \Sigma'_{\sigma_{i},k} & \text{if } k+2|k'+2, \\ \{0, e^{i\pi/2}, e^{i\pi}, e^{i3\pi/2}\} & \text{otherwise.} \end{cases}$$
(14)

From this we deduce that  $\Sigma'_k$  is completely contained in  $\Sigma_{k'}$  if k' + 2 is divisible by k + 2, whereas if this condition is not satisfied, the intersection will form a smaller group corresponding to  $\pi/2$  rotations. Letting  $k \in 2\mathbb{Z} - 1$  (odd) and  $k' \in 2\mathbb{Z}$  (even), the intersection is given by

$$\Sigma'_{\sigma_i,k} \cap \Sigma_{\sigma_i,k'} = \begin{cases} \Sigma'_{\sigma_i,k} & \text{if } k+2|k'+2, \\ \{0, e^{i\pi}\} & \text{otherwise.} \end{cases}$$
(15)

That is, the odd k subgroup is completely contained in the even one if k' + 2 is divisible by k + 2, and if not, the intersection is constituted by the group corresponding to  $\pi$  rotations. However, the reverse is never true, where the even k group would be completely contained in the odd k group since all even k groups contain a  $\pi/2$  and a  $3\pi/2$  rotation, while odd k groups never do.

We now apply this analysis to our particular case by comparing the k = 6 group with the others. As depicted in Fig. 9(b), this group is a 16 cycle at the generator level and, for all k = 3, 4, 5, we have  $k' + 2 \nmid k + 2$ , i.e., a 16 cycle is not divisible by the 10, 12, 14 cycles (k = 3, 4, 5). However, the generators in the k = 2 are 8 cycles and  $8 \mid 16$ , so all rotations in the k = 2 group are being faithfully represented by elements in the k = 6 braid group. Or, equivalently, the structure of the k = 2 braid group is entirely encoded in the k = 6 group, which is not true for k = 3, 4, 5. Hence, there is no *a priori* reason to expect the k = 6 model to perform better than the k = 3, 5 models, since the k = 2 model is nonuniversal. We can only state for certain that the k = 6 model is better than the k = 2model, but since the k = 2 model is not universal, the gap in performance between this model and the k = 3, 5 models is enormous, which is why it is not obvious that the k = 6 model should exceed the k = 3, 5 cases in performance. In fact, the k = 6 model is the first even k model that is universal. Moreover, if we apply the same analysis to k = 8, we find that k + 2 |k' + 2 only if we let k' = 3. This means that the Fibonacci braid group is isomorphic [according to f defined in Eq. (13)] to a subgroup of the braid group labeled by k = 8. So in this case it should hold that the k = 8 model is at least as good as the Fibonacci model with regards to braiding, which also conforms with the results shown in Fig. 9.



FIG. 9. Comparison of the k = 2, 3, 4, 5, 6, 8 anyon models. For all models, the compilation error as a function of the braid word length (a) is consistent with an overall power-law convergence to the target gate. The cyclicity of each model, illustrated in the Argand plane (b), reveals that the k = 2 model is contained within the k = 6 model and that the k = 3 model is contained within the k = 8 model. The k = 2 and k = 4 cases are supplemented with  $R_{\sqrt{2\pi}}$  phase gates.

#### C. Decoherence in nonuniversal anyon models

Adding a phase gate to the otherwise topologically protected braid generators comes with a price. Unlike the topological gates that are immune to conventional sources of noise, the added phase-gate generator cannot be implemented in hardware without accompanying decoherence. The more phase gates are used, the more adverse the effect of the noise brought along. It is therefore preferable to keep the phase-gate count as low as possible, as the cumulative effect of the noise during braiding may have terminal consequences for the computation.

For the Ising anyon model, we might expect the unconstrained fraction of phase gates contained in a braid word to be about 20% on average for long sequences, since there are in total five generators, four topological and one conventional, in the set. To see if it is possible to suppress the dependence on this "necessary but undesirable" generator, we introduce an acceptance probability in the Monte Carlo algorithm  $p \sim e^{-Cn/l}$ , where  $C \in \mathbb{R}$ , *n* is the number of phase gates in the sequence, and l is the length of the braid word. Thus, as n increases, the acceptance probability decreases. Adding a phase gate to the braid word can thus be regarded as resulting in an energy penalty, akin to that introduced in the spin chain picture discussed in Sec. II A 1, but here the energy is proportional to the number of phase gates already present in the chain. In Fig. 10 we show the fraction of phase gates used in a compiled braid word as a function of the control parameter C for a fixed braid word precision.

From this we infer that the optimized phase-gate dependence saturates at values much lower than the expected 20%. Specifically, the k = 2 results converge toward 10% and the k = 4 results toward 5%. To explain this observation, we consider the group structure generated by the braid generators. All one-qubit models have two generators (and their inverses) that are cyclical. Specifically, for any generator  $\sigma_i$ , there exists a nonzero integer q such that  $\sigma_i^q = I$ , where I is the identity. As the generators are



FIG. 10. Ratio  $N_{\phi}/l$  of the number of noisy phase gates  $N_{\phi}$  and the braid word length  $l = N_{\phi} + N_{\sigma}$ , where  $N_{\sigma}$  is the number of topologically protected gates, as a function of the acceptance parameter *C* for compilation of a fixed length l = 50, fixed precision  $d = 5 \times 10^{-3}$  braid word. Horizontal lines estimate the saturated fractions.

8 cycles and 12 cycles in the k = 2 and k = 4 models, respectively, the order of the subgroups generated by these elements independently are of the same order as the elements that generate them, i.e., 8 and 12. For simplicity, consider the subgroup  $\Sigma_{\sigma_1}$  generated by  $\sigma_1$  [67]. We claim that the k = 4 braid group is of greater order due to its cyclicity. To make this more explicit, we consider the coset structure in the two groups. Since every distinct element in the main group must belong to a coset of the  $\sigma_1$  subgroup, the order of the subgroup divides the order of the main group, since each coset has to contain the same number of elements as the subgroup [68]. Thus, if  $\Sigma_{\sigma_1}$  denotes the subgroup of the full group  $\Sigma$  that is generated by  $\sigma_1$ , and *n* denotes the index of this subgroup, i.e.,  $[\Sigma_{\sigma_1} : \Sigma] = n$ , we may express the order of  $\Sigma$  as

$$|\Sigma| = |\Sigma_{\sigma_1}| [\Sigma_{\sigma_1} : \Sigma] = |\Sigma_{\sigma_1}| n.$$
(16)

Because of the cyclicity of the groups, not only is the order of the cyclic subgroups  $\Sigma_{\sigma_1}$  and  $\Sigma_{\sigma_2}$  greater for k = 4, but so is the index  $n_{k=4}$ . Hence, the order of the k = 4 braid group is greater than that of the k = 2 braid group.

Considering a sphere of radius *R*, see Fig. 11, each element in the group will occupy a solid angle  $\Omega = 4\pi/|\Sigma|$ , assuming that the points are somewhat evenly distributed over the surface, which should be a fair assumption for dense gate sets. This solid angle corresponds to a spherical cap with circular boundary and an arc length that defines the "curved" radius *r*. The solid angle on a sphere is  $\Omega = A/R^2$ , where *A* is the area of the corresponding spherical cap. In spherical coordinates we thus find that

$$\Omega = \frac{1}{R^2} \int_0^{2\pi} \int_0^{\theta} R^2 \sin(\theta) d\varphi d\theta = 2\pi [1 - \cos(\theta)].$$
(17)

Setting this equal to  $4\pi/|\Sigma|$  yields  $\theta = \arccos(1 - 2/|\Sigma|)$ , which results in an expression for the orthodromic distance *r* of

$$r(|\Sigma|) = \int_0^\theta Rd\theta = R \arccos\left(1 - \frac{2}{|\Sigma|}\right).$$
(18)

This distance is the maximum distance for any point on the sphere to a group element, as each element is occupying the same area and solid angle. Note that this function goes to 0 as the group order  $|\Sigma|$  goes to  $\infty$ , which corresponds to the fully universal anyon models for which the target gate can be approximated to arbitrary accuracy.

We also conclude that the average distance from any group element to any point on the sphere is shorter in the k = 4 model than in the k = 2 model since  $|\Sigma_{k=4}| > |\Sigma_{k=2}|$ . This further implies a weaker phase-gate dependence for k = 4, in agreement with the results presented in Fig. 10.



FIG. 11. Schematic of a Bloch sphere illustrating the notation used in the text.

According to conventional wisdom, in decoherence prone quantum computation about a thousand physical gubits may be required per one logical gubit to facilitate error correction [69,70]. In contrast, our results suggest that the hybrid Ising anyon model and the k = 4 model might only require an order of magnitude fewer physical qubits for each logical one in order to suppress the logical error to arbitrarily low levels, since in these systems the phase-gate count can be suppressed to 10% and 5%, respectively. Of course, this estimate needs to be taken with a grain of salt until tested on real hardware. Nevertheless, protocols such as that discussed in Ref. [71] have been developed that utilize fusion to purify phase rotated states from which the phase gates can be extracted. These processes are prone to errors and, since the number of distilled states needed in order to implement a certain number of phase gates should be proportional to the number of phase gates, we conclude that correspondingly fewer distilled states are required in the  $SU(2)_2$  and  $SU(2)_4$  models, compared to a fully conventional quantum computer. In Fig. 12 we demonstrate the effect of decoherence on the compiler error when noise is added to 5%, 10%, or 100% of the gates for the cases of k = 4, 2, and 2, respectively. These curves represent the error purely due to noise when the logical error is subtracted for the braid word lengths 50, 250, 1250, and 6250. As is evident in Fig. 12, the longer the braid word, the more severe the effect of the noise since a higher number of phase gates is used. The 100% case corresponds to a 100% conventional quantum computation with the Ising anyon model, for which none of the generators would possess intrinsic topological protection, or they would all be prone to strong topological decoherence at the hardware level, e.g., due to quasiparticle poisoning [72]. This case is included as a benchmark and reference to conventional quantum computing platforms.

The decoherence noise is modeled as small random unitary rotations. In the su(2) basis we can express the corresponding operator as

$$U_{\text{noise}} = e^{i\vec{\theta}\cdot\vec{\sigma}},$$



FIG. 12. The braid word error purely due to the  $e^{i\sqrt{2}\pi}$  phase gates deployed in the hybrid k = 4 (purple circles) and k = 2 (cyan stars, yellow squares) Ising anyon models as functions of the strength  $\nu$ of the phase-gate noise. The braid word length *l* considered is noted in each frame.

where  $\vec{\sigma}$  is a vector of Pauli matrices and  $\vec{\theta} = (\theta_1, \theta_2, \theta_3)$ . We sample the parameters  $\theta_i$  from a narrow normal distribution with zero mean, i.e.,  $\theta_i \in N(0, \nu)$ , where  $\nu$  is the standard deviation. By increasing  $\nu$ , greater phase-gate noise fluctuations are allowed, which means that the standard deviation may be interpreted as the "strength" of the noise. An in-depth analysis of the impact of various specific kinds of noise sources is provided in Ref. [73].



In Fig. 13 we show the results when the noise is applied to the braid words. We set  $v = \{0, 10^{-5}, 10^{-4}, 10^{-3}\}$  in Figs. 13(a)–13(d), respectively. In the v = 0 case the noise is absent and the MCESKA should be applied to achieve the best absolute accuracy. As v is gradually increased, error minima first appear and continuously shift toward shorter braid word lengths, Figs. 13(b) and 13(c), until



FIG. 13. Absolute error, including the inherent braid word approximation and the contributions from the noise in Fig. 12, as a function of the braid word length. Panels (a)–(d) correspond to the noise levels v = $0, 10^{-5}, 10^{-4}, 10^{-3}$ , respectively. The inset in (a) shows the optimal braid word length corresponding to the minima in (a)–(d), as a function of the noise strength  $\nu$ . Note that, when the minimum appears to occur at the end of the interval, the true minimum may be located outside the interval. This is accounted for in the inset in (a), which presents the locations of the true minima. The same unitaries  $U_0$  have been used for all of the curves.

 $\nu = 10^{-3}$  is reached in Fig. 13(d), for which the error minima are obtained at the zeroth depth in the algorithm for l = 50. Hence, for the noisy gate region, the best results would be achieved with the direct Monte Carlo method.

Summarizing, in the zero noise case the full power of the Monte Carlo enhanced Solovay-Kitaev algorithm should be employed, whereas in the intermediate noise region a small number of recursions could be beneficial. For  $\nu \ge 10^{-3}$ , the plain Monte Carlo method should be invoked for the best results. Note that  $\nu = 10^{-3}$  is still quite small so it is reasonable to assume that the noise will be in this range or greater in realistic near-future applications.

The inset in Fig. 13(a) shows the optimal braid word length, the locations of the minima in (a)–(d), as a function of the phase-gate noise v. As the noise gets stronger, the optimal braid word length gets monotonically shorter. This highlights the important observation that, although in a decoherence free universal TQC such as the Fibonacci anyon model, arbitrary accuracies can in principle be achieved just by increasing the length of the braid words; in realistic applications the best attainable accuracy is always noise limited and no further benefit can be gained from deploying excessively long braid words.

## **IV. CONCLUSIONS**

We develop a generic Monte Carlo enhanced Solovay-Kitaev quantum compiler algorithm to search for braid word approximations to quantum logic gates. Motivated by the potential of Majorana fermion quasiparticle zero modes as a physical realization of the Ising anyon model, we deploy the MCESKA to assess and compare the performance and potential of the Fibonacci and the Ising anyon models for topological quantum computation. Furthermore, we expand our analysis to include the k = 4, 5, 6, and 8 SU(2)<sub>k</sub> anyon models. We find that the plain Monte Carlo quantum compiler outperformed the brute force search method in terms of efficiency and required resources while achieving comparable accuracy, and when combined with the SKA, leveraged the performance by 2 orders of magnitude, compared to Dawson's and Nielsen's implementation of the SKA in Ref. [42]. Although other implementations that are even more efficient than the basic SKA exist, they are typically nongeneric, model-specific algorithms [52–57]. One of the major benefits of the MCESKA is that it retains full model independent generality while providing efficient means to perform quantum gate compilation. Similar benefits have recently been achieved using a machine learning approach [43]. Moreover, the MCESKA is a versatile algorithm that can easily accommodate arbitrary constraints on the braid words. For instance, an inclusion of a phase-gate acceptance criterion allowed us to suppress the noisy phase-gate count significantly. It is also directly applicable to multiqubit systems with an arbitrary number of braid generators, and can be applied to compile gates for both braid-based and measurement-only topological quantum computers, as well as for compiling quantum circuits for conventional gate-based quantum computers.

Presently, physical systems hosting Majorana fermion zero modes appear to be among the most promising platforms for TQC. Since the resulting Ising anyon model cannot achieve universal quantum computation by braiding alone, it means that such systems will have to also deal with conventional forms of decoherence. Our results suggest that the hybrid anyon models' susceptibility to conventional types of decoherence due to environmental noise can be reduced by efficient gate compilation that minimizes the use of the auxiliary, noisy phase gates. The seemingly ineffective raw Ising anyon model can be made computationally universal by adding an irrational phase gate to its generator set. This extra gate drastically enhances the quality of the generator set and the results presented in Fig. 8 surprisingly indicate that it could actually perform slightly better than the inherently universal Fibonacci model that enjoys full benefits of topological protection.

When phase-gate noise is introduced to the anyon models, however, we find that, even in the case of rather weak noise, the use of long braid words results in larger compilation errors than the shorter ones because of the necessary use of a larger number of noisy phase gates. The downside of this is that the theoretical accuracy of the hybrid topological quantum computation is limited by the conventional kinds of noise, while the upside is that relatively short braid words of only tens or hundreds of braidings can be used, which is good news from the future hardware implementation point of view.

Most importantly, where as a fully conventional quantum computer of the present day may be estimated to require of the order of a thousand physical qubits per logical qubit [74] due to having to dispense vast resources on error correction protocols, a hybrid topological quantum computer based on Ising anyons might only need an order of magnitude fewer in order to achieve comparable computational accuracy. This demonstrates that even the hybrid topological quantum computer models retain a clear topological advantage over the conventional kinds of quantum computers.

In conclusion, that a hybrid Ising anyon model may, under similar circumstances, perform significantly better than a conventional decoherence prone quantum computer seems promising for the quest of realizing Majorana fermion-based topological quantum computers.

# ACKNOWLEDGMENTS

We are grateful to Chris Vale for useful discussions. This work was performed on the OzSTAR national facility at Swinburne University of Technology. The OzSTAR program receives funding in part from the Astronomy National Collaborative Research Infrastructure Strategy (NCRIS) allocation provided by the Australian Government. This research was funded by the Australian Government through the Australian Research Council (ARC) Future Fellowship project FT180100020.

# APPENDIX A: ELEMENTS OF TOPOLOGICAL QUANTUM COMPUTATION

The theoretical landscape of anyon theory is incredibly rich and substantial with modular tensor category theory [75–77] and topological quantum field theory (TQFT) [78–80] being the main pillars. Here, though, we are primarily concerned with applications in the context of quantum computation. The transformations induced when exchanging two anyons are not restricted to a factor  $\pm 1$ as for bosons and fermions, but instead an arbitrary phase may be acquired. This special attribute, along with the intrinsic topological protection possessed by topological states, constitute the motivational foundation for the pursuit of TQC.

When two anyons are exchanged, the world lines will trace out a braid in (2 + 1)-dimensional space-time with two spatial dimensions and one time dimension. The set of braids together with the composition operation constitute a group known as the braid group [81]. In particular, we are interested in the three-stranded braid group  $\mathbb{B}_3$  as this group can be used for encoding and processing one-qubit quantum gates. Letting  $\sigma_1$  denote the braid formed when the first anyon is wrapped around the second, and  $\sigma_2$  denote the braid corresponding to the second wrapped around the third, the generator set  $\Sigma_{\mathbb{B}_3}$  of  $\mathbb{B}_3$  is  $\Sigma_{\mathbb{B}_3} = \{\sigma_1, \sigma_2, \sigma_2^{-1}, \sigma_1^{-1}\}.$  These generators are presented pictorially in Figs. 14 and 15 with time flowing in the upward direction indicated by the arrows. These braid diagrams correspond to planar projections of the (2 + 1)dimensional anyon world lines. When two lines intersect, the continuous line is understood to lay on top of the discontinuous line.

It is evident from these figures that, when a braid is composed with its inverse by stacking the diagram on the left



FIG. 14. A pictorial representation of the generators of the braid group  $\mathbb{B}_3$ . The  $\sigma_1$  operation swaps the positions of the first two anyons,  $\sigma_2$  swaps the positions of the last two anyons, and the identity operation *I* does nothing to the system.



FIG. 15. The inverse operation  $\sigma_i^{-1}$  of the braid  $\sigma_i$ .

in Fig. 15 on top of the one on the right, or vice versa, the braid will "untie" and become identical to the identity operation. If we consider the generic braid group  $\mathbb{B}_N$  on N strands with generators  $\{\sigma_i\}_{i=1}^{N-1}$ , we can also conclude that any nonadjacent braids have to commute. In addition to this, consistency when permuting the temporal order in which the crossings of the three strands appear must be imposed. These three conditions form what is knows as the Yang-Baxter equations [82]:

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{if } |i - j| \ge 2,$$
 (A1a)

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$
 if  $1 \le i \le N - 2$ , (A1b)

$$\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = I.$$
 (A1c)

In Fig. 16 we show a graphical representation of the second equation in the Yang-Baxter equations, which illustrates that the strands can be deformed such that the temporal order is changed. It should be clear that the configuration on the left-hand side can be deformed into that on the right-hand side, and vice versa, without changing the topology. The set of equations in (A1) admits many matrix solutions. The simplest one corresponds to the one-dimensional representation and yields a trivial phase factor  $e^{i\phi}$ . However, there are also solutions constituting multidimensional representations, which give rise to a richer structure [10,15].

Thus far we have only discussed anyons and the emergence of quasiparticles with fractional statistics in two dimensions generically. Anyons can further be categorized into abelian and nonabelian subspecies. These two



FIG. 16. A graphical representation of the Yang-Baxter Eq. (A1b).

subspecies are distinguished by the commutativity of the corresponding braid group they transform under; abelian anyons transform under an abelian braid group representation that is one dimensional, and nonabelian anyons under a higher-dimensional nonabelian braid group representation. The dimensionality of the corresponding representation space has important consequences for what happens when multiple anyons are involved. If we consider two anyons and perform a dilation transformation, these quasiparticles may be regarded as one composite object. This process is known as fusion. Because of the simple structure of abelian anyons, the fusion outcome is always definite, whereas for the nonabelian anyons, it is indefinite. Considering the fusion product of two nonabelian anyons with charges  $\alpha$  and  $\beta$ , they may, for instance, fuse into the vacuum denoted by 1 or a quasiparticle with charge  $\psi$ . Mathematically, this is expressed as

$$\alpha \otimes \beta = \mathbf{1} \oplus \psi. \tag{A2}$$

The decomposition rule in Eq. (A2) arises entirely due to the reducibility of the joint representation spaces in the nonabelian case, whereas the simple one-dimensional structure of abelian anyons have no nontrivial invariant subspaces, thus resulting in a definite fusion outcome.

In TQC, the core idea is to utilize the fusion product as a qubit in which information can be encoded. Moreover, since the state of the anyons can be transformed by braiding them, the corresponding braid group may be used for producing a circuit of quantum gates. A computational process is thus initiated by creating pairs of nonabelian anyons from the vacuum, followed by a particular series of braids that have been determined in advance based on the chosen quantum circuit. At the end of the braiding, the anyons are brought (sequentially fused) together, which is the read out. Taking the fusion product in Eq. (A2) as an example, we can either measure a vacuum, or a composite object  $\psi$ , each with a certain probability that normalizes to 1.

#### APPENDIX B: SU(2)<sub>k</sub> ANYON MODELS

In the pursuit of quantum computation a wide range of mathematical models have been suggested. Some of the most notable anyon models are the so-called  $SU(2)_k$  models. These models correspond to various truncations of the spin chain expansion.

Nonabelian SU(2)<sub>k</sub> theories are gauge invariant only up to a phase  $2\pi nk$ , where *n* is the winding number. When computing the amplitude for a given process, this quantity is gauge invariant only if *k* is an integer. Hence,  $k \in \mathbb{Z}$  labels the theory, and is referred to as the level of the theory. For more detailed descriptions of TQFTs and SU(2)<sub>k</sub> Chern-Simons theories in particular, see, e.g., Refs. [78,83,84].

### 1. Deformed SU(2) spin algebras

In quantum mechanics the joint tensored space of interacting spins can be decomposed into a direct sum of orthogonal irreducible subspaces. In particular, for spins  $S_1$  and  $S_2$ , this is expressed as

$$\mathbf{S}_1 \otimes \mathbf{S}_2 = |\mathbf{S}_1 - \mathbf{S}_2| \oplus \cdots \oplus (\mathbf{S}_1 + \mathbf{S}_2).$$
(B1)

If we consider all representations of SU(2), the spins may take any integer or half-integer value, i.e.,  $S_i = \frac{1}{2}, 1, \frac{3}{2}, 2, ...$  This sequence continues to infinity, but what if we terminate it after a specific value? This is essentially what is meant by deforming the algebra as only a subset of all representations are allowed. Thus, if we consider generalized angular momenta  $j_i$  and choose some truncation level k, the corresponding algebra decomposes as [85]

$$j_1 \otimes j_2 = |j_1 - j_2| \oplus (|j_1 - j_2| + 1) \oplus \cdots \oplus \min(j_1 + j_2, k - j_1 - j_2)$$
(B2)

with  $l = \frac{1}{2}, 1, \frac{3}{2}, 2, ..., k/2$  the allowed values for the generalized spin and  $k \to \infty$  corresponding to the full SU(2) algebra.

For the sake of concreteness, let us consider two spin- $\frac{1}{2}$  particles for which

$$\frac{1}{2} \otimes \frac{1}{2} = 0 \oplus 1. \tag{B3}$$

In words, two spin- $\frac{1}{2}$  spaces decompose as a spin-0 (singlet) space and a spin-1 (triplet) representation space. This is the only nontrivial fusion rule for k = 2. Similarly, for two spin-1 particles at level k = 3, we have

$$1 \otimes 1 = 0 \oplus 1, \tag{B4}$$

since the spin-2 representation is now excluded. Note that the notion of spin and angular momentum is used here in a general sense. That is, it could be any type of "charge" obeying the same algebra. In this particular context, these labels represent topological charges of anyons and the tensor product represents the fusion of two anyons, i.e., their combined global charge. However, when k is odd, there exists a fusion automophism, which defines a duality between the integer and half-integer charges. In general, we have the map [86]

$$\frac{k}{2} \otimes j = j', \tag{B5}$$

where *j* has half-integer spin (or integer) and *j'* has integer spin (or half-integer if *j* has integer spin). Complete sets of fusion rules are shown in Tables I–V, respectively, for k = 8, 6, 4, 3 and 2 SU(2)<sub>k</sub> anyon models.

In TQC we let the fusion product constitute a qubit. First, anyon pairs are created from the vacuum, then the



FIG. 17. Two Bratteli diagrams for (a) k = 2 and (b) k = 3. The vertex numbers correspond to the degeneracy of the fusion outcome and thus the dimension of the Hilbert space. These numbers are determined by the number of paths from the origin leading to a particular vertex. The integer N is the number of spin- $\frac{1}{2}$  anyons participating in the fusion process and S is the total spin (charge) [45].

computation is carried out by braiding them, and finally they are brought together (fused), which corresponds to the read out. For instance, in Eq. (B4) one would measure a spin equal to 0 with a probability  $p_0$ , or 1 with probability  $p_1$ , where  $p_0 + p_1 = 1$ . The degeneracy of the fusion outcome for an arbitrary N-anyon system can be neatly summarized using a Bratteli diagram; see Fig. 17 [45]. Bratteli diagrams are very useful as they provide a simple way of determining the dimension of the fusion space. The dimension depends on the topological charge of the anyons, and is determined by the number of paths leading to that particular vertex. In general, the dimension of the fusion space of N anyons can be computed as

$$\lfloor n \rfloor_q^N = \left(\frac{q^{n/2} - q^{-n/2}}{q^{1/2} - q^{-1/2}}\right)^N,$$
 (B6)

where  $n \in \frac{1}{2}\mathbb{Z}$  and  $q = e^{i2\pi/(k+2)}$  [45]. This is referred to as a *q*-deformed integer and it can be shown that all SU(2) representations are recovered, i.e.,  $\lfloor n \rfloor_q \to n$  and thus  $q \to 1$ , as we let  $k \to \infty$  [87]. In fact, this is the very reason why the Hilbert spaces spanned by multiple full SU(2) spins can be decomposed into irreducible subspaces since these systems correspond to  $k \to \infty$ , which yields an integer dimension. Thus, we can think of  $\lfloor n \rfloor_q$  as a deformation of the integer *n*. When *k* takes on a finite value, however, the deformed integer will in many cases be irrational, which means that such a decomposition is not



FIG. 18. Two fusion tree representations, (a) and (b), of the process  $q_1 \otimes q_2 \otimes q_3 \otimes q_4$  where 1 represents the vacuum.

always possible as we eliminated higher-dimensional representation spaces, leaving a deformed structure behind. This nontrivial decomposition signals an existence of nonabelian braiding statistics, which will be discussed in more detail in the next subsection.

It is convenient to introduce a schematic notation for the fusion processes. Let us denote by  $q_i$  the charge of the *i*th anyon and by  $x_i$  the fusion outcome of anyons *i* and *i* + 1; then a fusion process can be represented as a tree diagram. In Fig. 18(a) a fusion process involving the charges  $q_1$ ,  $q_2$ ,  $q_3$ , and  $q_4$  is presented. Henceforth, we shall adopt this notation for fusion processes.

### 2. F moves and R moves

When anyons participate in a fusion process, the final outcome must be independent of the order in which the anyons are being fused, since the total charge must be preserved. Or in mathematical terms, we have to enforce associativity upon the fusion rules. For instance, in Fig. 18(a), the anyons are fused sequentially, but we could just as well have fused  $q_1$  with  $q_2$  right away to form  $x'_1$  (this is essentially what is happening already as  $q_1$  is first fused with the vacuum, which implies that  $x'_1 = x_2$ ) and then  $x'_1 = x_2$  with the fusion outcome  $x'_2$  of  $q_3$  and  $q_4$ . This process is depicted in Fig. 18(b).

In topological quantum computation the two configurations, Figs. 18(a) and 18(b), correspond to different basis states and a change from one basis to another is realized by applying an F move. For simplicity, let us consider three anyons a, b, c and their fusion product d, which can be formed in  $N_{abc}^d$  distinct ways. Their fusion space  $V_{abc}^d$ can then be decomposed in two different, but up to an isomorphism, similar ways such that [11]

$$V^{d}_{abc} \simeq \bigoplus_{e} V^{e}_{ab} \otimes V^{d}_{ec} \simeq \bigoplus_{e'} V^{e'}_{bc} \otimes V^{d}_{ae'}.$$
 (B7)

First, the tensor product of the vector spaces corresponding to a and b forming e, and e and c forming d, can be composed, where e is summed over. And second, the tensor product of the vector spaces corresponding to b and cforming e', and a and e' forming d can be composed, where e' is summed over. We may also assign ket vectors to the



FIG. 19. A graphical illustration of the F move corresponding to the Eq. (B10).

different bases

$$|(ab)c \rightarrow d; e, \mu, \nu\rangle \equiv |ab; e, \mu\rangle \otimes |ec; d, \nu\rangle$$
 (B8)

and

$$|a(bc) \to d; e', \mu', \nu'\rangle \equiv |ae'; d, \nu'\rangle \otimes |bc; e', \mu'\rangle.$$
(B9)

Here  $\mu$ ,  $\nu$ ,  $\mu'$ , and  $\nu'$  label the specific fusion channels out of the  $N_{abc}^d$  unique products. The transformation F maps the basis  $a \otimes (b \otimes c)$  to  $(a \otimes b) \otimes c$  and can be formulated as

$$|(ab)c \to d; e, \mu, \nu\rangle$$
  
= 
$$\sum_{e',\mu',\nu'} (F^d_{abc})^{e'\mu'\nu'}_{e\mu\nu} |a(bc) \to d; e', \mu', \nu'\rangle, \quad (B10)$$

or expressed graphically as shown in Fig. 19. Moreover, braiding two of the charges should not change the total charge. In Fig. 20 we illustrate this charge conservation in terms of an R move. By applying these transformations sequentially, it is possible to derive two consistency equations known as the hexagon equation

$$\sum_{\lambda\gamma} [R_e^{ac}]_{\alpha\lambda} [F_d^{acb}]_{(e\lambda\beta)(g\gamma\nu)} [R_g^{bc}]_{\gamma\mu}$$
$$= \sum_{f \sigma \delta \psi} [F_d^{cab}]_{(e\alpha\beta)(f \delta \sigma)} [R_d^{fc}]_{\sigma\psi} [F_d^{abc}]_{(f \delta \psi)(g\mu\nu)}$$
(B11)

and the pentagon equation

$$\sum_{\delta} [F_e^{fcd}]_{(g\beta\gamma)(l\delta\nu)} [F_e^{abl}]_{(f \ \alpha\delta)(k\lambda\mu)}$$

$$= \sum_{h\sigma\psi\rho} [F_g^{abc}]_{(f \ \alpha\beta)(h\sigma\psi)} [F_e^{ahd}]_{(g\sigma\gamma)(k\lambda\rho)} [F_k^{bcd}]_{(h\psi\rho)(l\mu\nu)},$$
(B12)

and a graphical representation of these equations can be found, for instance, in Refs. [8,13,86].

The solutions to this set of equations embody all essential information about the anyon model since we are mostly interested in the transformation properties under F moves and R moves. Suppose that we would like to exchange charges a and b and that our initial basis is  $|a(bc) \rightarrow d\rangle$ . We would first have to transform the basis to  $|(ab)c \rightarrow d\rangle$ under the action of F, in order to execute the exchange, and thereafter return to the initial basis by acting with the  $F^{-1}$ . Hence, in this new basis, the braid generators would be given by

$$B_{ab} = F^{-1} R_{ab} F \tag{B13}$$

and

$$B_{bc} = R_{bc}.$$
 (B14)

The solutions to the hexagon and pentagon equations for an arbitrary value of k have been determined in the comprehensive literature on quantum groups; see, for instance, Refs. [87–89]. These solutions are

$$R_{ab}^{c} = (-1)^{(a+b-c)/2} q^{-[a(a+2)+b(b+2)-c(c+2)]/2}$$
(B15)

and

$$(F_d^{abc})_f^e = (-1)^{a+b+c+d} \Delta(a,b,e) \Delta(c,d,e)$$
$$\times \Delta(b,c,f) \Delta(a,d,f) \sqrt{\lfloor 2e+1 \rfloor} \sqrt{\lfloor 2f+1 \rfloor}$$
$$\times \begin{cases} a & b & e \\ c & d & f \end{cases},$$
(B16)

where

$$\begin{cases} a & b & e \\ c & d & f \end{cases} = \sum_{n} \frac{(-1)^{n} \lfloor n+1 \rfloor}{\lfloor a+b+c+d-n \rfloor!} \times \frac{1}{\lfloor a+c+e+f-n \rfloor! \lfloor b+d+e+f-n \rfloor! \lfloor n-a-b-e \rfloor!} \\ \times \frac{1}{\lfloor n-c-d-e \rfloor! \lfloor n-b-c-f \rfloor! \lfloor n-a-d-f \rfloor!}.$$
(B17)

Equation (B17) is a *q*-deformed version of the Wigner 6j symbol describing the transformation under recoupling in the representation theory of  $SU(2)_k$ .

# 3. Universal quantum computation

Computational universality is required in order to carry out general purpose quantum computation. The



FIG. 20. A graphical illustration of the *R* move.

Solovay-Kitaev theorem, discussed in more detail in Sec. II C, states that universality is achieved only if the gate set is generating a topologically dense cover in SU(2). Thus, an important question is for what values of k is this satisfied. All information about the relation between the level k and universality can be summarized in the following two theorems [13].

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

Here  $\rho_{k,n}$  is a representation of the braid group  $\mathbb{B}_n$  on *n* strands. It was later shown by Freedman *et al.* [90] that the whole special unitary group will be contained in the closed image of this representation for these particular values of *k*, which led to the second fundamental theorem [90].

**Theorem 3** (Freedman, Larsen, Wang). When the image of  $\overline{\rho_{k,n}}$  is infinite, it holds that  $SU(V_{k,n}) \subset image(\overline{\rho_{k,n}})$ .

In words, this simply entails that, when the closed image is infinite, the special unitary group will be contained in the image, which further implies that universality is achieved. This is a very natural result as the Bloch sphere is a compact manifold. Hence, if the image contains an infinite number of unique points, the set must fill up the entire sphere densely.

# 4. The Fibonacci and Ising anyon models

The Fibonacci (k = 3) and Ising (k = 2) anyon models are the simplest and by far the most studied SU(2)<sub>k</sub> models. By virtue of the automorphism defined in Eq. (B5), the SU(2)<sub>3</sub> Fibonacci anyon model only has integer (or halfinteger) charges. In particular, for k = 3, we have j = 0, 1, which yields the fusion rules shown in Table V where 0 corresponds to the vacuum charge 1 and 1 to the Fibonacci anyon  $\tau$ . These fusion rules, as well as those for any other value of k, can be derived from Eq. (B2). Moreover, solving the hexagon and pentagon equations, Eqs. (B12) and (B11), provides the explicit forms of the braid matrix R and the basis change matrix F, i.e.,

$$R_{k=3} = \begin{pmatrix} e^{-i4\pi/5} & 0\\ 0 & e^{i3\pi/5} \end{pmatrix},$$
  
$$F_{k=3} = \begin{pmatrix} \varphi^{-1/2} & \varphi^{-1/2}\\ \varphi^{-1/2} & -\varphi^{-1/2} \end{pmatrix},$$
 (B18)

which in turn can be used to obtain the braid matrices

$$\sigma_1 = R_{k=3} = \begin{pmatrix} e^{-i4\pi/5} & 0\\ 0 & e^{i3\pi/5} \end{pmatrix}$$
(B19)

and

$$\sigma_2 = (FRF^{-1})_{k=3} = \begin{pmatrix} \varphi^{-1}e^{i4\pi/5} & \varphi^{-1/2}e^{-i3\pi/5} \\ \varphi^{-1/2}e^{-i3\pi/5} & -\varphi^{-1} \end{pmatrix},$$
(B20)

where  $\varphi = (1 + \sqrt{5})/2$  is the golden ratio. The emergence of this particular number is due to the expansion of the anyon Hilbert space as anyons are added to the system. Two anyons yield a Hilbert space of dimension 2, three of dimension 3, four of dimension 5, etc., resulting in the Fibonacci sequence and the quantum dimension  $d_{k=3} = (1 + \sqrt{5})/2$  of the Hilbert space. The quantum dimension may also be computed by means of Eq. (B6) by inserting k = 3. The Fibonacci generators are tenth roots of unity and the entries of the matrices generated by Fibonacci braids are all members of

| $\otimes$   | $j_1 = 0$  | $j_1 = \frac{1}{2}$   | $j_1 = 1$   | $j_1 = \frac{3}{2}$  | $j_1 = 2$  | $j_1 = \frac{5}{2}$   | $j_1 = 3$   | $j_1 = \frac{7}{2}$   | $j_1 = 4$  |
|---|--|---|---|--|--|---|---|---|--|
| $j_{2} = 0$ $j_{2} = \frac{1}{2}$ $j_{2} = 1$ $j_{2} = \frac{3}{2}$ $j_{2} = 2$ $j_{2} = \frac{5}{2}$ $j_{2} = 3$ $j_{2} = \frac{7}{2}$ $j_{2} = 4$ | $ \begin{array}{c} 0 \\ \frac{1}{2} \\ 1 \\ \frac{3}{2} \\ 2 \\ \frac{5}{2} \\ 3 \\ \frac{7}{2} \\ 4 \end{array} $ | $ \begin{array}{c} \frac{1}{2} \\ 0 \oplus 1 \\ \frac{1}{2} \oplus \frac{3}{2} \\ 1 \oplus 2 \\ \frac{3}{2} \oplus \frac{5}{2} \\ 2 \oplus 3 \\ \frac{5}{2} \oplus \frac{7}{2} \\ 3 \oplus 4 \\ \frac{7}{2} \end{array} $ | $1$ $\frac{1}{2} \oplus \frac{3}{2}$ $0 \oplus 1 \oplus 2$ $\frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2}$ $1 \oplus 2 \oplus 3$ $\frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2}$ $2 \oplus 3 \oplus 4$ $\frac{5}{2} \oplus \frac{7}{2}$ $3$ | $ \begin{array}{c} \frac{3}{2} \\ 1 \oplus 2 \\ \frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2} \\ 0 \oplus 1 \oplus 2 \oplus 3 \\ \frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2} \\ 1 \oplus 2 \oplus 3 \oplus 4 \\ \frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2} \\ 2 \oplus 3 \\ \frac{5}{2} \oplus \frac{5}{2} \\ 2 \oplus 3 \\ \frac{5}{2} \\ $ | $2$ $\frac{3}{2} \oplus \frac{5}{2}$ $1 \oplus 2 \oplus 3$ $\frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2}$ $0 \oplus 1 \oplus 2 \oplus 3 \oplus 4$ $\frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2}$ $1 \oplus 2 \oplus 3$ $\frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2}$ $2$ | $ \begin{array}{c} \frac{5}{2} \\ 2 \oplus 3 \\ \frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2} \\ 1 \oplus 2 \oplus 3 \oplus 4 \\ \frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2} \oplus \frac{7}{2} \\ 0 \oplus 1 \oplus 2 \oplus 3 \\ \frac{1}{2} \oplus \frac{3}{2} \oplus \frac{4}{2} \\ 1 \oplus 2 \\ \frac{3}{2} \end{array} $ | $3$ $5 \oplus 7$ $2 \oplus 3 \oplus 4$ $3 \oplus 5 \oplus 7$ $2 \oplus 3 \oplus 4$ $3 \oplus 5 \oplus 7$ $1 \oplus 2 \oplus 3$ $1 \oplus 2 \oplus 3$ $1 \oplus 2$ $1 \oplus 1 \oplus 2$ $1 \oplus 3$ $1 \oplus $ | $\begin{array}{c} \frac{7}{2} \\ 3 \oplus 4 \\ \frac{5}{2} \oplus \frac{7}{2} \\ 2 \oplus 3 \\ \frac{3}{2} \oplus \frac{5}{2} \\ 1 \oplus 2 \\ \frac{1}{2} \oplus \frac{3}{2} \\ 0 \oplus 1 \\ \frac{1}{2} \end{array}$ | $ \begin{array}{c} 4 \\ \frac{7}{2} \\ 3 \\ \frac{5}{2} \\ 2 \\ \frac{3}{2} \\ 1 \\ \frac{1}{2} \\ 0 \end{array} $ |

TABLE I. Fusion table for the k = 8 anyon model.

| $\otimes$  | $j_1 = 0$  | $j_1 = \frac{1}{2}$   | $j_1 = 1$   | $j_1 = \frac{3}{2}$   | $j_1 = 2$   | $j_1 = \frac{5}{2}$   | $j_1 = 3$   |
|--|--|---|---|---|---|---|---|
| $     \begin{array}{r}       j_2 = 0 \\       j_2 = \frac{1}{2} \\       j_2 = 1 \\       j_2 = \frac{3}{2} \\       j_2 = 2 \\       j_2 = \frac{5}{2} \\       j_2 = 3     \end{array} $ | $ \begin{array}{c} 0 \\ \frac{1}{2} \\ 1 \\ \frac{3}{2} \\ 2 \\ \frac{5}{2} \\ 3 \end{array} $ | $ \begin{array}{c} \frac{1}{2} \\ 0 \oplus 1 \\ \frac{1}{2} \oplus \frac{3}{2} \\ 1 \oplus 2 \\ \frac{3}{2} \oplus \frac{5}{2} \\ 2 \oplus 3 \\ \frac{5}{2} \end{array} $ | $1$ $\frac{\frac{1}{2} \oplus \frac{3}{2}}{0 \oplus 1 \oplus 2}$ $\frac{\frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2}}{1 \oplus 2 \oplus 3}$ $\frac{\frac{3}{2} \oplus \frac{5}{2}}{2}$ | $1 \bigoplus 2$ $\frac{1}{2} \bigoplus \frac{3}{2} \bigoplus \frac{5}{2}$ $0 \bigoplus 1 \bigoplus 2 \bigoplus 3$ $\frac{1}{2} \bigoplus \frac{3}{2} \bigoplus \frac{5}{2}$ $1 \bigoplus 2 \bigoplus 3$ $\frac{1}{2} \bigoplus \frac{3}{2} \bigoplus \frac{5}{2}$ $1 \bigoplus 2$ $\frac{3}{2}$ | $2$ $\frac{3}{2} \oplus \frac{5}{2}$ $1 \oplus 2 \oplus 3$ $\frac{1}{2} \oplus \frac{3}{2} \oplus \frac{5}{2}$ $0 \oplus 1 \oplus 2$ $\frac{1}{2} \oplus \frac{3}{2}$ $1$ | $ \begin{array}{c} \frac{5}{2}\\ 2 \oplus 3\\ \frac{3}{2} \oplus \frac{5}{2}\\ 1 \oplus 2\\ \frac{1}{2} \oplus \frac{3}{2}\\ 0 \oplus 1\\ \frac{1}{2} \end{array} $ | $ \begin{array}{c} 3 \\ 5 \\ 2 \\ 2 \\ 3 \\ 2 \\ 1 \\ 1 \\ 2 \\ 0 \end{array} $ |

TABLE II. Fusion table for the k = 6 anyon model.

the polynomial ring  $\mathbb{Z}[e^{i\pi/5}] = \{c_1 + c_2 e^{i\pi/5} + c_3 e^{i2\pi/5} + c_4 e^{i3\pi/5} | c_i \in \mathbb{Z}\}$ . Rings, like groups, are closed structures, which implies that only unitary matrices with entries in this ring can be approximated exactly.

The SU(2)<sub>2</sub> Ising anyon model has charges  $j = 0, \frac{1}{2}, 1$ , where in addition to the vacuum (j = 0), we have the Ising anyon  $\sigma$   $(j = \frac{1}{2})$  and the  $\psi$  particle (j = 1). Computing the fusion rules of these particles yields the fusion table in Table VI. Similarly to the Fibonacci model the *F* and *R* matrices can be computed to be

$$R_{k=2} = e^{-i\pi/8} \begin{pmatrix} 1 & 0\\ 0 & i \end{pmatrix}, \qquad F_{k=2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1\\ 1 & -1 \end{pmatrix},$$
(B21)

which in turn yield the braids matrices

$$\sigma_1 = R_{k=2} = e^{-i\pi/8} \begin{pmatrix} 1 & 0\\ 0 & i \end{pmatrix}$$
 (B22)

and

$$\sigma_2 = (FRF^{-1})_{k=2} = \frac{e^{-i4\pi/8}}{\sqrt{2}} \begin{pmatrix} 1 & i\\ i & 1 \end{pmatrix}.$$
 (B23)

An alternative method of determining the F and R matrices is to employ the Temperley-Lieb algebra, which may be regarded as a pictorial string representation of Eqs. (A1), and the Jones-Wenzl projectors [87,91]. This approach allows computation of the matrices for any value of k by means of graphical calculus [91].

It is evident in the structure of the *F* matrix that the quantum dimension of the Ising anyon model is  $d_{k=2} = \sqrt{2}$ . An interesting property of the Ising braid group representation for n = 2 is that it maps bijectively onto the

TABLE III. Fusion table for the k = 5 anyon model.

| $\otimes$ | <i>j</i> <sub>1</sub> =0 | $j_1 = 1$             | $j_1 = 2$    |
|-----------|--------------------------|-----------------------|--------------|
| $j_2 = 0$ | 0                        | 1                     | 2            |
| $j_2 = 1$ | 1                        | $0 \oplus 1 \oplus 2$ | 1            |
| $j_2 = 2$ | 2                        | 1                     | $0 \oplus 1$ |

Clifford group, meaning that Ising anyons are an implementation of the Clifford group via braiding. For systems comprised of  $n \neq 2$  qubits, however, it only maps onto subgroups of the Clifford group [92]. The Clifford group can be made universal by adding a  $\pi/4$  gate, so it must also hold that the two-qubit Ising anyon model becomes universal with this choice of supplementary phase. In Sec. III we discussed the fact that any nonuniversal single-qubit anyon model can be made universal via the addition of an irrational phase gate to the generator set.

### 5. Model-k (k = 4, 5, 6, 8) anyons

We briefly outline the structure of the anyon models labeled by k = 4, 5, 6, 8. Contrary to the Ising and Fibonacci cases, the higher-level models provide multiple options of fusion products that can be used as a qubit. For k = 4, the model contains the charges  $j = 0, \frac{1}{2}, 1, \frac{3}{2}, 2$  and the fusion table is provided in Table IV.

Similarly, Eq. (B2) may be used for obtaining the fusion tables for k = 5, 6, 8 as well. In the k = 5 model we have the charges  $j = 0, \frac{1}{2}, 1, \frac{3}{4}, 2, \frac{5}{2}$ , but due to the duality defined by Eq. (B5), there exists an automorphism from the integer subset to the half-integer subset, which means that we only have to consider one of them. Therefore, in the k = 5 model it is sufficient to consider the j = 0, 1, 2

TABLE IV. Fusion table for the k = 4 anyon model.

|                                  |               | . 1  |   | . 3   |                                  |
|----------------------------------|---------------|--|---|---|----------------------------------|
| $\otimes$                        | $j_1 = 0$     | $j_1 = \frac{1}{2}$  | $j_1 = 1$   | $j_1 = \frac{3}{2}$                                     | $j_1 = 2$                        |
| $j_2 = 0$                        | 0             | $\frac{1}{2}$  | 1   | $\frac{3}{2}$   | 2                                |
| $j_2 = \frac{1}{2}$<br>$j_2 = 1$ | $\frac{1}{2}$ | $\begin{array}{c} 0 \oplus 1 \\ \frac{1}{2} \oplus \frac{3}{2} \end{array}$    | $\frac{1}{2} \oplus \frac{3}{2}$<br>$0 \oplus 1 \oplus 2$ | $1 \oplus 2$<br>$\frac{1}{2} \oplus \frac{3}{2}$        | $\frac{3}{2}$                    |
| $j_2 = \frac{3}{2}$              | $\frac{3}{2}$ | $\stackrel{\scriptscriptstyle 2}{1} \oplus \stackrel{\scriptscriptstyle 2}{2}$ | $\frac{1}{2} \oplus \frac{3}{2}$                          | $\begin{array}{c} 2 \oplus 2 \\ 0 \oplus 1 \end{array}$ | $\frac{1}{2} \oplus \frac{3}{2}$ |
| $j_2 = 2$                        | 2             | $\frac{3}{2}$  | 1   | $\frac{1}{2} \oplus \frac{3}{2}$                        | 0                                |

TABLE V. Fusion table for the k = 3 anyon model.

| $\otimes$ | <i>j</i> <sub>1</sub> =0 | $j_1 = 1$    |
|-----------|--------------------------|--------------|
| $j_2 = 0$ | 0                        | 1            |
| $j_2 = 1$ | 1                        | $0 \oplus 1$ |

TABLE VI. Fusion table for the k = 2 anyon model.

| $\otimes$  | <i>j</i> <sub>1</sub> =0   | $j_1 = \frac{1}{2}$                             | $j_1 = 1$                                      |
|--|--|---|--|
| $     \begin{array}{r} j_2 = 0 \\ j_2 = \frac{1}{2} \\ j_2 = 1 \end{array} $ | $     \begin{array}{c}       0 \\       \frac{1}{2} \\       1     \end{array} $ | $0 \oplus 1 \\ \frac{\frac{1}{2}}{\frac{1}{2}}$ | $\begin{array}{c}1\\\frac{1}{2}\\0\end{array}$ |

cases. The fusion table for the k = 5 anyon model is shown in Table III.

In the k = 6 and k = 8 models, shown respectively in Tables II and I, such a map between the substructures does not exist, which means that all charges are distinct, i.e.,  $j = 0, \frac{1}{2}, 1, \frac{3}{4}, 2, \frac{5}{2}, 3$  for k = 6 and  $j = 0, \frac{1}{2}, 1, \frac{3}{4}, 2, \frac{5}{2}, 3, \frac{7}{2}, 4$  for k = 8. Inspecting the fusion tables shows that all of them contain indefinite fusion products, which means that all of the models have some charges transforming under a nonabelian braid group. However, due to Theorems 2 and 3, the models labeled by k = 2 (Ising) and k = 4 are nonuniversal, which means that their generator sets must be supplemented with an additional gate in order to carry out general purpose computation.

- [1] X.-G. Wen, Colloquium: Zoo of quantum-topological phases of matter, Rev. Mod. Phys. **89**, 041004 (2017).
- [2] E. Witten, Three lectures on topological phases of matter, Riv. del Nuovo Cim. **39**, 313 (2016).
- [3] A. Kitaev and C. Laumann, in *Exact Methods in Low-Dimensional Statistical Physics and Quantum Computing*, Lecture Notes of the Les Houches Summer School Vol. 89 (Oxford University Press, 2008), p. 101.
- [4] H. Bombín, Topological Order with a Twist: Ising Anyons from an Abelian Model, Phys. Rev. Lett. 105, 030403 (2010).
- [5] R. B. Laughlin, Anomalous Quantum Hall Effect: An Incompressible Quantum Fluid with Fractionally Charged Excitations, Phys. Rev. Lett. 50, 1395 (1983).
- [6] J. M. Leinaas and J. Myrheim, On the theory of identical particles, Nuovo Cimento B Ser. 37, 1 (1977).
- [7] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. 303, 2 (2003).
- [8] B. Field and T. Simula, Introduction to topological quantum computation with non-Abelian anyons, Quantum Sci. Technol. 3, 021 045004 (2018).
- [9] V. Lahtinen and J. K. Pachos, A short introduction to topological quantum computation, SciPost Phys. 3, 021 (2017).
- [10] J. K. Pachos, Introduction to Topological Quantum Computation (Cambridge University Press, Cambridge, 2012).
- [11] J. Preskill, in *Topological Quantum Computation*, Lecture Notes for Physics Vol. 219 (2004).
- [12] A. Y. Kitaev, Quantum computations: Algorithms and error correction, Russ. Math. Surv. 52, 1191 (1997).
- [13] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, Non-Abelian anyons and topological quantum computation, Rev. Mod. Phys. 80, 1083 (2008).

- [14] A. Lerda, Anyons: Quantum Mechanics of Particles with Fractional Statistics (Springer Science & Business Media, Springer, Berlin, Heidelberg, 2008), Vol. 14.
- [15] F. Wilczek, Fractional Statistics and Anyon Superconductivity (World Scientific, 1990), Vol. 5.
- [16] V. Gurarie and L. Radzihovsky, Resonantly paired fermionic superfluids, Ann. Phys. 322, 2 (2007).
- [17] S. Tewari, S. Das Sarma, C. Nayak, C. Zhang, and P. Zoller, Quantum Computation Using Vortices and Majorana Zero Modes of a  $p_x + ip_y$  Superfluid of Fermionic Cold Atoms, Phys. Rev. Lett. **98**, 010506 (2007).
- [18] T. Mizushima, M. Ichioka, and K. Machida, Role of the Majorana Fermion and the Edge Mode in Chiral Superfluidity near a p-Wave Feshbach Resonance, Phys. Rev. Lett. 101, 150409 (2008).
- [19] L. Jiang, T. Kitagawa, J. Alicea, A. R. Akhmerov, D. Pekker, G. Refael, J. I. Cirac, E. Demler, M. D. Lukin, and P. Zoller, Majorana Fermions in Equilibrium and in Driven Cold-Atom Quantum Wires, Phys. Rev. Lett. **106**, 220402 (2011).
- [20] R. M. Lutchyn, E. P. A. M. Bakkers, L. P. Kouwenhoven, P. Krogstrup, C. M. Marcus, and Y. Oreg, Majorana zero modes in superconductor-semiconductor heterostructures, Nat. Rev. Mater. 3, 52 (2018).
- [21] G. Livanas, M. Sigrist, and G. Varelogiannis, Alternative paths to realize Majorana fermions in superconductorferromagnet heterostructures, Sci. Rep. 9, 6259 (2019).
- [22] M. Sato and S. Fujimoto, Majorana fermions and topology in superconductors, J. Phys. Soc. Jpn 85, 072001 (2016).
- [23] H. Zhang, D. E. Liu, M. Wimmer, and L. P. Kouwenhoven, Next steps of quantum transport in Majorana nanowire devices, Nat. Commun. 10, 5128 (2019).
- [24] E. Prada, P. San-Jose, M. W. A. de Moor, A. Geresdi, E. J. H. Lee, J. Klinovaja, D. Loss, J. Nygård, R. Aguado, and L. P. Kouwenhoven, From Andreev to Majorana bound states in hybrid superconductor-semiconductor nanowires, Nat. Rev. Phys. 2, 575 (2020).
- [25] C. W. J. Beenakker, Search for non-Abelian Majorana braiding statistics in superconductors, SciPost Phys. Lect. Notes 15 (2020).
- [26] T. D. Stanescu and S. Tewari, Majorana fermions in semiconductor nanowires: Fundamentals, modeling, and experiment, J. Phys. Condens. Matter 25, 233201 (2013).
- [27] Y. Kasahara, T. Ohnishi, Y. Mizukami, O. Tanaka, S. Ma, K. Sugii, N. Kurita, H. Tanaka, J. Nasu, Y. Motome, *et al.*, Majorana quantization and half-integer thermal quantum Hall effect in a Kitaev spin liquid, Nature 559, 227 (2018).
- [28] Z.-W. Zuo, H. Li, L. Li, L. Sheng, R. Shen, and D. Y. Xing, Detecting Majorana fermions by use of superconductorquantum Hall liquid junctions, Europhys. Lett. 114, 27001 (2016).
- [29] T. Simula, Quantised Vortices; A Handbook of Topological Excitations (2019), https://doi.org/10.1088/2053-2571/aaf b9d.
- [30] S. Vaitiekenas, G. W. Winkler, B. van Heck, T. Karzig, M.-T. Deng, K. Flensberg, L. I. Glazman, C. Nayak, P. Krogstrup, R. M. Lutchyn, and C. M. Marcus, Flux-induced topological superconductivity in full-shell nanowires, Science 367 (2020).

- [31] A. Vaezi and M. Barkeshli, Fibonacci Anyons From Abelian Bilayer Quantum Hall States, Phys. Rev. Lett. 113, 236804 (2014).
- [32] R. S. K. Mong, M. P. Zaletel, F. Pollmann, and Z. Papić, Fibonacci anyons and charge density order in the 12/5 and 13/5 quantum Hall plateaus, Phys. Rev. B 95, 115136 (2017).
- [33] J. S. Xia, W. Pan, C. L. Vicente, E. D. Adams, N. S. Sullivan, H. L. Stormer, D. C. Tsui, L. N. Pfeiffer, K. W. Baldwin, and K. W. West, Electron Correlation in the Second Landau Level: A Competition between Many Nearly Degenerate Quantum Phases, Phys. Rev. Lett. 93, 176809 (2004).
- [34] Y. Komijani, Kondo-based qubits for topological quantum computation, Phys. Rev. B 101, 235131 (2019).
- [35] P. Bonderson, M. Freedman, and C. Nayak, Measurement-Only Topological Quantum Computation, Phys. Rev. Lett. 101, 010501 (2008).
- [36] P. Bonderson, M. Freedman, and C. Nayak, Measurementonly topological quantum computation via anyonic interferometry, Ann. Phys. 324, 787 (2009).
- [37] T. Karzig, C. Knapp, R. M. Lutchyn, P. Bonderson, M. B. Hastings, C. Nayak, J. Alicea, K. Flensberg, S. Plugge, Y. Oreg, C. M. Marcus, and M. H. Freedman, Scalable designs for quasiparticle-poisoning-protected topological quantum computation with Majorana zero modes, Phys. Rev. B 95, 235305 (2017).
- [38] S. Plugge, A. Rasmussen, R. Egger, and K. Flensberg, Majorana box qubits, New J. Phys. 19, 012001 (2017).
- [39] T. B. Smith, M. C. Cassidy, D. J. Reilly, S. D. Bartlett, and A. L. Grimsmo, Dispersive readout of majorana qubits, PRX Quantum 1, 020313 (2020).
- [40] M. Burrello, H. Xu, G. Mussardo, and X. Wan, Topological Quantum Hashing with the Icosahedral Group, Phys. Rev. Lett. 104, 160502 (2010).
- [41] V. Kliuchnikov, A. Bocharov, and K. M. Svore, Asymptotically Optimal Topological Quantum Compiling, Phys. Rev. Lett. 112, 140504 (2014).
- [42] C. M. Dawson and M. A. Nielsen, The Solovay-Kitaev algorithm, Quantum Inf. Comput. 6, 81 (2006).
- [43] Y.-H. Zhang, P.-L. Zheng, Y. Zhang, and D.-L. Deng, Topological Quantum Compiling with Reinforcement Learning, Phys. Rev. Lett. 125, 170501 (2020).
- [44] N. E. Bonesteel, L. Hormozi, G. Zikos, and S. H. Simon, Braid Topologies for Quantum Computation, Phys. Rev. Lett. 95, 140503 (2005).
- [45] L. Hormozi, G. Zikos, N. E. Bonesteel, and S. H. Simon, Topological quantum compiling, Phys. Rev. B 75, 165310 (2007).
- [46] N. Prokof'ev and B. Svistunov, Worm Algorithms for Classical Statistical Models, Phys. Rev. Lett. 87, 160601 (2001).
- [47] M. Boninsegni, N. Prokof'ev, and B. Svistunov, Worm Algorithm for Continuous-Space Path Integral Monte Carlo Simulations, Phys. Rev. Lett. 96, 070601 (2006).
- [48] J. Bringewatt, W. Dorland, and S. P. Jordan, Polynomial time algorithms for estimating spectra of adiabatic Hamiltonians, Phys. Rev. A 100, 032336 (2019).

- [49] S. P. Jordan, D. Gosset, and P. J. Love, Quantum-Merlin-Arthur–complete problems for stoquastic Hamiltonians and Markov matrices, Phys. Rev. A 81, 032331 (2010).
- [50] S. Bravyi, D. P. Divincenzo, R. I. Oliveira, and B. M. Terhal, The complexity of stoquastic local Hamiltonian problems, Quantum Inf. Comput. 8 (2006).
- [51] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
- [52] V. Kliuchnikov, Synthesis of unitaries with Clifford+T circuits, arXiv:1306.3200 [quant-ph] (2013).
- [53] A. Paetznick and K. M. Svore, Repeat-until-success: Non-deterministic decomposition of single-qubit unitaries, Quantum Inf. Comput. 14, 1277 (2014).
- [54] P. Selinger, Efficient Clifford+T approximation of singlequbit operators, Quantum Inf. Comput. 15, 159 (2015).
- [55] A. Bocharov, M. Roetteler, and K. M. Svore, Efficient synthesis of probabilistic quantum circuits with fallback, Phys. Rev. A 91, 052317 (2015).
- [56] N. J. Ross and P. Selinger, Optimal ancilla-free Clifford+ T approximation of z-rotations, Quantum Inf. Comput. 16 (2014).
- [57] V. Kliuchnikov, D. Maslov, and M. Mosca, Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits, IEEE Trans. Comput. 65, 161 (2016).
- [58] R. Raussendorf and J. Harrington, Fault-Tolerant Quantum Computation with High Threshold in two Dimensions, Phys. Rev. Lett. 98, 190504 (2007).
- [59] A. G. Fowler, A. M. Stephens, and P. Groszkowski, Highthreshold universal quantum computation on the surface code, Phys. Rev. A 80, 052312 (2009).
- [60] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation, Phys. Rev. A 86, 032324 (2012).
- [61] E. T. Campbell, B. M. Terhal, and C. Vuillot, Roads towards fault-tolerant universal quantum computation, Nature 549, 172 (2017).
- [62] D. Gottesman, in *Quantum Information Science and its Contributions to Mathematics*, Proceedings of Symposia in Applied Mathematics Vol. 68 (2010), p. 13.
- [63] P. Webster and S. D. Bartlett, Fault-tolerant quantum gates with defects in topological stabilizer codes, Phys. Rev. A 102, 022403 (2020).
- [64] B. J. Brown, S. D. Bartlett, A. C. Doherty, and S. D. Barrett, Topological Entanglement Entropy with a Twist, Phys. Rev. Lett. 111, 220402 (2013).
- [65] A. Sawicki and K. Karnas, Criteria for universality of quantum gates, Phys. Rev. A 95, 062303 (2017).
- [66] P. Bonderson, D. J. Clarke, C. Nayak, and K. Shtengel, Implementing Arbitrary Phase Gates with Ising Anyons, Phys. Rev. Lett. 104, 180505 (2010).
- [67] Note that we equally well could have chosen  $\sigma_2$ .
- [68] This result is known as Lagrange's theorem [93].
- [69] R. W. Heeres, P. Reinhold, N. Ofek, L. Frunzio, L. Jiang, M. H. Devoret, and R. J. Schoelkopf, Implementing a universal gate set on a logical qubit encoded in an oscillator, Nat. Commun. 8, 1 (2017).
- [70] C. Jones, M. A. Fogarty, A. Morello, M. F. Gyure, A. S. Dzurak, and T. D. Ladd, Logical Qubit in a Linear Array

of Semiconductor Quantum Dots, Phys. Rev. X 8, 021058 (2018).

- [71] C. Levaillant, B. Bauer, M. Freedman, Z. Wang, and P. Bonderson, Universal gates via fusion and measurement operations on  $SU(2)_4$  anyons, Phys. Rev. A **92**, 012301 (2015).
- [72] S. Das Sarma, M. Freedman, and C. Nayak, Majorana zero modes and topological quantum computation, npj Quantum Inf 1, 15001 (2015).
- [73] A. Conlon, D. Pellegrino, J. K. Slingerland, S. Dooley, and G. Kells, Error generation and propagation in Majoranabased topological qubits, Phys. Rev. B 100, 134307 (2019).
- [74] F. Arute *et al.*, Quantum supremacy using a programmable superconducting processor, Nature (London) 574, 505 (2019).
- [75] P. Panangaden and É. O. Paquette, in New structures for Physics (Springer, 2010), p. 983.
- [76] A. Blass and Y. Gurevich, in *Martin Davis on Computability, Computational Logic, and Mathematical Foundations*, edited by E. Omodeo and A. Policriti, Outstanding Contributions to Logic Vol. 10. (Springer, Cham, Switzerland, 2016).
- [77] L. Kong, Anyon condensation and tensor categories, Nucl. Phys. B 886, 436 (2014).
- [78] E. Witten, Topological quantum field theory, Commun. Math. Phys. 117, 353 (1988).
- [79] M. F. Atiyah, Topological quantum field theories, Publ. Math. l'IHÉS 68, 175 (1988).
- [80] G. V. Dunne, in Aspects Topologiques de la Physique en Basse Dimension. Topological Aspects of Low Dimensional Systems, edited by A. Comtet, T. Jolicœur, S. Ouvry, and F. David, Les Houches – Ecole d'Ete de Physique Theorique Vol. 69 (Springer, Berlin, Heidelberg, 1999).
- [81] C. N. Yang and M.-L. Ge, Braid Group, Knot Theory, and Statistical Mechanics II (World Scientific, Singapore, 1994).
- [82] M. Jimbo, Introduction to the Yang-Baxter equation, Int. J. Mod. Phys. A 4, 3759 (1989).

- [83] E. Fradkin, C. Nayak, A. Tsvelik, and F. Wilczek, A Chern-Simons effective field theory for the Pfaffian quantum Hall state, Nucl. Phys. B 516, 704 (1998).
- [84] K. Gawelenedzki and A. Kupiainen, SU(2) Chern-Simons theory at genus zero, Commun. Math. Phys. 135, 531 (1991).
- [85] C. Gils, E. Ardonne, S. Trebst, D. A. Huse, A. W. W. Ludwig, M. Troyer, and Z. Wang, Anyonic quantum spin chains: Spin-1 generalizations and topological stability, Phys. Rev. B 87, 235120 (2013).
- [86] S. Trebst, M. Troyer, Z. Wang, and A. W. W. Ludwig, A short introduction to Fibonacci anyon models, Prog. Theor. Phys. Supp. 176, 384 (2008).
- [87] C. Delaney, E. C. Rowell, and Z. Wang, Local unitary representations of the braid group and their applications to quantum computing, Rev. Colomb. Mat. 50, 211 (2016).
- [88] J. Fuchs, Affine Lie Algebras and Quantum Groups: An Introduction, with Applications in Conformal Field Theory (Cambridge University Press, Cambridge, 1995).
- [89] A. Kirillov and N. Y. Reshetikhin, in New Developments in the Theory of Knots (World Scientific, 1991), p. 202.
- [90] M. H. Freedman, M. Larsen, and Z. Wang, A modular functor which is universal for quantum computation, Commun. Math. Phys. 227, 605 (2002).
- [91] E. C. Rowell and Z. Wang, Mathematics of topological quantum computing, Bull. Am. Math. Soc. 55, 183 (2018).
- [92] A. Ahlbrecht, L. S. Georgiev, and R. F. Werner, Implementation of Clifford gates in the Ising-anyon topological quantum computer, Phys. Rev. A 79, 032311 (2009).
- [93] R. L. Roth, A history of Lagrange's theorem on groups, Math. Mag. 74, 99 (2001).

*Correction:* The Acknowledgments section was inadvertently removed during the production cycle and has been reinserted.