Protected gates for topological quantum field theories

Michael E. Beverland,[1] Oliver Buerschaper,[2] Robert Koenig,[3]
Fernando Pastawski,[1] John Preskill,[1] and Sumit Sijher[4]

[1]*Institute for Quantum Information and Matter, California Institute of Technology, Pasadena,
California 91125, USA*
[2]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin,
14195 Berlin, Germany*
[3]*Institute for Advanced Study and Zentrum Mathematik, Technische Universität München,
85748 Garching, Germany*
[4]*Institute for Quantum Computing and Department of Applied Mathematics,
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

We study restrictions on locality-preserving unitary logical gates for topological quantum codes in two spatial dimensions. A locality-preserving operation is one which maps local operators to local operators — for example, a constant-depth quantum circuit of geometrically local gates, or evolution for a constant time governed by a geometrically local bounded-strength Hamiltonian. Locality-preserving logical gates of topological codes are intrinsically fault tolerant because spatially localized errors remain localized, and hence sufficiently dilute errors remain correctable. By invoking general properties of two-dimensional topological field theories, we find that the locality-preserving logical gates are severely limited for codes which admit non-abelian anyons, in particular, there are no locality-preserving logical gates on the torus or the sphere with M punctures if the braiding of anyons is computationally universal. Furthermore, for Ising anyons on the M-punctured sphere, locality-preserving gates must be elements of the logical Pauli group. We derive these results by relating logical gates of a topological code to automorphisms of the Verlinde algebra of the corresponding anyon model, and by requiring the logical gates to be compatible with basis changes in the logical Hilbert space arising from local F-moves and the mapping class group. © *2016 AIP Publishing LLC.* [http://dx.doi.org/10.1063/1.4939783]

I. INTRODUCTION

In order to reliably compute, it is necessary to protect information against noise. For quantum computations, this is particularly challenging because noise in the form of decoherence threatens the very quantum nature of the process. Adding redundancy by encoding information into a quantum error-correcting code is a natural, conceptually appealing approach towards building noise-resilient scalable computers based on imperfect hardware.

Among the known quantum error-correcting codes, the class of the so-called topological codes stands out. Examples in 2D include the toric code and quantum double models,[27] the surface codes,[8] the 2D color codes,[4] variants of these codes,[3,17] and the Levin-Wen model.[32] In 3D, known examples are the 3D color code of Bombin and Martin-Delgado,[6] as well as the models of Haah[22] and Michnicki.[35] These codes are attractive for a number of reasons: their code space is topologically protected, meaning that small local deformations or locally acting noise does not affect encoded information. The degree of this protection (measured in information-theoretic notions in terms of code distance, and manifesting itself in physical properties such as gap stability) scales with the system size: in other words, robustness essentially reduces to the question of scalability. Finally, the code space of a topological code is the degenerate ground space of a geometrically local Hamiltonian: this means that syndrome information can be extracted by local measurements, an important feature for actual realizations. Furthermore, this implies that a topological code is essentially a

57, 022201-1

phase of a many-body system and can be characterized in terms of its particle content, their statistics, and the quantum field theory emerging in the continuum limit. In particular, the quantum field theory provides a description of such systems which captures all universal features, independently of microscopic details.

While quantum error-correcting codes can provide the necessary protection of information against noise, a further requirement for quantum computation is the ability to execute gates in a robust manner. Again, topological codes stand out: they usually provide certain intrinsic mechanisms for executing gates in a robust way. More precisely, there are sequences of local code deformations, under which the information stays encoded in a code with macroscopic distance, but undergoes some unitary transformation. In principle, this provides a robust implementation of computations by sequences of local, and hence, potentially experimentally realizable actions. In the case of 2D-topological codes described by topological quantum field theories (TQFTs), this corresponds to adiabatic movement (braiding) of quasi-particle excitations (also called anyons).

Unfortunately, as is well known, braiding (by which we mean the movement either around each other or more generally around non-trivial loops) of anyons does not always give rise to a universal gate set. Rather, the set of gates is model-dependent: braiding of $D(\mathbb{Z}_2)$-anyons generates only global phases on the sphere, and elements of the Pauli group on non-zero genus surfaces. Braiding of Ising anyons gives Clifford gates, whereas braiding of Fibonacci anyons generates a dense subgroup of the set of unitaries (and is, therefore, universal within suitable subspaces of the code space). In other words, braiding alone, without additional tricks such as magic state distillation[9] (which has a large overhead[16]), is not, in general, sufficient to provide universal fault-tolerant computation; unfortunately, the known systems with universal braiding behavior are of a rather complex nature, requiring, e.g., 12-body interactions among spins.[32] Even ignoring the question of universality, the use of braiding has some potential significant drawbacks: in general (for non-abelian anyons), it requires an amount of time which scales with the system size (or code distance) to execute a single logical gate. (Mathematically, this is reflected by the fact that string-operators cannot be implemented in constant depth for general non-abelian anyon models — in contrast to, e.g., the toric code.[44]) This implies that error-correction steps will be necessary even during the execution of such a gate (see, e.g., Refs. 38, 24, 12, and 11 for a recent discussion of the robustness of braiding). This may pose an additional technological challenge, for example, if the intermediate topologies are different.

Given the limitations of braiding, it is natural to look for other mechanisms for implementing robust gates in topological codes. For stabilizer quantum codes, the notion of transversal gates has traditionally been used almost synonymously with fault-tolerant gates: their key feature is the fact that they do not propagate physical errors. More generally, for topological stabilizer codes, we can consider logical gates implementable by constant-depth quantum circuits as a proxy for robust gates: they can increase the weight of a physical error only by a constant and are thus sufficiently robust when combined with suitable error-correction gadgets. Note that finite-depth local circuits represent a much broader class than transversal gates.

Gate restrictions on transversal as well as constant-depth local circuits have been obtained for stabilizer and more general codes. Eastin and Knill[14] argued that for any code protected against local errors, transversal gates can only generate a finite group and, therefore, do not provide universality. Bravyi and König[10] consider the group of logical gates that may be implemented by such constant-depth local circuits on geometrically local topological stabilizer codes. They found that such gates are contained in $\mathcal{P}_D$, the Dth level of the Clifford hierarchy, where D is the spatial dimension in which the stabilizer code is geometrically local.

In this work, we characterize the set of gates implementable by a locality-preserving unitary in a system described by a 2D TQFT. By doing so, we both specialize and generalize the results of Ref. 10: we restrict our attention to dimension 2, but go beyond the set of local stabilizer codes in two significant ways.

First, we obtain statements which are independent of the particular realization (e.g., the toric code model) but are instead phrased in terms of the TQFT (i.e., the anyon model describing the system). In this way, we obtain a characterization which holds for a gapped phase of matter, rather than just for a particular code representing that phase. On a conceptual level, this is similar in

spirit to the work of Ref. 15, where statements on the computational power for measurement-based quantum computation were obtained that hold throughout a certain phase. Here, we use the term phase loosely — we say that two systems are in the same phase if they have the same particle content. To avoid having to make any direct reference to an underlying lattice model, we replace the notion of a constant-depth local circuit by the more general notion of a locality-preserving unitary: this is a unitary operation which maps local operators to local ones.

Second, our results and techniques also apply to non-abelian anyon models (whereas stabilizer codes only realize certain abelian models, unless, e.g., domain walls or "twists" are added[3] that break homogeneity). In particular, we obtain statements that can be applied, e.g., to the Levin-Wen models,[32] as well as chiral phases. For such systems, restrictions on protected gates were previously not known. Again, knowledge of the underlying microscopic model is unnecessary to apply our results, which only depend on the type of anyons present in the system. Our approach relates locality-preserving unitaries to certain symmetries of the underlying anyon model; this imposes constraints on the allowed operations. We consider the Fibonacci and Ising models as paradigmatic examples and find that there are no non-trivial gates in the former, and only Pauli operations in the latter case. Our focus on these anyons models is for concreteness only, but our methods and conclusions apply more generally. Some of our more general conclusions are that

(i) protected gates generically (see Section IV E discussing the necessity of certain technical assumptions) form only a finite group and

(ii) when the representation of the mapping class group is computationally universal (i.e., forms a dense subgroup), then there are no non-trivial protected gates.

Our observations are summarized in Table I. According to our results, the class of locality-preserving unitaries (which is distinguished from the point of view of error correction) is too restricted and needs to be supplemented with alternative mechanisms to achieve universality.

Finally, let us comment on limitations, as well as open problems arising from our work. The first and most obvious one is the dimensionality of the systems under consideration: our methods apply only to $2D$ TQFTs. The mathematics of higher-dimensional TQFTs is less developed, and currently an active research area (see, e.g., Ref. 30). While the techniques of Ref. 10, which have recently been significantly strengthened by Pastawski and Yoshida,[37] also apply to higher-dimensional codes (such as Haah's), they are restricted to the stabilizer formalism (but importantly, Ref. 37 also obtain statements for subsystem codes). Obtaining non-abelian analogues of our results in higher dimensions appears to be a challenging research problem. A full characterization of the case $D = 3$ is particularly desirable from a technological viewpoint.

Even in $2D$, there are obvious limitations of our results: the systems we consider are essentially "homogeneous" lattices with anyonic excitations in the bulk. We are not considering defect lines, or condensation of anyons at boundaries, for example, our discussion excludes the quantum double models constructed in Ref. 2, which have domain walls constructed from condensation at boundaries using the folding trick. Again, we expect that obtaining statements on protected gates for these

TABLE I. We study different anyon models (first column). The second column describes the properties of the unitary group generated by the (projective) representation of the mapping class group (see Section II F) — this corresponds to braiding for punctured spheres. The third column characterizes the set of protected gates. Our results suggest a trade-off between the computational power of the mapping class group representation and that of gates implementable by locality-preserving unitaries.

Model	Mapping class group contained in	Locality-preserving unitaries contained in
$D(\mathbb{Z}_2)$	Pauli group	Restricted Clifford group
Abelian anyon model	Generalized Pauli group	Generalized Clifford group
Fibonacci model	Universal	Global phase (trivial)
General anyon model	Universal	Global phase (trivial)
Ising model	Clifford group	Pauli group
Generic anyon model	Model-dependent	Finite group

models requires additional technology in the form of more refined categorical notions, as discussed by Kitaev and Kong.[29] Also, although we identify possible locality preserving logical unitaries, our arguments do not show that these can necessarily be realized, either in general TQFTs or in specific models that realize TQFTs. Finally, our work is based on the (physically motivated) assumption that a TQFT description is possible and the underlying data are given. For a concrete lattice model of interacting spins, the problem of identifying this description (or associated invariants[26,33,23]), as well as constructing the relevant string-operators (as has been done for quantum double models[27,5] as well as the Levin-Wen models[32]), is a problem in its own right.

A. Rough statement of problem

Our results concern families of systems defined on any 2-dimensional orientable manifold (surface) Σ, which we will take to be closed unless otherwise stated. Typically, such a family is defined in terms of some local physical degrees of freedom (spins) associated with sites of a lattice embedded in Σ. We refer to the joint Hilbert space $\mathcal{H}_{\text{phys},\Sigma}$ of these spins as the "physical" Hilbert space. The Hamiltonian H_Σ on $\mathcal{H}_{\text{phys},\Sigma}$ is local, i.e., it consists only of interactions between "neighbors" within constant-diameter regions on the lattice. More generally, assuming a suitable metric on Σ is chosen, we may define locality in terms of the distance measure on Σ.

We are interested in the ground space $\mathcal{H}_\Sigma$ of H_Σ. For a topologically ordered system, this ground space is degenerate with dimension growing exponentially with the genus of Σ and is, therefore, suitable for storing and manipulating quantum information. We will give a detailed description of this space below (see Section II); it has a preferred basis consisting of labelings associated with some set $\mathbb{A}$. This is a finite set characterizing all distinct types of anyonic quasiparticle excitations of H_Σ in the relevant low energy sector of $\mathcal{H}_{\text{phys},\Sigma}$.

Importantly, the form of $\mathcal{H}_\Sigma$ is independent of the microscopic details (in the definition of H_Σ): it is fully determined by the associated TQFT. In mathematical terms, it can be described in terms of the data of a modular tensor category, which also describes fusion, braiding, and twists of the anyons. We will refer to $\mathcal{H}_\Sigma$ as the TQFT Hilbert space.

The significance of $\mathcal{H}_\Sigma$ is that it is protected: local observables cannot distinguish between states belonging to $\mathcal{H}_\Sigma$. This implies that $\mathcal{H}_\Sigma$ is an error-correcting code with the property that local regions are correctable: any operator supported in a small region which preserves the code space must act trivially on it (otherwise it could be used to distinguish between ground states).

To compute fault-tolerantly, one would like to operate on information encoded in the code space $\mathcal{H}_\Sigma$ by acting with a unitary $U : \mathcal{H}_{\text{phys},\Sigma} \to \mathcal{H}_{\text{phys},\Sigma}$ on the physical degrees of freedom.[45] There are a number of features that are desirable for such a unitary to be useful — physical realizability being an obvious one. For fault-tolerance, two conditions are particularly natural:

(i) The unitary U should preserve the code space, $U\mathcal{H}_\Sigma = \mathcal{H}_\Sigma$, so that the information stays encoded. We call a unitary U with this property an automorphism of the code and denote its restriction to $\mathcal{H}_\Sigma$ by $[U] : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$. The action $[U]$ defines the logical operation or gate that U realizes.

(ii) Typical errors should remain correctable under the application of the unitary U. In the context of topological codes, which correct sufficiently local errors, and where a local error model is usually assumed, this condition is satisfied if U does not significantly change the locality properties of an operator: if an operator X has support on a region $\mathcal{R} \subset \Sigma$, then the support of $UXU^\dagger$ is contained within a constant-size neighborhood of $\mathcal{R}$. We call such a unitary a locality-preserving unitary.

We call a unitary U satisfying (i) and (ii) a locality-preserving unitary automorphism of the code (or simply a topologically protected gate). Our goal is to characterize the set of logical operations that have the form $[U]$ for some locality-preserving[46] unitary automorphism U. For example, if $\mathcal{H}_\Sigma$ is a topologically ordered subspace of $\mathcal{H}_{\text{phys},\Sigma}$, the Hilbert space of a spin lattice, then (ii) is satisfied if U is a constant-depth local circuit. Another important example is the constant-time evolution $U = \mathcal{T} \exp[-i \int dt H(t)]$ of a system through a bounded-strength geometrically local Hamiltonian $H(t)$. Here, Lieb-Robinson bounds[34,7] provide quantitative statements on how the resulting unitary

may be exponentially well approximated by a locality-preserving unitary. This is relevant since it describes the time evolution of a physical system and can also be used to model adiabatic transformations of the Hamiltonian.[13]

From a computational point of view, the group

$$\langle \{ [U] \mid U \text{ locality-preserving unitary automorphism} \} \rangle$$

generated by such gates is of particular interest: it determines the computational power of gates that are implementable fault-tolerantly with locality preserving automorphisms.

B. Outline

In Section II, we provide a brief introduction to the relevant concepts of TQFTs. We then derive our main results on the characterization of protected gates in Section III. Further restrictions on the allowed protected gates are provided in Sections IV and V. In Section VI, we apply our results to particular models, deriving, in particular, our characterizations for Ising and Fibonacci anyons. Finally, in Section VII, we use additional properties of abelian models to show that their protected gates must be contained within a proper subgroup of the generalized Clifford group, which is similar to the result of Ref. 10, but goes further.

II. TQFTs: BACKGROUND

In this section, we provide the necessary background on TQFTs. Our discussion will be rather brief; for a more detailed discussion of topological quantum computation and anyons, we refer to Ref. 39. Following Witten's work,[43] TQFTs have been axiomatized by Atiyah[1] based on Segal's work[40] on conformal field theories. Moore and Seiberg[36] derived the relations satisfied by the basic algebraic data of such theories (or more precisely, a modular functor). Here, we borrow some of the terminologies developed in full generality by Walker[25] (see also Ref. 19). For a thorough treatment of the category-theoretic concepts, we recommend the Appendix of Ref. 28.

Our focus is on the Hilbert space $\mathcal{H}_\Sigma$ spanned by the vacuum states of a TQFT defined on the orientable surface Σ. Recall that this is generally a subspace $\mathcal{H}_\Sigma \subset \mathcal{H}_{\text{phys},\Sigma}$ of a Hilbert space of physical degrees of freedom. The TQFT is specified by a finite set of anyon labels $\mathbb{A} = \{1, a, b, c, \ldots\}$, their *fusion rules* (described using a non-negative integer N_{ab}^c for each triple of anyons a, b, c, called fusion multiplicities), along with S, F, R, and T matrices (complex valued matrices with columns and rows indexed by anyon labels). If the TQFT arises from taking continuous limits of a local Hamiltonian model such as the toric code, the anyons are simply the elementary excitations of the model, and the fusion rules and matrices can be understood in terms of creating, combining, moving, and annihilating anyons in the surface. The anyon set must contain a trivial particle $1 \in \mathbb{A}$ such that when combined with any particle, the latter remains unchanged $N_{a1}^c = N_{1a}^c = \delta_a^c$, and each particle $a \in \mathbb{A}$ must have an antiparticle $\overline{a} \in \mathbb{A}$ such that $N_{a\overline{a}}^1 \neq 0$. We will restrict our attention to models where $N_{ab}^c \in \{0, 1\}$ for all $a, b, c \in \mathbb{A}$ for simplicity (our results generalize with only minor modifications).

A. String-like operators and relations

We are interested in the algebra $\mathcal{A}_\Sigma$ of operators $X : \mathcal{H}_{\text{phys},\Sigma} \to \mathcal{H}_{\text{phys},\Sigma}$ which preserve the subspace $\mathcal{H}_\Sigma$. We call such an element $X \in \mathcal{A}_\Sigma$ an automorphism and denote by $[X] : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$ the restriction to $\mathcal{H}_\Sigma$. We call X a representative (or realization) of $[X]$. Operators of the form $[X]$, where $X \in \mathcal{A}_\Sigma$, define an associative $*$-algebra $[\mathcal{A}_\Sigma]$ with unit and multiplication $[X][Y] = [XY]$. The unit element in $[\mathcal{A}_\Sigma]$ is represented by the identity operator id on the whole space $\mathcal{H}_{\text{phys},\Sigma}$.

Our constraints on protected gates are derived by studying how they transform certain operators acting on $\mathcal{H}_{\text{phys},\Sigma}$ (see Fig. 1). To define the latter, fix a simple closed curve $C : [0,1] \to \Sigma$ on the surface and an "anyon label" $a \in \mathbb{A}$. (The set of labels $\mathbb{A}$ is determined by the underlying model.) Then, there is a "string-operator" $F_a(C)$ acting on $\mathcal{H}_{\text{phys},\Sigma}$, supported in a constant-diameter neighborhood of C. It corresponds to the process of creating a particle-antiparticle-pair $(a, \overline{a})$, moving a
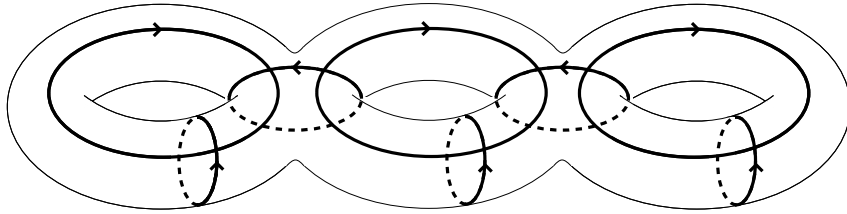
FIG. 1. Closed 2-manifolds are characterized by their genus g. The figure illustrates the 3-handled torus Σ_g corresponding to $g = 3$. A canonical set of $3g - 1$ generators of the mapping class group of the surface Σ_g can be specified in terms of a set $\mathcal{G} = \{C_j\}_{j=1}^{3g-1}$ of loops (each associated with a Dehn twist). Dragging an anyon a around such loop $C : [0, 1] \to \Sigma_g$ and fusing to the vacuum implements an undetectable operator $F_a(C)$; homologically non-trivial loops realize logical operations. The full algebra of logical operators is generated by the set of operators $\{F_a(C)\}_{a\in\mathbb{A}, C\in\mathcal{G}}$. However, these operators are generally not independent.

along C, and subsequently fusing to the vacuum. The last step in this process involves projection onto the ground space, which is not trivial in general: the operator $F_a(C)$ can involve post-selection, in which case it is a non-unitary element of $\mathcal{A}_\Sigma$.

The operators $\{F_a(C)\}_{a\in\mathbb{A}}$ form a closed subalgebra $\mathcal{A}(C) \subset \mathcal{A}_\Sigma$: they preserve the ground space and satisfy

$$F_a(C)F_b(C) = \sum_n N_{ab}^n F_n(C)\,, \qquad\qquad F_a(C)^\dagger = F_{\overline{a}}(C), \qquad \text{and} \qquad F_1(C) = \mathsf{id}_{\mathcal{H}_{\text{phys}}} \qquad (1)$$

for the fusion multiplicities N_{ab}^n (see Section II B). In addition, reversing the direction of C, i.e., considering $C^{-1}(t) \equiv C(1 - t)$, is equivalent to exchanging the particle with its antiparticle, i.e.,

$$F_a(C^{-1}) = F_{\overline{a}}(C)\,. \qquad (2)$$

Here, $a \mapsto \overline{a}$ is an involution on the set of particle labels $\mathbb{A}$, again defined by the underlying model. Properties (1) and (2) of the string-operators can be shown in the diagrammatic formalism mentioned below (but this is not needed here; we will use them as axioms).

We denote the restriction of $F_a(C)$ to the code space $\mathcal{H}_\Sigma$ by $[F_a(C)]$. Note that, while $[F_a(C)]$ is unitary in abelian anyon models, this is not the case in general.

Example 2.1 (D(G) and Kitaev's toric code). As an example, consider a model described by the quantum double $D(G)$ of a finite group G, for which Kitaev has constructed a lattice model.[27] In the case where G is abelian, we have $D(G) \cong G \times G$, i.e., the particles and fusion rules are simply given by the product group $\mathbb{A} = G \times G$.

Specializing to $G = \mathbb{Z}_2$ gives the particles commonly denoted by $1 = (0,0)$ (vacuum), $m = (1,0)$, $e = (0,1)$, and $\epsilon = m \times e = (1,1)$. For the toric code model, the associated ribbon operators are

$$F_1(C) = \mathsf{id}, \quad F_e(C) = \bar{X}(C), \quad F_m(C) = \bar{Z}(C), \quad F_\epsilon(C) = \bar{X}(C)\bar{Z}(C)\,,$$

where $\bar{X}(C) = \otimes_{j\in\partial_+ C} X_j$ and $\bar{Z}(C) = \otimes_{j\in\partial_- C} Z_j$ are appropriate tensor products of Pauli-X and Pauli-Z-operators along C (as specified in Ref. 27).

Specializing to $G = \mathbb{Z}_N$, with $\omega_N = \exp(2\pi i/N)$ and generalized N-dit Pauli operators X and Z (and their inverses), defined by their action

$$X|j\rangle = |j + 1 \bmod N\rangle \qquad Z|j\rangle = \omega_N^j |j\rangle$$

on computational basis states $\{|j\rangle\}_{j=0,\ldots,N-1}$, we can consider such a model (the $\mathbb{Z}_N$-toric code) with generalized ribbon operators. Here,

$$F_{(a,a')}(C) = \bar{X}(C)^a \bar{Z}(C)^{a'}\,,$$

where $\bar{X}(C)$ is a tensor product of Pauli-X and its inverse depending on the orientation of the underlying lattice, and similarly for $\bar{Z}(C)$.

It is easy to check that operators associated with the same loop commute, i.e.,

$$[F_{(a,a')}(C), F_{(b,b')}(C)] = 0 , \tag{3}$$

and since $Z^a X^b = \omega_N^{ab} X^b Z^a$, we get the commutation relation

$$F_{(a,a')}(C_1) F_{(b,b')}(C_2) = \omega_N^{ab'-a'b} F_{(b,b')}(C_2) F_{(a,a')}(C_1) \tag{4}$$

for any two strings C_1, C_2 intersecting once.

Returning to the general case, the algebra of string operators does not necessarily satisfy relations as simple as (3) and (4). Nevertheless, some essential features hold under very general assumptions. We express these as postulates; they can be seen as a subset of the isotopy-invariant calculus of labeled ribbon graphs associated with the underlying category (see, e.g., Ref. 18 for a discussion of the latter). That is, the properties expressed by our postulates are a subset of the axioms formalizing TQFTs and serve to capture the essential features in an algebraic manner. For particular systems (such as the toric code or the quantum double models), these postulates can be rigorously established (see Refs. 27 and 5), whereas in other cases, only partial results are known (see, e.g., the discussion in Ref. 42 (p. 107)) but they are conjectured to hold. We sidestep the independent important and challenging problem of rigorously establishing these postulates, and instead derive some consequences. Throughout our work, we hence assume that the models under consideration satisfy our postulates.

Postulate 2.2 (Completeness of string-operators). Consider an operator U with support in some region $\mathcal{R}$ which preserves the code space $\mathcal{H}_\Sigma$. Then, its action on the code space is equivalent to that of a linear combination of products of operators of the form $F_a(C)$, for a closed loop $C : [0,1] \to \mathcal{R}$ which is supported in $\mathcal{R}$. That is, we have

$$[U] = \sum_j \beta_j \prod_k [F_{a_{j,k}}(C_{j,k})] .$$

This postulate essentially means that, as far as the logical action is concerned, we may think of $[U]$ as a linear combination of products of closed-loop string operators. Such products $F_{a_m}(C_m) \cdots F_{a_1}(C_1)$ can conveniently be thought of as "labeled" loop gases embedded in the three-manifold $\Sigma \times [0,1]$, where, for some $0 < t_1 < \cdots < t_m < 1$, the operator $F_{a_j}(C_j)$ is applied at "time" t_j (and hence a labeled loop is embedded in the slice $\Sigma \times \{t_j\}$). Diagrammatically, one represents such a product by the projection onto Σ with crossings representing temporal order, as in

$$F_{a_2}(C_2) F_{a_1}(C_1) = \quad\underset{\displaystyle F_{a_2}(C_2) \qquad\qquad F_{a_1}(C_1)}{\text{}} . \tag{5}$$

One may manipulate every term in a linear combination representing U without changing the logical action according to certain local "moves," in particular, the order of application of these moves is irrelevant (a fact formalized by MacLane's theorem[31]).

For our purposes, we only require the following "local" moves, which relate two products U and U' of string-operators given by diagrams such as (5). More generally, they may be applied term-by-term to any linear combination if each term contains the same local sub-diagram.

Postulate 2.3 (String deformation (see Fig. 2)). Suppose operators $U, U' \in \mathcal{A}_\Sigma$ are identical on the complement of some region $\mathcal{R}$. Assume further that inside $\mathcal{R}$, both U and U' contain a single string describing the dragging of the same anyon type along a path C and C', respectively, where C' can be locally deformed into C. Then the logical action of U and U' must be equivalent: $[U] = e^{i\theta}[U']$ for some unimportant phase $e^{i\theta}$.

In particular, this postulate implies that if C and C' are two closed homologically equivalent loops and a is an arbitrary anyon label, then the operators $F_{a(C)}$ and $F_a(C')$ realized by "dragging"
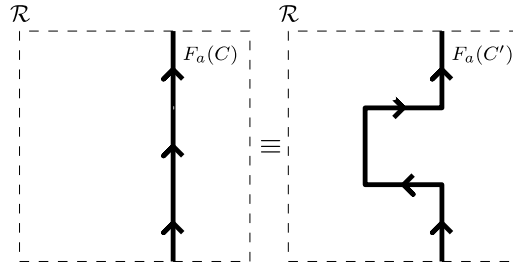
FIG. 2. The content of Postulate 2.3: We can deform a line without changing the logical action of the string-operator.

the specified anyon along C and C', respectively, have equivalent logical action on the code space, $[F_a(C)] = e^{i\theta}[F_a(C')]$.

The next postulate involves local operators, and essentially states that the space $\mathcal{H}_\Sigma$ is a quantum error-correcting code protecting against local errors. While we may state it in a form only referring to local operators, we will find it more intuitive to combine it with the deformation postulate: this extends correctability from small regions to contractible loops (i.e., loops that are homotopic to a point).

Postulate 2.4 (Error correction postulate). If C is a contractible loop, then for each $a \in \mathbb{A}$, the operator $F_a(C)$ has trivial action on the space $\mathcal{H}_\Sigma$ up to a global constant d_a, that is,

$$[F_a(C)] = d_a \mathsf{id}_{\mathcal{H}_\Sigma} . \tag{6}$$

This postulate essentially means that we may remove certain closed loops from diagrams such as (5).

An immediate consequence of these postulates is the following statement.

Proposition 2.1 (Local completeness of string operators). Consider an operator $O \in \mathcal{A}_\Sigma$ whose support is contained within a constant-diameter neighborhood of a simple loop C. Then $[O] = [\tilde{X}]$ for some $\tilde{X} \in \mathcal{A}(C)$. In other words, the logical action of O is identical to that of a linear combination of string-operators $F_a(C)$.

This proposition can be seen as a consequence of the completeness condition for strings (Postulate 2.2), the string deformation Postulate 2.3 and (1). A similar argument leads us to the following conclusion.

Proposition 2.2 (Global completeness of few homology classes). The full logical algebra $[\mathcal{A}_\Sigma]$ is generated by the logical algebras $[\mathcal{A}(C)]$ associated with a finite number of inequivalent non-contractible simple loops C.

Proof. That the algebra $[\mathcal{A}_\Sigma]$ is finite-dimensional can be seen from the finite dimensionality of the code space $\mathcal{H}_\Sigma$. By Postulate 2.2, the algebra $[\mathcal{A}_\Sigma]$ is generated by $\{\mathcal{A}(C)\}_C$. Let us start from a trivial algebra and build up $[\mathcal{A}_\Sigma]$ from a finite number of loops. As long as the algebra is not complete, we may include additional loops C such that $[\mathcal{A}(C)]$ is not included in the partially generated algebra. Such a loop C must be inequivalent to the previously included loops due to Postulate 2.3. After a number of steps no greater than the square of the ground space dimension, we will have constructed the complete algebra.   □

Therefore, there exists a finite, *minimal* set of loops which is sufficient to span $[\mathcal{A}_\Sigma]$.

B. The Verlinde algebra

It is convenient to formally introduce some algebraic data defined by the underlying anyon model. We will return to the discussion of string-operators in Sec. II C and relate them to this algebraic language.

As before, let $\mathbb{A}$ be the set of particle labels (generally a finite set), and let $a \mapsto \overline{a}$ be the involution giving the antiparticle associated with particle a. The *fusion rules* of the model are encoded in integers N_{ab}^c, which are called fusion multiplicities. We will restrict our attention to models where $N_{ab}^c \in \{0,1\}$ for all $a,b,c \in \mathbb{A}$ for simplicity (our results generalize with only minor modifications).

The *Verlinde algebra* Ver is the commutative associative $*$-algebra spanned by elements $\{\mathbf{f}_a\}_{a \in \mathbb{A}}$ satisfying the relations

$$\mathbf{f}_a \mathbf{f}_b = \sum_c N_{ab}^c \mathbf{f}_c \qquad \text{and} \qquad \mathbf{f}_a^\dagger = \mathbf{f}_{\overline{a}} \, . \tag{7}$$

Note that $\mathbf{f}_1 = \mathrm{id}$ is the identity element because the numbers $\{N_{ab}^c\}$ satisfy $N_{a1}^c = N_{1a}^c = \delta_{ac}$.

Since every anyon model is braided by definition, one indeed has $N_{ab}^c = N_{ba}^c$ and the algebra Ver is a finite-dimensional commutative C^*-algebra. Therefore, $\mathsf{Ver} \cong \mathbb{C}^{\oplus(\dim \mathsf{Ver})}$ is a direct sum of copies of $\mathbb{C}$. The fusion multiplicity N_{ab}^c may also be written in terms of the modular S-matrix, whose matrix elements are, in the diagrammatic calculus, given by the Hopf link and the total quantum dimension $\mathcal{D}$ by

$$S_{ab} = \tfrac{1}{\mathcal{D}} \, a \left(\!\!\bigcirc\!\!\bigcirc\!\!\right) b \, .$$

We consider (and restrict our attention to) the case where the S-matrix is unitary: here the isomorphism $\mathsf{Ver} \cong \mathbb{C}^{\oplus(\dim \mathsf{Ver})}$ can be made explicit, thanks to the *Verlinde formula*[41]

$$N_{ab}^c = \sum_x \frac{S_{ax} S_{bx} S_{\overline{c}x}}{S_{1x}} \, , \tag{8}$$

as the proof of the following Proposition 2.3 shows. (Note that $S_{1x} = d_x/\mathcal{D}$ where $\mathcal{D} = \sqrt{\sum_a d_a^2}$.) For this purpose, we define the elements

$$\mathbf{p}_a = S_{1a} \sum_b \overline{S_{ba}} \mathbf{f}_b \qquad \text{for all } a \in \mathbb{A} \, . \tag{9}$$

This relation can be inverted by making use of unitarity of the S-matrix,

$$\mathbf{f}_b = \sum_a \frac{S_{ba}}{S_{1a}} \mathbf{p}_a \qquad \text{for all } a \in \mathbb{A} \, . \tag{10}$$

The main statement we use is the following:

Proposition 2.3 (Primitive idempotents). The elements $\{\mathbf{p}_a\}_{a \in \mathbb{A}}$ are the unique complete set of orthogonal minimal idempotents spanning the Verlinde algebra,

$$\mathsf{Ver} = \bigoplus_a \mathbb{C} \mathbf{p}_a \, . \tag{11}$$

Furthermore, they satisfy

$$\sum_a \mathbf{p}_a = \mathbf{f}_1 = \mathrm{id} \, . \tag{12}$$

Proof. That $\{\mathbf{p}_a\}_{a \in \mathbb{A}}$ span the algebra Ver is evident from the fact that $\{\mathbf{f}_a\}_{a \in \mathbb{A}}$ span the algebra, and each $\mathbf{f}_a$ can be written in terms of $\{\mathbf{p}_a\}_{a \in \mathbb{A}}$ via Eq. (10). To show they are orthogonal idempotents $\mathbf{p}_a \mathbf{p}_b = \delta_{a,b} \mathbf{p}_a$, first note that

$$\begin{aligned}
\mathbf{p}_a \mathbf{p}_b &= S_{1a} S_{1b} \sum_{g,h} \overline{S_{ga} S_{hb}} \mathbf{f}_g \mathbf{f}_h \\
&= S_{1a} S_{1b} \sum_{g,h,j} \overline{S_{ga} S_{hb}} N_{gh}^j \mathbf{f}_j \\
&= S_{1a} S_{1b} \sum_{g,h,j,x} \overline{S_{ga} S_{hb}} \frac{S_{gx} S_{hx} S_{\overline{j}x}}{S_{1x}} \mathbf{f}_j,
\end{aligned}$$

where we used Verlinde formula (8) in the second step. With the unitarity of the *S*-matrix, we then obtain

$$\mathbf{p}_a\mathbf{p}_b = S_{1a}S_{1b}\sum_{j,x}\delta_{a,x}\delta_{b,x}\frac{S_{\bar{j}x}}{S_{1x}}\mathbf{f}_j$$

$$= \delta_{a,b}S_{1a}^2\sum_j\frac{S_{\bar{j}a}}{S_{1a}}\mathbf{f}_j$$

$$= \delta_{a,b}S_{1a}\sum_j S_{\bar{j}a}\mathbf{f}_j .$$

It follows that $\mathbf{p}_a\mathbf{p}_b = \delta_{a,b}\mathbf{p}_a$ from the symmetry property $S_{\bar{j}a} = \overline{S_{ja}}$, see, e.g., Ref. 28 [Eq. (224)]. It remains to verify that the set of projectors is unique. Consider $\mathbf{q}_b = \sum_a \alpha_{ba}\mathbf{p}_a$ for some constants $\alpha_{ba} \in \mathbb{C}$, such that $\mathbf{q}_a\mathbf{q}_b = \delta_{a,b}\mathbf{q}_a$. This implies

$$\mathbf{q}_a\mathbf{q}_b = \sum_{dc}\alpha_{ac}\alpha_{bd}\mathbf{p}_c\mathbf{p}_d$$

$$= \sum_c\alpha_{ac}\alpha_{bc}\mathbf{p}_c = \delta_{a,b}\sum_c\alpha_{ac}\mathbf{p}_c,$$

which implies $\alpha_{ac}\alpha_{bc} = \delta_{a,b}\alpha_{ac}$ for all $a,c \in \mathbb{A}$ by linear independence of the $\mathbf{p}_a$'s. This implies $\alpha_{ac} = 0, 1$, and can only form a complete basis for the algebra Ver if α_{ac} is a permutation matrix, implying $\{\mathbf{q}_a\}_{a\in\mathbb{A}} \equiv \{\mathbf{p}_a\}_{a\in\mathbb{A}}$. □

As explained in Sec. II C, the string operators of anyons around a loop *C* give rise to a representation of the Verlinde algebra. While the projections (introduced in Eq. (14)) associated with the idempotents are not a basis for the logical algebra $[\mathcal{A}_\Sigma]$, they are a basis of a subalgebra $[\mathcal{A}_\Sigma(C)]$ isomorphic to the Verlinde algebra. This algebra must be respected by the locality-preserving unitaries, and this is best understood in terms of the idempotents. This is the origin of the non-trivial constraints we obtain on the realizable logical operators.

C. Bases of the Hilbert space $\mathcal{H}_\Sigma$

Eq. (1) shows that the collection of operators $\{[F_a(C)]\}_{a\in\mathbb{A}}$ form a representation of the Verlinde (fusion) algebra Ver. By linear independence of operators $\{[F_a(C)]\}_{a\in\mathbb{A}}$, we see that the representation is faithful, such that the logical loop algebra is isomorphic to the Verlinde algebra

$$[\mathcal{A}(C)] \cong \text{Ver}. \tag{13}$$

This will be central in the following development. Considering primitive idempotents (9), it is natural to consider the corresponding operators in this representation, that is, we set

$$[P_a(C)] = S_{1a}\sum_b \overline{S_{ba}}[F_b(C)] . \tag{14}$$

Since the set $\{[F_a(C)]\}_{a\in\mathbb{A}}$ forms a representation of the Verlinde algebra, the $\{[P_a(C)]\}_{a\in\mathbb{A}}$ are orthogonal projectors as a consequence of Proposition 2.3. The inverse relation to (14) is given by

$$[F_b(C)] = \sum_a \frac{S_{ba}}{S_{1a}}[P_a(C)] . \tag{15}$$

While the projectors $[P_a(C)]$ associated with a loop do not span the full logical algebra, they do span the local logical algebra of operators supported along *C* which must be respected by locality preserving unitaries. Intuitively, $\{P_a(C)\}_{a\in\mathbb{A}}$ are projectors onto the smallest possible sectors of the Hilbert space which can be distinguished by a measurement supported on *C*.

A state in the image of $P_a(C)$ has the interpretation of carrying flux *a* through the loop *C*. In particular, since the code space $\mathcal{H}_\Sigma$ corresponds to the vacua of a TQFT, there are no anyons present on Σ; however, there can be flux associated to non-contractible loops. We can use the operators $\{P_a(C)\}_{a,C}$ to define bases of the Hilbert space $\mathcal{H}_\Sigma$.

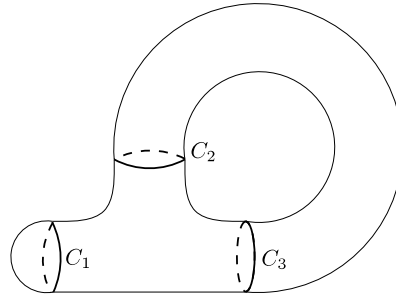Let us first define the Hilbert space $\mathcal{H}_\Sigma$ in more detail.

FIG. 3. A simple DAP decomposition of a torus utilizing a disc enclosed by C_1, an annulus enclosed by $\{C_2, C_3\}$, and a pair of pants enclosed by $\{C_1, C_2, C_3\}$. This decomposition is not minimal in that the same manifold could have been decomposed using a single loop.

Definition 2.5 (DAP-decomposition). Consider a minimal collection $C = \{C_j \mid C_j : [0,1] \to \Sigma\}_j$ of pairwise non-intersecting non-contractible loops, which cut the surface Σ into a collection of surfaces homeomorphic to discs, annuli, and pants. We call C a DAP-decomposition (see e.g., Fig. 3).

A *labeling* $\ell \colon C \mapsto \mathbb{A}$ is an assignment of an anyon label $\ell(C)$ to every loop $C \in C$ of a DAP decomposition. We call ℓ fusion-consistent if it satisfies the following conditions:

  (i)   For every loop $C \in C$ enclosing a disc on Σ, $\ell(C) = 1$, the vacuum label of the anyon model.
 (ii)   For every pair of loops $\{C_2, C_3\} \subset C$ defining an annulus in Σ, $\ell(C_2) = \overline{\ell(C_3)}$ assuming the loops are oriented such that the annulus is found to the left.
(iii)   For every triple $\{C_1, C_2, C_3\} \subset C$ defining a pair of pants in Σ, the labeling ℓ satisfies the fusion rule

$$N_{\ell(C_1),\ell(C_2)}^{\overline{\ell(C_3)}} \neq 0,$$

where the loops are oriented such that the pair of pants is found to the left.

Here, we may assume $\ell(C^{-1}) = \overline{\ell(C)}$, where C^{-1} denotes the loop coinciding with C but with opposite orientation.

Now fix any DAP-decomposition C of Σ and let $\mathsf{L}(C) \subset \mathbb{A}^{|C|}$ be the set of fusion-consistent labelings. The Hilbert space $\mathcal{H}_\Sigma$ is the formal span of elements of $\mathsf{L}(C)$,

$$\mathcal{H}_\Sigma := \sum_{\ell \in \mathsf{L}(C)} \mathbb{C}\ell = \sum_{\ell \in \mathsf{L}(C)} \mathbb{C}|\ell\rangle.$$

Any fusion-consistent labeling $\ell \in \mathsf{L}(C)$ defines an element $|\ell\rangle \in \mathcal{H}_\Sigma$ such that the vectors $\{|\ell\rangle\}_{\ell \in \mathsf{L}(C)}$ are an orthonormal basis (which we call $\mathcal{B}_C$) of $\mathcal{H}_\Sigma$, and this defines the inner product.

It is important to remark that this construction of $\mathcal{H}_\Sigma$ is independent of the DAP-decomposition C of Σ in the following sense: if C and C' are two distinct DAP-decompositions, then there is a unitary basis change between the bases $\mathcal{B}_C$ and $\mathcal{B}_{C'}$. In most cases under consideration, this basis change can be obtained as a product of unitaries associated with local "moves" connecting two DAP decompositions C and C'. One such basis change is associated with a four-punctured sphere (the
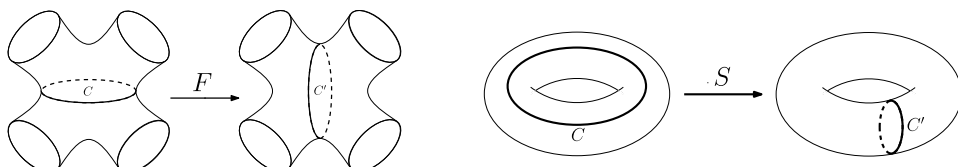

FIG. 4. Two DAP-decompositions $C = \{C\}$ and $C' = \{C'\}$ of either the 4-punctured sphere (left), or the torus (right), are related by an F-move or an S-move, respectively.

F-move), and specified by the unitary F-matrix in Fig. 4. Another matrix of this kind, the S-matrix (which also arose in our discussion of the Verlinde algebra), connects the two bases $\mathcal{B}_C$ and $\mathcal{B}_{C'}$ of $\mathcal{H}_{\text{torus}}$ associated with the first and second non-trivial cycles on the torus (Fig. 4). In this case, writing $\mathcal{B}_C = \{|a\rangle_C\}_a$ and $\mathcal{B}_{C'} = \{|a\rangle_{C'}\}_a$ since each basis element $|\ell\rangle$ is specified by a single label $\ell(C), \ell(C') \in \mathbb{A}$, we have the relation

$$|a\rangle_{C'} = \sum_b S_{ba} |b\rangle_C \,. \tag{16}$$

Other unitary basis changes arise from the representation of the mapping class group, as discussed in Section II F. All these basis changes constitute the second ingredient for the non-trivial constraints we obtain on the realizable logical operators.

A basis element $|\ell\rangle \in \mathcal{B}_C$ associates the anyon label $\ell(C)$ with each curve $C \in \mathcal{C}$. The vector $|\ell\rangle$ is the (up to a phase) unique simultaneous +1-eigenvector of all the projections $\{P_{\ell(C)}\}_{C \in \mathcal{C}}$. It is also a simultaneous eigenvector with respect to Dehn-twists along each curve $C \in \mathcal{C}$ with eigenvalue $e^{i\theta_{\ell(C)}}$. The action of Dehn-twists along curves C' not belonging to $\mathcal{C}$ can be obtained by applying the local moves to change into a basis $\mathcal{B}_{C'}$ associated with a DAP-decomposition C' containing C'.

D. Open surfaces: Labeled boundaries

So far, we have been discussing the Hilbert space $\mathcal{H}_\Sigma$ associated with closed surfaces; this does not cover the physically important case of pinned localized excitations (which correspond to punctures/holes in the surface). Here, we describe the modifications necessary to deal with surfaces with boundaries. We assume that the boundary $\partial\Sigma = \bigcup_{\alpha=1}^M \hat{C}_\alpha$ is the disjoint union of M simple closed curves, and assume that an orientation $\hat{C}_\alpha : [0,1] \to \partial\Sigma$ has been chosen for each boundary component $\hat{C}_\alpha$ such that Σ is found to the left. In addition, we fix a label $a_\alpha \in \mathbb{A}$ for every boundary component $\hat{C}_\alpha$. We call this a labeling of the boundary. Let us write $\Sigma(a_1, \ldots, a_M)$ for the resulting object (i.e., the surfaces, its oriented boundary components, and the associated labels). We call $\Sigma(a_1, \ldots, a_M)$ a surface with labeled boundary components; slightly abusing notation, we sometimes write $\Sigma = \Sigma(a_1, \ldots, a_M)$ when the presence of boundaries is understood/immaterial.

A TQFT associates to every surface $\Sigma(a_1, \ldots, a_M)$ with labeled boundary components a Hilbert space $\mathcal{H}_{\Sigma(a_1, \ldots, a_M)}$. The construction is analogous to the case of closed surfaces and based on DAP-decompositions. The only modification compared to the case of closed surfaces is that only DAP-decompositions including the curves $\{\hat{C}_\alpha\}_{\alpha=1}^M$ are allowed; furthermore, the labeling on these boundary components is fixed by $\{a_\alpha\}_{\alpha=1}^M$. That is, "valid" DAP-decompositions are of the form $C = \{C_1, \ldots, C_N, \hat{C}_1, \ldots, \hat{C}_M\}$ with curves $\{C_j\}_{j=1}^N$ "complementing" the boundary components, and valid labelings are fusion-consistent, i.e., $\ell \in \mathsf{L}(C)$ with the additional condition that they agree with the boundary labels, $\ell(\hat{C}_\alpha) = a_\alpha$ for $\alpha = 1, \ldots, M$. To simplify the discussion, we will often omit the boundary components $\{\hat{C}_\alpha\}_\alpha$ and focus on the remaining degrees of freedom associated with the curves $\{C_j\}_j$. It is understood that boundary labelings have to be fusion-consistent with the labeling $\{a_\alpha\}_\alpha$ of the boundary under consideration.

As a final remark, note that boundary components labeled with the trivial particle $1 \in \mathbb{A}$ correspond to contractible loops in a surface without this boundary (i.e., obtained by "gluing in a disc"). This means that they can be omitted: we have the isomorphism

$$\mathcal{H}_{\Sigma(1)} \cong \mathcal{H}_{\Sigma'} \,,$$

where Σ' is the surface with one boundary component less that of Σ.

1. Example: The M-anyon Hilbert space

A typical example we are interested in is the labeled surface

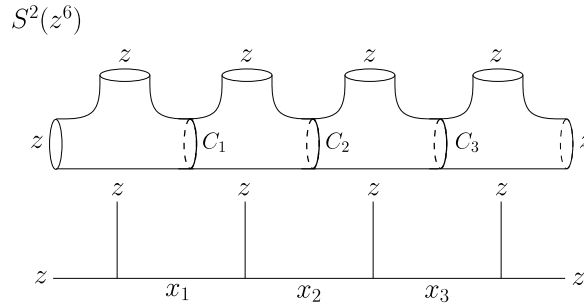$$S^2(z^M) = S^2(\underbrace{z, \ldots, z}_{M \text{ times}}) \,,$$

FIG. 5. The "standard" DAP-decomposition of the 6-punctured sphere, and the corresponding fusion-tree notation representing the labeling which assigns $\ell(C_i) = x_i$.

where $S^2(\ ,\ ,\ \ldots,\ ,\ )$ is the punctured sphere, and $z \in \mathbb{A}$ is some fixed anyon type (we assume that each boundary component has the same orientation). The Hilbert space $\mathcal{H}_{S^2(z^M)}$ is the space of M anyons of type z. When $M = N + 3$ for some $N \in \mathbb{N}$, we can choose a "standard" DAP-decomposition $C = \{C_j\}_{j=1}^{N}$ as shown in Fig. 5. A fusion-consistent labeling ℓ of the standard DAP-decomposition C corresponds to a sequence $(x_1, \ldots, x_N) = (\ell(C_1), \ldots, \ell(C_N))$ such that

$$N_{zz}^{x_1} = N_{x_N z}^{\overline{z}} = 1 \qquad \text{and} \qquad N_{x_j z}^{x_{j+1}} = 1 \qquad \text{for all } j = 1, \ldots, N - 1, \tag{17}$$

as illustrated by Fig. 5.

E. The gluing postulate

Throughout our work, we restrict our attention to models satisfying an additional property we refer to as the gluing postulate (which is often called the "gluing axiom" in the literature). Consider a closed curve C embedded in Σ. We will assume that C is an element of a DAP-decomposition C; although this is not strictly necessary, it will simplify our discussion. Now consider the surface Σ' obtained by cutting Σ along C. Compared to Σ, this is a surface with two boundary components C_1', C_2' (both isotopic to C) added. We will assume that these have opposite orientation. A familiar example is the case where cutting Σ along C results in two disconnected surfaces $\Sigma' = \Sigma_1 \cup \Sigma_2$, as depicted in Fig. 6 in the case where Σ is the 4-punctured sphere.

Let a be a particle label. We will denote by $\mathcal{H}_{\Sigma'(a,\overline{a})}$ the Hilbert space associated with the open surface Σ', where boundary C_1' is labeled by a and boundary C_2' by $\overline{a}$. The gluing postulate states that the Hilbert space of the surface Σ has the form

$$\mathcal{H}_\Sigma \cong \bigoplus_a \mathcal{H}_{\Sigma'(a,\overline{a})}, \tag{18}$$

where the direct sum is over all particle labels a that occur in different fusion-consistent labelings of C. In the special case where cutting along C gives two components Σ_1, Σ_2, we have $\mathcal{H}_\Sigma \cong \bigoplus_a \mathcal{H}_{\Sigma_1(a)} \otimes \mathcal{H}_{\Sigma_2(\overline{a})}$.
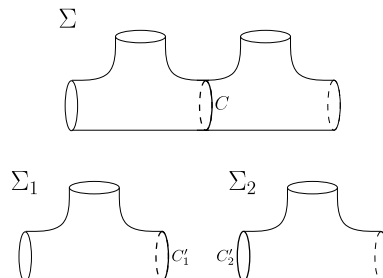

FIG. 6. Cutting a surface Σ along some closed curve C of a DAP-decomposition yields a disconnected surface $\Sigma' = \Sigma_1 \cup \Sigma_2$ having additional boundary components C_1' and C_2'.

Isomorphism (18) can easily be made explicit. A first observation is that $\mathcal{H}_\Sigma$ decomposes as $\mathcal{H}_\Sigma = \bigoplus_a \mathcal{H}_{a,\Sigma}(C)$, where

$$\mathcal{H}_{a,\Sigma}(C) := \mathsf{span}\{|\ell\rangle \mid \ell \in \mathsf{L}(C), \ell(C) = a\} \tag{19}$$

is the space spanned by all labelings which assign the label a to C. It, therefore, suffices to argue that

$$\mathcal{H}_{a,\Sigma}(C) \cong \mathcal{H}_{\Sigma'(a,\overline{a})} . \tag{20}$$

To do so, observe that the DAP-decomposition C of Σ gives rise to a DAP-decomposition $C' = C\backslash\{C\}$ of Σ'. Any labeling $\ell \in \mathsf{L}(C)$ with $\ell(C) = a$ restricts to a labeling $\ell' \in \mathsf{L}(C')$ of the labeled surface $\Sigma'(a,\overline{a})$. Conversely, any labeling $\ell' \in \mathsf{L}(C')$ of the surface $\Sigma'(a,\overline{a})$ provides a labeling $\ell \in \mathsf{L}(C)$ (by setting $\ell(C) = a$). This defines isomorphism (20) in terms of basis states $\{|\ell\rangle\}_{\ell\in\mathsf{L}(C)}$ and $\{|\ell'\rangle\}_{\ell'\in\mathsf{L}(C')}$.

1. Example: Decomposing the M-anyon Hilbert space

Consider the M-punctured sphere $\Sigma = S^2(z^M)$ with the standard DAP decomposition of Fig. 5 and boundary labels z (corresponding to M anyons of type z). Cutting $S^2(z^M)$ along C_j gives a surface Σ'_j which is the disjoint union of two punctured spheres, with $j + 2$ and $M - j$ punctures, respectively. The resulting surface labelings are $S^2(z^{j+1}, a)$ and $S^2(\overline{a}, z^{M-1-j})$. That is, if $\Sigma = S^2(z^M)$ is the original surface and $\Sigma'_j(a,\overline{a})$ is the resulting one, then

$$\mathcal{H}_{\Sigma'_j(a,\overline{a})} = \mathcal{H}_{S^2(z^{j+1},a)} \otimes \mathcal{H}_{S^2(\overline{a},z^{M-1-j})} . \tag{21}$$

This is illustrated in Fig. 7 for the case $M = 6$ and $j = 2$.

F. The mapping class group

In the following, we denote by MCG_Σ the *mapping class group* of the surface Σ. Physically, a mapping class group element for a surface Σ gradually deforms the surface, but returns to the original configuration. For the n-punctured sphere, the mapping class group includes braiding of the punctures. For the torus, a Dehn twist is an element of the mapping class group. More formally, elements of MCG_Σ are isotopy classes of orientation-preserving diffeomorphisms of Σ preserving labels and commuting with boundary parametrization (see, e.g., Ref. 19). Slightly abusing notation, we will often simply write $\vartheta \in \mathsf{MCG}_\Sigma$ for an equivalence class represented by a map $\vartheta : \Sigma \to \Sigma$. If Σ is the torus, then the mapping class group is generated by two elements, $\mathsf{MCG}_\Sigma = \langle s, t \rangle$ where s and t are the standard generators of the modular group. For the M-punctured sphere $S^2(z^M)$, we will also need the $M - 1$ elements $\{\sigma_j\}_{j=1}^{M-1}$, where σ_j braids holes j and $j + 1$.
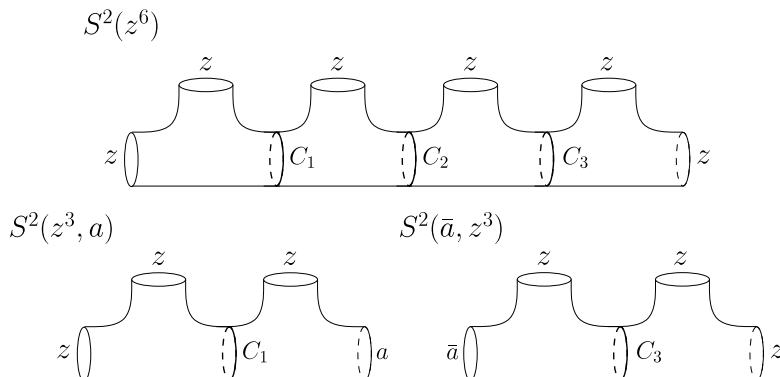

FIG. 7. The 6-punctured sphere $S^2(z^6)$ shown with three curves $C_1, C_2, C_3 \in C$ of a DAP-decomposition. Cutting along C_2 with labeling $\ell(C_2) = a$ results in the two surfaces $S^2(z^3, a)$ and $S^2(\overline{a}, z^3)$.

The Hilbert space $\mathcal{H}_\Sigma$ is equipped with a projective unitary representation

$$
\begin{aligned}
\mathsf{MCG}_\Sigma &\rightarrow \mathsf{U}(\mathcal{H}_\Sigma), \\
\vartheta &\mapsto \mathbf{V}(\vartheta)
\end{aligned}
\tag{22}
$$

of the mapping class group MCG_Σ. For example, for the torus, $\mathbf{V}(s) = S$ and $\mathbf{V}(t) = T$ are the usual S- and T-matrices defined by the modular tensor category. For the M-punctured sphere $S^2(z^M)$ with $M = N + 3$, we again use the standard DAP-decomposition with associated basis $\{|x\rangle\}_x$. Here, the sequences $x = (x_1, \ldots, x_N)$ are subject to the fusion rules (see (17)) and the action on such vectors is

$$
\begin{aligned}
\mathbf{V}(\sigma_1)|x\rangle &= R^{zz}_{x_1}|x\rangle, \\
\mathbf{V}(\sigma_k)|x\rangle &= \sum_{x'} B(x_{k-1}, x_{k+1})_{x'x_k}|x_1, \ldots, x_{k-1}, x', x_{k+1}, \ldots, x_N\rangle \qquad \text{for } k = 2, \ldots, N+1, \\
\mathbf{V}(\sigma_{N+2})|x\rangle &= \overline{R^{zz}_{x_1}}|x\rangle,
\end{aligned}
$$

where $B(a, b) = \tilde{F}^{-1}\tilde{R}\tilde{F}$ is the braid matrix. Here, the matrices $\tilde{F}$ and $\tilde{R}$ are given in terms of the tensors F and R associated with the TQFT.[47]

III. CONSTRAINTS ON LOCALITY-PRESERVING AUTOMORPHISMS

In this section, we derive restrictions on topologically protected gates for general non-abelian models. Our strategy will be to consider what happens to string-operators. We will first consider operators associated with a single loop C, and derive restrictions on the map $F_a(C) \mapsto UF_a(C)U^\dagger$, or, more precisely, its effect on logical operators, $[F_a(C)] \mapsto [UF_a(C)U^\dagger]$. We will argue that this map implements an isomorphism of the Verlinde algebra and exploit this fact to derive a constraint which is "local" to a specific loop. We will subsequently consider more "global" constraints arising from fusion rules, as well as basis changes.

We would like to characterize locality-preserving unitary automorphisms $U \in \mathcal{A}_\Sigma$ in terms of their logical action $[U]$. For example, in the toric code, where the physical qubits are embedded in the edges of the square lattice, the locality preserving unitaries include the well-known transversal gates of single-qubit unitaries applied to each qubit. More general examples of locality preserving unitaries in the toric code are finite depth circuits composed of gates of arbitrary unitaries applied to physical qubits in geometrically local patches of fixed diameter.

A first goal is to characterize the map

$$
\begin{aligned}
\rho_U : [\mathcal{A}_\Sigma] &\rightarrow [\mathcal{A}_\Sigma], \\
[X] &\mapsto [UXU^{-1}],
\end{aligned}
\tag{23}
$$

which determines the evolution of logical observables in the Heisenberg picture. (Clearly, this does not depend on the representative, i.e., if $[X] = [X']$, then $\rho_U([X]) = \rho_U([X'])$.) In fact, map (23) fully determines U up to a global phase since $[\mathcal{A}_\Sigma]$ contains an operator basis for linear maps on $\mathcal{H}_\Sigma$. However, it will often be more informative to characterize the action of $[U]$ on basis elements of $\mathcal{H}_\Sigma$. This will require additional effort.

The main observation is that map (23) defines an automorphism of $[\mathcal{A}_\Sigma]$, since

$$
\rho_U([X])\rho_U([X']) = \rho_U([X][X']) \qquad \text{for all } X, X' \in \mathcal{A}_\Sigma \qquad \text{and} \qquad \rho_U^{-1} = \rho_{U^{-1}}.
\tag{24}
$$

Combined with the locality of U, (24) severely constrains ρ_U. Using this fact, we obtain a number of very general constraints, which will be worked out in more detail in the following.

A. A local constraint from a simple closed loop

Specifying the action of ρ_U on all of $[\mathcal{A}_\Sigma]$ completely determines $[U]$ up to a global phase. However, this is not entirely straightforward; instead, we fix some simple closed curve C and

characterize the restriction to the subalgebra $\mathcal{A}(C) \subset \mathcal{A}_\Sigma$, i.e., the map

$$
\rho_U(C) : \quad [\mathcal{A}(C)] \quad \to \quad [\mathcal{A}(C)], \\
[X] \quad \mapsto \quad [UXU^{-1}],
\tag{25}
$$

Observe that this map is well-defined since UXU^{-1} is supported in a neighborhood of C (by the locality-preservation of U), and hence $[UXU^{-1}] = [X']$ for some operator $X' \in \mathcal{A}(C)$ (here we have used Proposition 2.1). It is also easy to see that it defines an automorphism of the subalgebra $[\mathcal{A}(C)]$.

As we argued above, the algebra $\mathcal{A}(C)$ is isomorphic to Ver. This carries over to $[\mathcal{A}(C)] \cong$ Ver $\cong \mathbb{C}^{\oplus|\mathbb{A}|}$. As Ver has idempotents $\mathbf{p}_{a \in \mathbb{A}}$, the logical algebra for loop C has idempotents $\{[P_a(C)]\}_{a \in \mathbb{A}}$. Note that the idempotents $\{[P_a(C)]\}_{a \in \mathbb{A}}$ in the logical algebra are unique, in that there is no linear combination of these idempotents which yields a distinct, complete set of idempotents. At the physical level, however, there can be huge redundancy, with many different physical operators corresponding to the same logical operator, i.e., $[P_a(C)] = [P_a'(C)]$, for $P_a(C) \neq P_a'(C)$. We use the following fact:

Lemma 3.1. The set of automorphisms of the algebra Ver *is in one-to-one correspondence with the permutations* $S_{|\mathbb{A}|}$. *For* $\pi \in S_{|\mathbb{A}|}$, *the associated automorphism* $\rho_\pi :$ Ver $\to$ Ver *is defined by its action on the central idempotents* $\mathbf{p}_a$

$$
\rho_\pi(\mathbf{p}_a) = \mathbf{p}_{\pi(a)} \qquad \text{for } a \in \mathbb{A}.
\tag{26}
$$

Proof. It is clear that (26) defines an automorphism for every $\pi \in S_{|\mathbb{A}|}$. Also, from Eq. (24), we see that $\mathbf{p}_a \mathbf{p}_b = \delta_{ab} \mathbf{p}_b$ implies $\rho(\mathbf{p}_a)\rho(\mathbf{p}_b) = \delta_{ab}\rho(\mathbf{p}_b)$, such that $\rho(\mathbf{p}_a) \in$ Ver are a complete set of projectors (Proposition 2.3). As there is a unique set of complete projectors for Ver, we conclude that $\rho(\mathbf{p}_a) = \mathbf{p}_{\pi(a)}$ for some permutation $\pi \in S_{|\mathbb{A}|}$. $\qquad \square$

Applying this to $[\mathcal{A}(C)]$ shows that a locality-preserving unitary automorphism realizes, up to *important* phases, a permutation of labelings. Let us emphasize that it is the projectors (idempotents) $[P_a(C)]$ which are being permuted, and not the string operators $[F_a(C)]$.

Proposition 3.1 (Local constraint). Let U be a locality-preserving automorphism of the code, and let $\rho_U([X]) = [UXU^{-1}]$.

(i)   *For each simple closed loop C on Σ, there is a permutation $\pi^C : \mathbb{A} \to \mathbb{A}$ of the particle labels such that*

$$
\rho_U : \quad [\mathcal{A}(C)] \quad \to \quad [\mathcal{A}(C)], \\
[P_a(C)] \quad \mapsto \quad [P_{\pi^C(a)}(C)] \qquad \text{for all } a \in \mathbb{A}
\tag{27}
$$

(and linearly extended to all of $[\mathcal{A}(C)]$).

(ii) *For some anyon model $\mathbb{A}$ with an associated S matrix, let $D_{a,b} = \delta_{a,b} \cdot d_a$ be the diagonal matrix with the quantum dimensions on the diagonal. Let $\pi^C : \mathbb{A} \to \mathbb{A}$ be a permutation associated with a loop C as in (i), and let Π be the matrix defined by $\Pi_{x,y} := \delta_{x,\pi^C(y)}$. Define the matrix*

$$
\Lambda := S\Pi^{-1}D\Pi D^{-1}\Pi^{-1}S^{-1} .
\tag{28}
$$

Then,

$$
\rho_U([F_b(C)]) = \sum_{b'} \Lambda_{b,b'}[F_{b'}(C)] .
\tag{29}
$$

Proof. We have already argued that (i) holds. For the proof of (ii), we use the relationship between $\{P_a(C)\}_a$ and $\{F_a(C)\}_a$ (cf. (14) and (15)) to get (suppressing the dependence on the loop C)

$$
\rho_U([F_b]) = \sum_a \frac{S_{b,a}}{S_{1,a}}[P_{\pi^C(a)}] = \sum_{b'}\left(\sum_a \frac{S_{b,a}}{S_{1,a}}S_{1,\pi^C(a)}\overline{S_{b',\pi^C(a)}}\right)[F_{b'}] .
$$

Claim (29) follows from this using $(\Pi^{-1}S^{-1})_{a,b'} = (S^{-1})_{\pi^C(a),b'} = \overline{S_{b',\pi^C(a)}}$ by the unitarity of S, as well as the fact that $S_{1,a} = d_a/\mathcal{D}$ and hence $\frac{S_{b,a}}{S_{1,a}} S_{1,\pi^C(a)} = (S\Pi^{-1}D\Pi D^{-1})_{b,a}$. $\qquad\square$

B. Global constraints from dap-decompositions, fusion rules, and the gluing postulate

For higher-genus surfaces, we can obtain information by applying Proposition 3.1 to all loops of a DAP-decomposition; these must then satisfy the following consistency condition.

Proposition 3.2 (Global constraint from fusion rules). Let U be a locality-preserving auto-morphism of the code. Let C be a DAP-decomposition of Σ, and consider the family of permutations $\vec{\pi} = \{\pi^C\}_{C \in \mathcal{C}}$ defined by Proposition 3.1. Then, this defines a permutation $\vec{\pi} : \mathsf{L}(\mathcal{C}) \to \mathsf{L}(\mathcal{C})$ of the set of fusion-consistent labelings via

$$\vec{\pi}(\ell)(C) := \pi^C[\ell(C)] \tag{30}$$

for all $C \in \mathcal{C}$. We have

$$U|\ell\rangle = e^{i\varphi(\ell)}|\vec{\pi}(\ell)\rangle \qquad \text{for all } \ell \in L(\mathcal{C}) \tag{31}$$

with some phase $e^{i\varphi(\ell)}$ depending on ℓ.

Proof. Let us fix some basis element $|\ell\rangle \in \mathcal{B}_{\mathcal{C}}$. The vector $|\ell\rangle$ is a $+1$-eigenvector of $P_{\ell(C)}(C)$ for each $C \in \mathcal{C}$; hence, according to (27), the vector $U|\ell\rangle$ is a $+1$-eigenvector of $P_{\pi^C[\ell(C)]}(C) = P_{\vec{\pi}(\ell)(C)}(C)$ for every $C \in \mathcal{C}$. This implies that it is proportional to $|\vec{\pi}(\ell)\rangle$; hence, we obtain (31). Fusion-consistency of $\vec{\pi}(\ell)$ follows because $U|\ell\rangle$ must be an element of $\mathcal{H}_\Sigma$. $\qquad\square$

Proposition 3.2 expresses the requirement that a locality-preserving automorphism U maps the set of fusion-consistent labelings into itself.

In fact, we can say more: it must be an isomorphism between the subspaces of $\mathcal{H}_\Sigma$ arising from the gluing postulate (i.e., Eq. (18)). This allows us to constrain the set of allowed permutations $\vec{\pi} = \{\pi^C\}_{C \in \mathcal{C}}$ arising from locality-preserving automorphisms even further:

Proposition 3.3 (Global constraint from gluing). Let C be an element of a DAP-decomposition of Σ. Recall that

$$\mathcal{H}_\Sigma = \bigoplus_a \mathcal{H}_{a,\Sigma}(C), \tag{32}$$

where the subspaces in the direct sum are defined by labelings associating a to C. Let U be a locality-preserving automorphism of the code and let $\pi^C : \mathbb{A} \to \mathbb{A}$ be the permutation associated with C by Proposition 3.1. Then, for every $a \in \mathbb{A}$ occurring in Eq. (32), the restriction of U to $\mathcal{H}_{a,\Sigma}(C)$ defines an isomorphism

$$\mathcal{H}_{a,\Sigma}(C) \cong \mathcal{H}_{\pi^C(a),\Sigma}(C). \tag{33}$$

In particular, if Σ' is the surface obtained by cutting Σ along C, then

$$\mathcal{H}_{\Sigma'(a,\overline{a})} \cong \mathcal{H}_{\Sigma'(\pi^C(a),\overline{\pi^C(a)})} \tag{34}$$

for every $a \in \mathbb{A}$ occurring in sum (32).

The reason we refer to Proposition 3.3 as a global constraint (even though it superficially only concerns a single curve C) is that the surface Σ' and hence spaces (34) depend on the global form of the surface Σ outside the support of C.

Proof. Proposition 3.2 implies that $U\mathcal{H}_{a,\Sigma}(C) \subset \mathcal{H}_{\pi^C(a),\Sigma}(C)$ for any a in expression (32). Since U acts unitarily on the whole space $\mathcal{H}_\Sigma$, this is compatible with (32) only if $U\mathcal{H}_{a,\Sigma}(C) = \mathcal{H}_{\pi^C(a),\Sigma}(C)$ for any such a. This proves (33). Statement (34) then immediately follows from (20). $\qquad\square$

A simple but useful implication of Proposition 3.3 is that

$$\dim\left(\mathcal{H}_{\Sigma'(a,\overline{a})}\right) = \dim\left(\mathcal{H}_{\Sigma'(\pi^C(a),\overline{\pi^C(a)})}\right) \tag{35}$$

is a necessary condition that π^C has to satisfy.

C. Global constraints from basis changes

Eq. (27) essentially tells us that a locality-preserving protected gate U can only permute particle labels; it indicates that such a gate U is related to certain symmetries of the anyon model. But (27) does not tell us what phases basis states may acquire. We show how to obtain constraints on these phases by considering basis changes. This also further constrains the allowed permutations on the labels of the idempotents.

Consider two DAP-decompositions C and C'. Expressed in the first basis $\mathcal{B}_C$, we have

$$U|\ell\rangle = e^{i\varphi(\ell)}|\vec{\pi}(\ell)\rangle \tag{36}$$

for some unknown phase $\varphi(\ell)$ depending only on the labeling $\ell \in \mathsf{L}(C)$. This means that with respect to the basis elements of $\mathcal{B}_C$, the operator U is described by a matrix $\mathbf{U} = \mathbf{\Pi}\mathbf{D}(\{\varphi(\ell)\}_\ell)$, where $\mathbf{\Pi}$ is a permutation matrix (acting on the fusion-consistent labelings $\mathsf{L}(C)$), and $\mathbf{D}$ is a diagonal matrix with entries $\{e^{i\varphi(\ell)}\}_\ell$ on the diagonal.

Analogously, we can consider the operator U expressed as a matrix $\mathbf{U}'$ in terms of the basis elements of $\mathcal{B}_{C'}$. We conclude that $\mathbf{U}' = \mathbf{\Pi}'\mathbf{D}(\{\varphi'(\ell)\}_\ell)$, for $\ell \in \mathsf{L}(C')$, with a (potentially different) permutation matrix $\mathbf{\Pi}'$, and (potentially different) phases $\{\varphi'(\ell)\}_\ell$.

Let $\mathbf{V}$ be the unitary change-of-basis matrix for going from $\mathcal{B}_C$ to $\mathcal{B}_{C'}$. Then, we must have

$$\mathbf{VU} = \mathbf{U}'\mathbf{V}. \tag{37}$$

We show below that this equation strongly constrains the phases as well as the permutations in (31). More specifically, we will examine constraints arising when using basis changes $\mathbf{V}$ defined by F-moves in Section V. In Section IV, we consider basis changes $\mathbf{V}$ defined by elements of the mapping class group.

IV. GLOBAL CONSTRAINTS FROM THE MAPPING CLASS GROUP

The following is based on the simple observation that we must have consistency conditions of form (37) for more general basis changes (in particular, basis changes not made up of F-moves only). We are particularly interested in the case where the basis change is the result of applying a mapping class group element.

A. Basis changes defined by the mapping class group

A key property of representation (22) of the mapping class group MCG_Σ is that it maps idempotents according to

$$V(\vartheta)P_a(C)V(\vartheta)^\dagger = P_a\big(\vartheta(C)\big). \tag{38}$$

Let us fix a "standard" DAP-decomposition C, and let $\mathcal{B}_C = \{|\ell\rangle_C\}_\ell$ be the corresponding standard basis.

Let ϑ be an arbitrary element of MCG_Σ. Consider the basis

$$\mathcal{B}_{\vartheta(C)} := \{V(\vartheta)|\ell\rangle\}_\ell.$$

Because of (38), this basis is a simultaneous eigenbasis of the complete set of commuting observables associated with the DAP decomposition $\vartheta(C) := \{\vartheta(C_j)\}_{j=1}^M$. The change of basis from $\mathcal{B}_C$ to $\mathcal{B}_{\vartheta(C)}$ is given by the image $V(\vartheta)$ of the mapping class group element ϑ.

In particular, if $\mathbf{V}(\vartheta)$ is the matrix representing $V(\vartheta)$ in the standard basis, then (37) implies

$$\mathbf{V}(\vartheta)\mathbf{\Pi}\mathbf{D} = \mathbf{\Pi}(\vartheta)\mathbf{D}(\vartheta)\mathbf{V}(\vartheta) \tag{39}$$

for some permutation matrix $\mathbf{\Pi}(\vartheta)$ and a diagonal matrix $\mathbf{D}(\vartheta)$ consisting of phases.

Some terminology will be useful: Let Δ be the set of matrices of the form $\mathbf{\Pi D}$, where $\mathbf{\Pi}$ is a permutation of fusion-consistent labelings, and $\mathbf{D}$ is a diagonal matrix with phases (these are sometimes called *unitary monomial matrices*). For $\mathbf{U} \in \Delta$ and $\vartheta \in \mathsf{MCG}_\Sigma$, we say that $\mathbf{U}$ intertwines with ϑ if

$$\mathbf{V}(\vartheta)\mathbf{U}\mathbf{V}(\vartheta)^\dagger \in \Delta .$$

Let $\Delta_\vartheta \subset \Delta$ be the set of matrices that intertwine with ϑ, and let

$$\Delta_{\mathsf{MCG}_\Sigma} = \bigcap_{\vartheta \in \mathsf{MCG}_\Sigma} \Delta_\vartheta$$

be the matrices that are intertwiners of the whole mapping class group representation. We have shown the following:

Theorem 4.1. *Let* $\mathbf{U}$ *be the matrix representing a protected gate* U *in the standard basis. Then* $\mathbf{U} \in \Delta_{\mathsf{MCG}_\Sigma}$.

As an example, consider the torus: since $T = \mathbf{V}(t)$ is diagonal, it is easy to see that for any $\mathbf{\Pi D} \in \Delta$, we have $T\mathbf{\Pi D}T^{-1} = \mathbf{\Pi D}'$ for some $\mathbf{D}'$. This implies that $\Delta_t = \Delta$ is generally not interesting, i.e., $\mathbf{U} \in \Delta_t$ does not impose an additional constraint. In contrast, mapping class group elements such as s and st generally give different non-trivial constraints.

B. Density of the mapping class group representation and absence of protected gates

The following statement directly links computational universality of the mapping class group representation to the non-existence of protected gates.

Corollary 4.2. Suppose the representation of MCG_Σ *is dense in the projective unitary group* $\mathsf{PU}(\mathcal{H}_\Sigma)$. *Then there is no non-trivial protected gate.*

Proof. Let U be an arbitrary protected gate and let $\mathbf{U} \in \Delta$ be the matrix representing it in the standard basis. Assume for the sake of contradiction that U is non-trivial. Then $\mathbf{U}$ is a unitary with at least two different eigenvalues $\lambda_1, \lambda_2 \in \mathrm{U}(1)$. In particular, there is a diagonalizing unitary $\mathbf{V}_1$ such that $\mathbf{V}_1\mathbf{U}\mathbf{V}_1^\dagger = \mathsf{diag}(\lambda_1, \lambda_2) \oplus \tilde{\mathbf{U}}$ for some matrix $\tilde{\mathbf{U}}$. Setting $\mathbf{V}_2 = H \oplus I$, where H is the Hadamard matrix

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

and $\mathbf{V} = \mathbf{V}_2\mathbf{V}_1$, we obtain that

$$\mathbf{V}\mathbf{U}\mathbf{V}^\dagger \notin \Delta \tag{40}$$

because this matrix contains both diagonal and off-diagonal elements. Note that if $\lambda_2 = -\lambda_1$, one may use the matrix

$$\frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$$

instead of H.

Observe also that (40) stays valid if we replace $\mathbf{V}$ by a sufficiently close approximation (up to an irrelevant global phase) $\tilde{\mathbf{V}} \approx \mathbf{V}$. In particular, by the assumed density, we may approximate $\mathbf{V}$ by a product $\tilde{\mathbf{V}} = \mathbf{V}(\vartheta_1)\cdots\mathbf{V}(\vartheta_m)$ of images of $\vartheta_1, \ldots, \vartheta_m \in \mathsf{MCG}_\Sigma$. But then we have

$$\mathbf{U} \notin \Delta_{\vartheta_1\cdots\vartheta_m} ,$$

which contradicts Theorem 4.1.   □

Note that, in general, the mapping class group is only dense on a subspace $\mathcal{H}_0 \subset \mathcal{H}_\Sigma$. This is the case, for example, when the overall system allows for configurations where anyons can be present or absent (e.g., a boundary may or may not carry a topological charge). In such a situation, $\mathcal{H}_\Sigma$ decomposes into superselection sectors which are defined by the gluing postulate (i.e., having fixed labels associated with certain closed loops associated). Corollary 4.2 can be adapted to this situation, e.g., as explained in the Appendix (Lemma 1.1).

C. Characterizing diagonal protected gates

Fix a DAP-decomposition C and let $\vartheta \in \mathsf{MCG}_\Sigma$. Let us call two (fusion-consistent) labelings ℓ_1, ℓ_2 *connected by* ϑ (denoted $\ell_1 \Leftrightarrow_\vartheta \ell_2$) if there is a labeling ℓ such that

$$0 \neq \langle \ell | V(\vartheta) | \ell_m \rangle \qquad \text{for } m = 1, 2 .$$

(Here $|\ell\rangle$ is the associated basis element of $\mathcal{B}_C$.) More generally, let us say ℓ_1, ℓ_2 are connected (written $\ell_1 \Leftrightarrow \ell_2$) if there exists an element $\vartheta \in \mathsf{MCG}_\Sigma$ such that $\ell_1 \Leftrightarrow_\vartheta \ell_2$. Clearly, this notion is symmetric in ℓ_1, ℓ_2, and furthermore, it is reflexive, i.e., $\ell_1 \Leftrightarrow \ell_1$ since $\ell_1 \Leftrightarrow_{\mathsf{id}} \ell_1$. We can, therefore, define an equivalence relation on the set of labelings: we write $\ell_1 \sim \ell_2$ if there are labelings $k_1, \ldots, k_m$ such that $\ell_1 \Leftrightarrow k_1 \Leftrightarrow \cdots \Leftrightarrow k_m \Leftrightarrow \ell_2$. We point out (for later use) that we can always find a finite collection $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ that generates the relation $\sim$ in the sense that $\ell_1 \sim \ell_2$ if and only if $\ell_1 \Leftrightarrow_{\vartheta_k} \ell_2$ for some k (after all, we only have a finite set of labelings ℓ).

Observe that if the representation of MCG_Σ has a non-trivial invariant subspace, then there is more than one equivalence class. We discuss an example of this below (see Section IV E). However, in important special cases such as the Fibonacci or Ising models, there is only one equivalence class for the relation $\sim$, i.e., any pair of labelings are connected (see Lemmas 6.3 and 6.4).

Lemma 4.3. Consider a protected gate U acting diagonally in the basis $\mathcal{B}_C$ as $U|\ell\rangle = e^{i\varphi(\ell)}|\ell\rangle$.

(i) *Suppose that U also acts diagonally in the basis $\mathcal{B}_{\vartheta(C)}$. Then $\varphi(\ell_1) = \varphi(\ell_2)$ for any pair $\ell_1 \Leftrightarrow_\vartheta \ell_2$ connected by ϑ.*

(ii) *Suppose that $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ generates the relation $\sim$, and U acts diagonally in each basis $\mathcal{B}_{\vartheta_k(C)}$. Then φ assigns the same value to every element of the same equivalence class under $\sim$.*

We will refer to a protected gate U with property (ii) as a $\sim$-trivial gate. One implication of Lemma 4.3 is that any protected gate which is close to the identity acts as a $\sim$-trivial gate (see the proof of Theorem 4.5). In Section IV D, we will show how to use this statement to prove that the set of protected gates is finite up to irrelevant phases.

Proof. Consider two labelings ℓ_1, ℓ_2 satisfying $\ell_1 \Leftrightarrow_\vartheta \ell_2$. Then, writing $\mathbf{V} = \mathbf{V}(\vartheta)$, we know that

$$\mathbf{V}_{\ell, \ell_1} \neq 0 \qquad \text{and} \qquad \mathbf{V}_{\ell, \ell_2} \neq 0 \tag{41}$$

for some labeling ℓ, where $\mathbf{V}_{\ell, k} = \langle \ell | V(\vartheta) | k \rangle$. Since U acts diagonally in both bases $\mathcal{B}_C$ and $\mathcal{B}_{\vartheta(C)}$ by assumption, (39) becomes simply

$$\mathbf{V} \mathbf{D} \mathbf{V}^\dagger = \mathbf{D}(\vartheta) \tag{42}$$

when written in the standard basis. Here, the diagonal matrices are given by $\mathbf{D} = \mathrm{diag}(\{\varphi(\ell)\}_\ell)$ and $\mathbf{D}(\vartheta) = \mathrm{diag}(\{\varphi'(\ell)\}_\ell)$. Taking the diagonal entry at position (ℓ, ℓ) in matrix equation (42), we get the identity

$$\sum_k e^{i(\varphi(k) - \varphi'(\ell))} |\mathbf{V}_{\ell, k}|^2 = 1. \tag{43}$$

By unitarity of the mapping class group representation, we also have

$$\sum_k |\mathbf{V}_{\ell, k}|^2 = 1. \tag{44}$$

By taking the real part of (43), it is straightforward to see that compatibility with (44) imposes that $\cos(\varphi(k) - \varphi'(\ell)) = 1$ whenever $|\mathbf{V}_{\ell,k}| \neq 0$ or

$$\varphi(k) \equiv \varphi'(\ell) \mod 2\pi \qquad \text{for all } k \text{ with } |\mathbf{V}_{\ell,k}| \neq 0.$$

With (41), we conclude that $\varphi(\ell_1) = \varphi'(\ell) = \varphi(\ell_2)$, which proves claim (i).

The claim (ii) immediately follows from (i). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

We will show how to apply this result to the Fibonacci model in Section VI A 2. Note that Lemma 4.3 does not generally rule out the existence of non-trivial diagonal protected gates in the standard basis (an example is a Pauli-Z in the Ising model, see Section VI B 1): it is important that the protected gate is diagonal in *several* different bases $\{\mathcal{B}_{\vartheta_k(C)}\}_k$.

A simple consequence of Lemma 4.3 is that any protected gate has a finite order up to certain phases:

Lemma 4.4. There is a finite n_0 (depending only on the dimension of $\mathcal{H}_\Sigma$) such that for every protected gate U, there is an $n \leq n_0$ such that U^n is a $\sim$-trivial phase gate.

Proof. Consider an arbitrary DAP-decomposition C and suppose U acts as (31) in the basis $\mathcal{B}_C$. Since the permutation $\vec{\pi}$ acts on the finite set $\mathsf{L}(C)$ of fusion-consistent labelings, it has finite order n_C. This means that U^{n_C} acts diagonally in the basis $\mathcal{B}_C$.

Assume $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ generate the relation $\sim$. Setting $n = \mathsf{lcm}(n_{\vartheta_1(C)}, \ldots, n_{\vartheta_M(C)})$, we can apply Lemma 4.3 to U^n to reach the conclusion that U^n is $\sim$-trivial. Furthermore, since the number n depends only on the permutation $\vec{\pi}$, and there are only finitely many such permutations, there is a finite n_0 with the claimed property. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

D. Finiteness of the set of protected gates

In the following, we will ignore phase differences that are "global" to subspaces of vectors defined by the equivalence classes of $\sim$. That is, we will call two protected gates U_1 and U_2 equivalent (written $U_1 \sim U_2$) if

$$\begin{aligned} \mathbf{U}_1 &= \mathbf{\Pi}\mathbf{D}_1 \\ \mathbf{U}_2 &= \mathbf{\Pi}\mathbf{D}_2 \end{aligned} \qquad \text{and} \qquad (\mathbf{D}_2)_{\ell,\ell} = e^{i\varphi([\ell])}(\mathbf{D}_1)_{\ell,\ell},$$

i.e., they encode the same permutation of fusion-consistent labels, and their phases only differ by a phase $\varphi([\ell])$ depending on the equivalence class $[\ell]$ that ℓ belongs to. This is equivalent to the statement that $\mathbf{U}_1^{-1}\mathbf{U}_2 = \mathbf{D}_1^{-1}\mathbf{D}_2$ acts as a phase dependent only on the equivalence class, i.e., $U_1^{-1}U_2$ is a $\sim$-trivial phase gate.

We obtain an Eastin and Knill[14] type statement, which is one of our main conclusions.

Theorem 4.5 (Finite group of protected gates). *The number of equivalence classes of protected gates is finite.*

In particular, this means that locality-preserving automorphisms on their own do not provide quantum computational universality.

Proof. Assume that there are infinitely many equivalence classes of protected gates. Then we can choose a sequence $\{U_n\}_{n \in \mathbb{N}}$ of protected gates indexed by integers and belonging to different equivalence classes each. Since the number of permutations of fusion-consistent labels is finite, there exists at least one permutation matrix $\mathbf{\Pi}$ such that there is an infinite subsequence of protected gates U_n with $\mathbf{U}_n = \mathbf{\Pi}\mathbf{D}_n$, i.e., they act with the same permutation. Applying the Bolzano-Weierstrass theorem to this subsequence, we conclude that there is a convergent subsequence of protected gates $\{U_{n_j}\}_{j \in \mathbb{N}}$ such that $\mathbf{U}_{n_j} = \mathbf{\Pi}\mathbf{D}_{n_j}$ for all j. Let $U = \lim_{j \to \infty} U_{n_j}$ be the corresponding limit, and let us define $\tilde{U}_j := U^{-1}U_{n_j}$. Clearly, each $\tilde{U}_j$ is a protected gate and

$$\tilde{\mathbf{U}}_j = \mathbf{D}^{-1}\mathbf{D}_{n_j} \tag{45}$$

acts non-trivially on subspaces defined by equivalence classes, i.e., $\tilde{U}_j$ is a $\sim$-non-trivial phase gate. This is because of the assumption that the original sequence $\{U_n\}_{n \in \mathbb{N}}$ has elements belonging to different equivalence classes. Furthermore, we have that

$$\lim_{j \to \infty} \tilde{\mathbf{U}}_j = \mathbf{I}, \tag{46}$$

where $\mathbf{I}$ is the identity matrix.

For a mapping class group element $\vartheta \in \mathsf{MCG}_\Sigma$, the matrix expressing the action of $\tilde{U}_j$ in the basis $\mathcal{B}_{\vartheta(C)}$ is given by $\mathbf{V}(\vartheta)\tilde{\mathbf{U}}_j\mathbf{V}(\vartheta)^\dagger$. Because $\tilde{U}_j$ is a protected gate, we get

$$\mathbf{V}(\vartheta)\tilde{\mathbf{U}}_j\mathbf{V}(\vartheta)^\dagger = \tilde{\mathbf{\Pi}}_j\tilde{\mathbf{D}}_j \tag{47}$$

for some permutation matrix $\tilde{\mathbf{\Pi}}_j$ and a diagonal matrix $\tilde{\mathbf{D}}_j$ of phases. Combining (46) and (47), using the unitarity of $\mathbf{V}(\vartheta)$ and continuity, we conclude that there exists some $N_0 = N_0(\vartheta)$ such that $\tilde{\mathbf{\Pi}}_j = \mathbf{I}$ for all $j \geq N_0$, i.e., $\mathbf{V}(\vartheta)\tilde{\mathbf{U}}_j\mathbf{V}(\vartheta)^\dagger$ is diagonal for sufficiently large j. Equivalently, for all $j \geq N_0$, $\tilde{U}_j$ acts diagonally in the basis $\mathcal{B}_{\vartheta(C)}$, as well as in the basis $\mathcal{B}_C$ (by (45)).

The latter conclusion can be extended uniformly to a finite collection $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ of mapping class group elements: there is a constant $N = N(\vartheta_1, \ldots, \vartheta_M)$ such that for all $j \geq N$, the protected gate $\tilde{U}_j$ acts as a diagonal matrix in all bases $\mathcal{B}_C, \mathcal{B}_{\vartheta_1(C)}, \ldots, \mathcal{B}_{\vartheta_M(C)}$. Taking a finite collection $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ that generates the relation $\sim$ and applying Lemma 4.3, we reach the conclusion that $\tilde{U}_j$ is a $\sim$-trivial phase gate for all $j \geq N$. This contradicts the fact that each $\tilde{U}_j$ is a $\sim$-non-trivial phase gate, as argued above.   □

E. Necessity of restricting to equivalence classes

Here, we briefly argue that without imposing $\sim$-equivalence on protected gates, one can end up with infinitely many protected gates (that are, however, not very interesting).

Concretely, consider a model such as the toric code, with local commuting projector Hamiltonian $H_{top} = -\sum_j \Pi_j$ acting on spins which we collectively denote by A. Let $\mathcal{H}_\Sigma$ be its ground space. We introduce a local spin-degree of freedom B_j associated with each term in the Hamiltonian, and let $B = \bigotimes_j B_j$ the space of these auxiliary degrees of freedom. Define an Ising-like Hamiltonian $H_I = -\sum_{\langle j,j' \rangle} Z_j Z_{j'}$ coupling all nearest neighbors in B (according to some notion). Finally, consider the following Hamiltonian:

$$H = J \cdot H_I - \sum_j \Pi_j \otimes |0\rangle\langle 0|_{B_j} - \sum_j \Pi_j \otimes |1\rangle\langle 1|_{B_j}. \tag{48}$$

This Hamiltonian is local, and for large J, has a ground space of the form

$$(\mathcal{H}_\Sigma \otimes |00 \cdots 0\rangle) \oplus (\mathcal{H}_\Sigma \otimes |11 \cdots 1\rangle). \tag{49}$$

In other words, the ground space (and similarly the low-energy subspace) splits as $\mathcal{H}_\Sigma^{(0)} \oplus \mathcal{H}_\Sigma^{(1)}$ into two isomorphic copies of the space $\mathcal{H}_\Sigma$.

Now take two arbitrary protected gates $U^{(0)}, U^{(1)}$ for H_{top} (these may be global phases, i.e., trivial), implementing logical operations $\overline{U}^{(0)}, \overline{U}^{(1)}$. Let us assume that they are implemented by circuits acting locally, i.e., they can be written (arbitrarily — the details do not matter) in the form

$$U^{(m)} = U_{j_1}^{(m)} U_{j_2}^{(m)} \cdots U_{j_{M_m}}^{(m)}$$

with each unitary U_j local near the support of Π_j. Then, we can define the unitary

$$U = \prod_{k=1}^{M_0} \left(U_{j_k}^{(0)} \otimes |0\rangle\langle 0|_{B_{j_k}} + \mathsf{id} \otimes |1\rangle\langle 1|_{B_{j_k}} \right) \prod_{k=1}^{M_1} \left(\mathsf{id} \otimes |0\rangle\langle 0|_{B_{j_k}} + U_{j_k}^{(1)} \otimes |1\rangle\langle 1|_{B_{j_k}} \right)$$

on $A \otimes B$. It is easy to check that U is a protected gate and its logical action is

$$\overline{U} = \overline{U}^{(0)} \oplus \overline{U}^{(1)}.$$

In particular, such a unitary can introduce an arbitrary relative phase between the "superselection" sectors $\mathcal{H}_\Sigma^{(0)}$, $\mathcal{H}_\Sigma^{(1)}$: we can choose $U^{(0)} = I$ and $U^{(1)} = e^{i\varphi}I$. The construction here corresponds to the direct sum of two TQFTs; the mapping class group representation is reducible and basis elements belonging to different sectors are inequivalent. Imposing the relation $\sim$ on the set of protected gates renders all such relative-phase gates equivalent.

A small caveat is in order here concerning the given microscopic example. Hamiltonian (48) indeed has (49) as its ground space. However, the latter is not an error-correcting code: whether a state belongs to $\mathcal{H}_\Sigma^{(0)}$ or $\mathcal{H}_\Sigma^{(1)}$ can be determined by a local measurement. Thus, information should only be encoded in either one of the superselection sectors, and this renders the introduction of (arbitrary) relative phases between two superselection sectors computationally trivial. The example given here is mainly intended to give a concrete realization of space (49) as the ground space of a local Hamiltonian, and to illustrate the fact that reducibility of the mapping class group representation has important consequences on the form of protected gates.

V. GLOBAL CONSTRAINTS FROM *F*-MOVES ON THE *n*-PUNCTURED SPHERE

We first consider the four-punctured sphere, where there are two inequivalent DAP-decompositions related by an F-move (i.e., the basis change **V** is the F-matrix). More generally (e.g., for the 5-punctured sphere), we need to consider several different F-moves and obtain a constraint of form (37) for every pair of bases related by such moves. We describe such global constraints in Section V C. The results obtained by considering F-moves are summarized in Section V D: there we outline a general procedure for characterizing protected gates.

The consideration of/restriction to n-punctured spheres is motivated by the fact that they correspond to $n-1$ anyons situated on a disc. Realizing such a system appears to be more feasible experimentally than designing, e.g., a higher-genus surface. For this reason, the n-punctured sphere is most commonly considered in the context of topological quantum computation. We point out, however, that our techniques immediately generalize to other (higher-genus) surfaces with or without punctures (although basis changes other than those given by the F-matrix need to be considered).

A. Determining phases for the four-punctured sphere: Fixed boundary labels

For a four-punctured sphere Σ, we can fix the labels on the punctures to $i, j, k, l \in \mathbb{A}$. The corresponding space $\mathcal{H}_{\Sigma(i,j,k,l)}$ associated to this open surface with labeled boundary components is the fusion space V_{kl}^{ij}. (In the non-abelian case, this space can have dimension larger than 1.) We have two bases $\mathcal{B}_C$, $\mathcal{B}_{C'}$ of this fusion space, corresponding to two different DAP-decompositions differing by one loop (Fig. 4). We can enumerate basis elements by the label assigned to this loop. Let $\{|a\rangle_C\}_a$ and $\{|a\rangle_{C'}\}_a$ be the elements of the bases $\mathcal{B}_C$ and $\mathcal{B}_{C'}$, respectively. Note that a ranges over all elements consistent with the fusion rules.

For the models considered in this article, these are $N_{ij}^a = N_{kl}^a = 1$. Let $Q = Q(i,j,k,l)$ be the set of such elements. The basis change is given by the F-matrix

$$|m\rangle_{C'} = \sum_n F_{kln}^{ijm}|n\rangle_C.$$

Considering a locality-preserving automorphism which preserves the boundary labels (this is reasonable if we think of them as certain boundary conditions of the system), we can apply the procedure explained above to find the action

$$U|a\rangle_C = e^{i\varphi(a)}|\pi^C(a)\rangle_C$$

on basis states. Here, $\pi^C: Q \to Q$ permutes fusion-consistent labels. To apply the reasoning above, we have to use the $|Q \times Q|$-basis change matrix **V** defined by $\mathbf{V}_{m,n} = F_{kln}^{ijm}$.

Solving consistency relation (37) (for the permutations π^C, $\pi^{C'}$ and phases $\{\varphi(a)\}_a, \{\varphi'(a)\}_a$) shows that for any permutation π^C that is part of a solution, the function φ takes the form
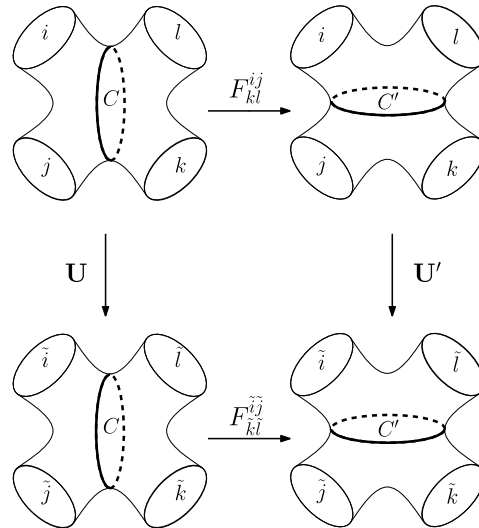
$$\varphi(a) = \eta + f(a), \tag{50}$$

FIG. 8. An isomorphism $\mathcal{H}_{\Sigma(i,j,k,l)} \to \mathcal{H}_{\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})}$ of two 4-punctured spheres can be given as either **U**, which relates the bases $\mathcal{B}_C$ of $\mathcal{H}_{\Sigma(i,j,k,l)}$ to $\tilde{\mathcal{B}}_C$ of $\mathcal{H}_{\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})}$, or as **U**$'$ relating different bases $\mathcal{B}_{C'}$ of $\mathcal{H}_{\Sigma(i,j,k,l)}$ to $\tilde{\mathcal{B}}_{C'}$ of $\mathcal{H}_{\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})}$. The bases of $\mathcal{H}_{\Sigma(i,j,k,l)}$ and $\mathcal{H}_{\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})}$ are related through the F-moves F^{ij}_{kl} and $F^{\tilde{i}\tilde{j}}_{\tilde{k}\tilde{l}}$, respectively. Consistency equation (54) can be expressed as a commutative diagram. In the case where $\Sigma(i,j,k,l) = \Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})$ have identical boundary labels such an isomorphism becomes an automorphism, and this reduces to consistency equation (53).

where η is a global phase and f belongs to a certain set of functions which we denote

$$\mathsf{Iso}\left(\underline{j\ \overset{\overset{\textstyle i}{|}}{}\ \cdot\ \overset{\overset{\textstyle l}{|}}{}\ k} \ \to\ \underline{j\ \overset{\overset{\textstyle i}{|}}{}\ \pi^C(\cdot)\ \overset{\overset{\textstyle l}{|}}{}\ k} \right). \tag{51}$$

(The reason for this notation will become clearer when we discuss isomorphisms in Sec. V B; here, we are concerned with relative phases arising from automorphisms.) In summary, we have

$$U|a\rangle_C = e^{i\eta} e^{if(a)} |\pi^C(a)\rangle_C \qquad \text{where } f \in \mathsf{Iso}\left(\underline{j\ \overset{\overset{\textstyle i}{|}}{}\ \cdot\ \overset{\overset{\textstyle l}{|}}{}\ k} \ \to\ \underline{j\ \overset{\overset{\textstyle i}{|}}{}\ \pi^C(\cdot)\ \overset{\overset{\textstyle l}{|}}{}\ k} \right).$$
$$\tag{52}$$

Here, set (51) can be computed by solving the consistency relation

$$\mathbf{V}\boldsymbol{\Pi}\mathbf{D}(\{\varphi(a)\}_a) = \boldsymbol{\Pi}'\mathbf{D}(\{\varphi'(a)\}_a)\mathbf{V}, \tag{53}$$

with $\mathbf{V}_{m,n} = F^{ijm}_{kln}$. This scenario is a special case of the commutative diagram displayed in Fig. 8.

B. Determining phases for the four-punctured sphere in general

Consider the four-punctured sphere Σ with fixed labels $i,j,k,l \in \mathbb{A}$ on the punctures. Let $\tilde{i},\tilde{j},\tilde{k},\tilde{l}$ be another set of labels such that the spaces $\mathcal{H}_{\Sigma(i,j,k,l)}$ and $\mathcal{H}_{\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})}$ are isomorphic. In this situation, we can try to characterize locality-preserving isomorphisms between two systems defined on $\Sigma(i,j,k,l)$ and $\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})$, respectively. This situation is slightly more general than what we considered before (automorphisms of the same system), but it is easy to see that all arguments applied so far extend to this situation. Note that we could have phrased our whole discussion in terms of isomorphisms between different spaces. However, we chose not to do so to minimize the amount of notation required; instead, we only consider this situation in this section. This generalization for the 4-punctured sphere is all we need to treat automorphisms on higher-genus surfaces.

For $\mathcal{H}_{\Sigma(i,j,k,l)}$, we have two bases $\mathcal{B}_C$, $\mathcal{B}_{C'}$, corresponding to two different DAP-decompositions differing by one loop. Similarly, for $\mathcal{H}_{\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})}$, we have two bases $\tilde{\mathcal{B}}_C$, $\tilde{\mathcal{B}}_{C'}$, corresponding to two different DAP-decompositions differing by one loop. We can enumerate the basis elements by the

label assigned to this loop. Let $\{|a\rangle_C\}_a$ and $\{|a\rangle_{C'}\}_a$ be the elements of the bases $\mathcal{B}_C$ and $\mathcal{B}_{C'}$, respectively. Here, a ranges over the set $Q = Q(i,j,k,l) \subset \mathbb{A}$ of all elements consistent with the fusion rules, i.e., we must have $N_{ij}^a = N_{kl}^a = 1$. Similarly, let $\{|\tilde{a}\rangle_C\}_{\tilde{a}}$ and $\{|\tilde{a}\rangle_{C'}\}_{\tilde{a}}$ be the elements of the bases $\tilde{\mathcal{B}}_C$ and $\tilde{\mathcal{B}}_{C'}$, respectively, where now $\tilde{a} \in \tilde{Q} = Q(\tilde{i},\tilde{j},\tilde{k},\tilde{l})$.

In this situation, we have two basis changes,

$$|m\rangle_{C'} = \sum_n \mathbf{V}_{m,n}|n\rangle_C \text{ where } \mathbf{V}_{m,n} = F_{kln}^{ijm} \qquad \text{and} \qquad |\tilde{m}\rangle_{C'} = \sum_{\tilde{n}} \tilde{\mathbf{V}}_{\tilde{m},\tilde{n}}|\tilde{n}\rangle_C \text{ where } \tilde{\mathbf{V}}_{\tilde{m},\tilde{n}} = F_{\tilde{k}\tilde{l}\tilde{n}}^{\tilde{i}\tilde{j}\tilde{m}}.$$

Now consider a locality-preserving isomorphism U which takes the boundary labels (i,j,k,l) to $(\tilde{i},\tilde{j},\tilde{k},\tilde{l})$. We can then apply the framework above to find the action

$$U|a\rangle_C = e^{i\varphi(a)}|\pi^C(a)\rangle_C \qquad \text{or} \qquad U|a\rangle_{C'} = e^{i\varphi'(a)}|\pi^{C'}(a)\rangle_{C'}$$

on basis states. Here, $\pi^C, \pi^{C'}: Q \to \tilde{Q}$ take fusion-consistent labels on $\Sigma(i,j,k,l)$ to fusion-consistent labels on $\Sigma(\tilde{i},\tilde{j},\tilde{k},\tilde{l})$. Because the spaces are isomorphic, we must have $|Q| = |\tilde{Q}|$; hence, $\pi^C, \pi^{C'}$ can be represented by permutation matrices $\mathbf{\Pi}, \mathbf{\Pi}'$ in the basis pairs $(\mathcal{B}_C, \tilde{\mathcal{B}}_C)$ or $(\mathcal{B}_{C'}, \tilde{\mathcal{B}}_{C'})$, respectively. Proceeding similarly with $\mathbf{U}$, we get the consistency equation $\tilde{\mathbf{V}}\mathbf{U} = \mathbf{U}'\mathbf{V}$ or

$$\tilde{\mathbf{V}}\mathbf{\Pi}\mathbf{D}(\{\varphi(a)\}_a) = \mathbf{\Pi}'\mathbf{D}(\{\varphi'(a)\}_a)\mathbf{V}, \tag{54}$$

which is expressed in the form of a commutative diagram as in Fig. 8. Equation (54) only differs from Equation (37) in allowing boundary labels to change and the basis transformation matrix $\tilde{\mathbf{V}}$ must change accordingly.

For a given set of boundary labels (i,j,k,l), $(\tilde{i},\tilde{j},\tilde{k},\tilde{l})$, and a fixed choice of π^C (which fixes $\mathbf{\Pi}$), any solution $(\mathbf{\Pi}', \{\varphi(a)\}_a, \{\varphi'(a)\}_a)$ of (54) has phases $\{\varphi(a)\}_a$ of the "universal" form

$$\varphi(a) = \eta + f(a) \qquad \text{for all } a \in Q(i,j,k,l), \tag{55}$$

where $\eta \in [0, 2\pi)$ is an arbitrary global phase independent of a, and f belongs to a set $\mathsf{Iso}\left(\begin{array}{c} i \\ j \;|\; \cdot \;|\; k \end{array} \; l \to \begin{array}{c} \tilde{i} \\ \tilde{j} \;|\; \pi^C(\cdot) \;|\; \tilde{k} \end{array} \; \tilde{l} \right)$ of functions that can be computed from (54) as discussed below.

In summary, we have shown that U acts as

$$U|a\rangle_C = e^{i\eta}e^{if(a)}|\pi^C(a)\rangle_C \qquad \text{with} \qquad f \in \mathsf{Iso}\left(\begin{array}{c} i \\ j \;|\; \cdot \;|\; k \end{array} \; l \to \begin{array}{c} \tilde{i} \\ \tilde{j} \;|\; \pi^C(\cdot) \;|\; \tilde{k} \end{array} \; \tilde{l} \right),$$

$$\tag{56}$$

and where the latter set can be determined by solving consistency relation (54).

C. Localization of phases for higher-genus surfaces

We now argue that the phases appearing in Eq. (31) of Proposition 3.2 also factorize into certain essentially local terms, similar to how the overall permutation $\vec{\pi}$ of fusion-consistent labelings decomposes into a collection $\vec{\pi} = \{\pi^C\}_{C \in \mathcal{C}}$ of permutations of labels. More precisely, we will argue that conclusion (56) can be extended to more general surfaces.

Consider a fixed DAP-decomposition C of Σ. We call a curve $C \in \mathcal{C}$ *internal* if the intersection of Σ with a ball containing C has the form of a 4-punctured sphere with boundary components C_1, C_2, C_3, C_4 consisting of curves "neighboring" C in the DAP decomposition. We call $N(C) = \{C_1, C_2, C_3, C_4\}$ the neighbors (or neighborhood) of C as illustrated in Fig. 9. Key to the following observations is that a basis vector $|\ell\rangle$ whose restriction to these neighbors is given by $\ell \upharpoonright N(C) = (\ell(C_1), \ldots, \ell(C_4))$ gets mapped under U to a vector proportional to $|\vec{\pi}(\ell)\rangle$, which assigns the labels $\vec{\pi}(\ell) \upharpoonright N(C) = (\pi^{C_1}[\ell(C_1)], \ldots, \pi^{C_4}[\ell(C_4)])$ to the same curves. This means that the restriction of U to this subspace satisfies similar consistency conditions as the isomorphisms between Hilbert spaces associated with the 4-punctured spheres $\Sigma(\ell \upharpoonright N(C))$ and $\Sigma(\vec{\pi}(\ell) \upharpoonright N(C))$ studied in Section V A. In particular, for a fixed labeling ℓ, the dependence of the phase $\varphi(\ell)$ on the label $\ell(C)$ is given by a function from the set $\mathsf{Iso}\left(\begin{array}{c} i \\ j \;|\; \cdot \;|\; k \end{array} \; l \to \begin{array}{c} \tilde{i} \\ \tilde{j} \;|\; \pi^C(\cdot) \;|\; \tilde{k} \end{array} \; \tilde{l} \right)$, where $(i,j,k,l) = \ell \upharpoonright N(C)$
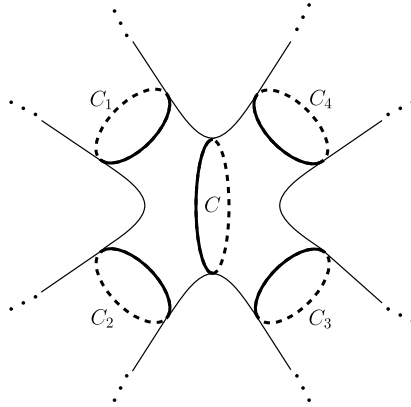
FIG. 9. For some DAP-decomposition C of a surface Σ, a curve $C \in C$ is considered internal if its neighbors $N(C) = \{C_1, C_2, C_3, C_4\}$ define the boundaries of a 4-punctured sphere.

and $(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l}) = \vec{\pi}(\ell) \upharpoonright N(C)$. In the following, we simply write $\mathsf{Iso}\left(\ell \upharpoonright N(C) \xrightarrow{\pi^C} \vec{\pi}(\ell) \upharpoonright N(C)\right)$ for this set.

Proposition 5.1 (Localization of internal phases). Let U be a locality-preserving automorphism. Let C be a DAP-decomposition of Σ, and let $\vec{\pi} = \{\pi^C\}_{C \in C}$ be the family of permutations defined by Proposition 3.1. Let $\varphi(\ell)$ for $\ell \in \mathsf{L}(C)$ be defined by (31). If $C \in C$ is internal, then

$$\varphi(\ell) = \eta(\ell \upharpoonright C \setminus \{C\}) + f_{\vec{\pi} \upharpoonright N(C)}(\ell \upharpoonright N(C), \ell(C))$$

for some functions η and f. Furthermore, we have

$$f_{\vec{\pi} \upharpoonright N(C)}(\ell \upharpoonright N(C), \cdot) \in \mathsf{Iso}\left(\ell \upharpoonright N(C) \xrightarrow{\pi^C} \vec{\pi}(\ell) \upharpoonright N(C)\right).$$

In particular, the dependence of $\varphi(\ell)$ on $\ell(C)$ is "local" and "controlled" by the labeling $\ell \upharpoonright N(C)$ of the neighbors.

In other words, if we fix a family of permutations $\vec{\pi}$, and the labels on the neighbors $N(C)$, then the dependence on the label $\ell(C)$ of the internal edge is essentially fixed.

Proof. We will focus our attention on the subspace $\mathcal{H}_{(i,j,k,l,\star)} \subseteq \mathcal{H}_\Sigma$ spanned by labelings ℓ with $(\ell(C_1), \ell(C_2), \ell(C_3), \ell(C_4)) = (i, j, k, l)$ and $\ell \upharpoonright C \setminus \{C, C_1, C_2, C_3, C_4\} = \star$ fixed (arbitrarily). For the purpose of this proof, it will be convenient to represent basis vectors $|\ell\rangle$ associated with such a labeling $\ell \in \mathsf{L}(C)$ as a vector

$$|\ell\rangle = |\ell(C), \ell(C_1), \ell(C_2), \ell(C_3), \ell(C_4), \star\rangle = |a, i, j, k, l, \star\rangle.$$

Defining $\tilde{\imath} = \pi^{C_1}(i)$, $\tilde{\jmath} = \pi^{C_2}(j)$, $\tilde{k} = \pi^{C_3}(k)$, $\tilde{l} = \pi^{C_4}(l)$, we can rewrite (31) in the form

$$U|a, i, j, k, l, \star\rangle = \mathrm{e}^{\mathrm{i}\varphi(a,i,j,k,l,\star)}|\pi^C(a), \tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l}, \tilde{\star}\rangle,$$

where $\tilde{\star} = \vec{\pi}_\upharpoonright(\star)$ for some map $\vec{\pi}_\upharpoonright$ taking labelings of the set $C \setminus \{C, C_1, C_2, C_3, C_4\}$ consistent with (i, j, k, l) to those consistent with $(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l})$. We conclude that the restriction of U to $\mathcal{H}_{(i,j,k,l,\star)}$ implements an isomorphism $\mathcal{H}_{(i,j,k,l,\star)} \cong \mathcal{H}_{(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l}, \tilde{\star})}$. Since these spaces are isomorphic to $\mathcal{H}_{\Sigma(i,j,k,l)}$ and $\mathcal{H}_{\Sigma(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l})}$, respectively, we can apply the result of Section V B. Indeed, the consistency relation imposed by the F-move is entirely local, not affecting labels associated with curves not belonging to $\{C, C_1, C_2, C_3, C_4\}$. We conclude from (56) that

$$\varphi(a, i, j, k, l, \star) = \eta(i, j, k, l, \star) + f(a), \text{ where } f \in \mathsf{Iso}\left(\begin{array}{c} i \\ j \mid \quad \cdot \quad \mid k \\ l \end{array} \rightarrow \begin{array}{c} \tilde{\imath} \\ \tilde{\jmath} \mid \pi^C(\cdot) \mid \tilde{k} \\ \tilde{l} \end{array} \right).$$

Since $(a, i, j, k, l, \star)$ were arbitrary, this proves the claim. $\square$

For example, for $S^2(z^{N+3})$ (as described above), we can apply Proposition 5.1 to the jth internal edge C_j to obtain

$$\varphi(x) = \eta_j(x_1, \ldots, \widehat{x}_j, \ldots, x_N) + f_j(x_{j-1}, x_j, x_{j+1}), \tag{57}$$

where

$$f_j(x_{j-1}, \cdot, x_{j+1}) \in \mathsf{Iso}\left(\underset{x_{j-1}|}{\overset{z}{\rule{0pt}{0pt}}} \quad \cdot \quad \underset{|x_{j+1}}{\overset{z}{\rule{0pt}{0pt}}} \to \quad \underset{\tilde{x}_{j-1}|}{\overset{z}{\rule{0pt}{0pt}}} \pi^{C_j}(\cdot) \underset{|\tilde{x}_{j+1}}{\overset{z}{\rule{0pt}{0pt}}} \right)$$

and

$$\tilde{x}_{j-1} = \pi^{C_{j-1}}(x_{j-1}), \qquad \tilde{x}_{j+1} = \pi^{C_{j+1}}(x_{j+1}).$$

Here, we use $\hat{x}_j$ to indicate that this argument is omitted.

D. Characterizing protected gates on the *M*-punctured sphere using *F*-moves

The results in this section give the following procedure for characterizing protected gates associated with $\mathcal{H}_{S^2(z^M)}$, the Hilbert space of $M = N + 3$ anyons of type z. We know from Proposition 3.2 that the action $U|\ell\rangle = e^{i\varphi(\ell)}|\vec{\pi}(\ell)\rangle$ on fusion-consistent labelings is parametrized by certain families $\vec{\pi} = \{\pi^C\}_{C \in \mathcal{C}}$ of permutations, as well as a function φ describing the phase-dependence. To characterize the latter, we have the following:

(i)   Determine the set of allowed "local" permutations π^C and associated phases f for any occurring internal curve C. This amounts to solving consistency equation (54) for the four-punctured sphere, with appropriate boundary labels. For the standard pants decomposition of the $N + 3$-punctured sphere, this means finding all pairs

$$\left(\pi^{C_j}, f_j\right) \qquad \text{where } f_j \in \mathsf{Iso}\left(\underset{x_{j-1}|}{\overset{z}{\rule{0pt}{0pt}}} \quad \cdot \quad \underset{|x_{j+1}}{\overset{z}{\rule{0pt}{0pt}}} \to \quad \underset{\tilde{x}_{j-1}|}{\overset{z}{\rule{0pt}{0pt}}} \pi^{C_j}(\cdot) \underset{|\tilde{x}_{j+1}}{\overset{z}{\rule{0pt}{0pt}}} \right).$$

These correspond to isomorphisms between the Hilbert spaces associated with the labeled surfaces $S^2(z, x_{j-1}, x_{j+1}, z)$ and $S^2(z, \tilde{x}_{j-1}, \tilde{x}_{j+1}, z)$, where $x_{j-1}, \tilde{x}_{j-1} \in Q(j - 1), x_{j+1}, \tilde{x}_{j+1} \in Q(j + 1)$.

(ii) We constrain the family $\vec{\pi} = \{\pi^C\}_{C \in \mathcal{C}}$ of allowed permutations by using the global constraints arising from fusion rules and gluing (Proposition 3.3). In the case of $N + 3$ Fibonacci anyons on the sphere with standard pants decomposition $\mathcal{C}$, dimensional arguments show that all $\pi^{C_j} = \mathsf{id}$ are equal to the identity permutation. For Ising anyons, the fusion rules imply that every permutation with even index is equal to the identity permutation, $\pi^{C_{2j}} = \mathsf{id}$ (in fact, there is only a single allowed label).

(iii) We determine the phases $\varphi(\ell)$ by using the localization property of Proposition 5.1 for internal curves C. For $N + 3$ anyons of type z on the sphere, this results in the consistency conditions

$$\varphi(x) = \eta_j(x_1, \ldots, \widehat{x}_j, \ldots, x_N) + f_j(x_{j-1}, x_j, x_{j+1}), \qquad \text{where}$$

$$f_j(x_{j-1}, \cdot, x_{j+1}) \in \mathsf{Iso}\left(\underset{x_{j-1}|}{\overset{z}{\rule{0pt}{0pt}}} \quad \cdot \quad \underset{|x_{j+1}}{\overset{z}{\rule{0pt}{0pt}}} \to \quad \underset{\tilde{x}_{j-1}|}{\overset{z}{\rule{0pt}{0pt}}} \pi^{C_j}(\cdot) \underset{|\tilde{x}_{j+1}}{\overset{z}{\rule{0pt}{0pt}}} \right) \qquad \text{for } j = 1, \ldots, N. \tag{58}$$

In Section VI B, we apply this procedure to Ising anyons; in this case, system of Equations (58) can be solved explicitly.

VI. THE FIBONACCI AND ISING MODELS

In what follows, we apply the results of Secs. III–V to the Fibonacci and Ising models. These can be considered as representative examples of non-abelian anyon models. We illustrate the use of the developed constraints in different scenarios.

In Section VI A 1, we show that there is no non-trivial gate for the Fibonacci model on the torus. This derivation uses the characterization of protected gates in terms of matrices intertwining with the mapping class group representation obtained in Section IV A. Note that we cannot apply Corollary 4.2 because the representation of the mapping class group on the torus is finite for the Fibonacci model.

In Section VI A 2, we then consider a system with M Fibonacci anyons (where $M \geq 4$ so that the space $\mathcal{H}_{S^2(\tau^M)}$ has non-zero dimension). We establish the following statement:

Theorem 6.1 (Fibonacci anyon model). *For $M \geq 4$, any locality-preserving automorphism U on the M-punctured sphere $S^2(\tau^M)$ is trivial (i.e., proportional to the identity).*

This proof is a direct consequence of Corollary 4.2 and the known density of braiding.[21,20] We additionally provide an independent proof not relying on this result.

Finally, we consider systems with M Ising anyons; the associated Hilbert space $\mathcal{H}_{S^2(\sigma^M)}$ has non-zero dimension if and only if $M \geq 4$ is even. In this case, there is a natural isomorphism $\mathcal{H}_{S^2(\sigma^M)} \cong (\mathbb{C}^2)^{\otimes M/2-1}$ (described below, see Eq. (64)). Defining the $(M/2 - 1)$-qubit Pauli group on the latter space in the usual way, we get the following statement:

Theorem 6.2 (Ising anyon model). *Any locality-preserving automorphism U of $S^2(\sigma^M)$, where $M \geq 4$ is even, belongs to the $(M/2 - 1)$-qubit Pauli group.*

Our derivation of this result relies on the use of F-moves, as discussed in Section V.

A. The Fibonacci model

For the Fibonacci model, we have $\mathbb{A} = \{1, \tau\}$ and the only non-trivial fusion rule is $\tau \times \tau = 1 + \tau$ with $d_\tau = \phi = (1 + \sqrt{5})/2$.

1. On the torus

We first consider the torus Σ and show that every protected gate is trivial. We do so by computing some of the sets Δ_ϑ, $\vartheta \in \mathsf{MCG}_\Sigma$ defined in Section IV A. Recall (see Section II F) that the mapping class group of the torus is generated by two elements s, t.

The matrix $\mathbf{V}(s) = S$ representing s is the usual S-matrix (expressed with respect to the ordering $(1, \tau)$)

$$S = \frac{1}{\sqrt{\phi + 2}} \begin{pmatrix} 1 & \phi \\ \phi & -1 \end{pmatrix}.$$

In particular, consistency condition (39) becomes

$$S \mathbf{\Pi} D S^{-1} \in \Delta,$$

where $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_\tau)$ and $\lambda_a \in \mathrm{U}(1)$. We consider the two cases:

1. For $\mathbf{\Pi} = I$, we get (using $\phi^2 = \phi + 1$)

$$S \mathbf{\Pi} D S^{-1} = \frac{1}{\phi + 2} \begin{pmatrix} \lambda_1 + \lambda_\tau(\phi + 1) & (\lambda_1 - \lambda_\tau)\phi \\ (\lambda_1 - \lambda_\tau)\phi & \lambda_1(\phi + 1) + \lambda_\tau \end{pmatrix}.$$

For this to be a unitary monomial matrix, all entries must have modulus 0 or 1. Since $\phi/(\phi + 2) < 1/2$, the off-diagonal elements always have modulus less than 1, and hence must be zero. That is, we must have $\lambda_1 = \lambda_\tau =: \lambda$, and it follows that the right hand side is in Δ. This implies that $\mathbf{\Pi} D = \lambda I$.

2. For $\mathbf{\Pi} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we get

$$S \mathbf{\Pi} D S^{-1} = \frac{1}{\phi + 2} \begin{pmatrix} (\lambda_1 + \lambda_\tau)\phi & \lambda_1(\phi + 1) - \lambda_\tau \\ \lambda_\tau(\phi + 1) - \lambda_1 & -(\lambda_1 + \lambda_\tau)\phi \end{pmatrix}.$$

To have the absolute value of the first entry equal to 0 (see above), we must have $\lambda_\tau = -\lambda_1$ and we get

$$S\mathbf{\Pi D}S^{-1} = \lambda_1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

which is a unitary monomial matrix. That is, we have $\mathbf{\Pi D} = \lambda \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Summarizing, we conclude that

$$\Delta_s = \left\{ \lambda I, \lambda \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \middle| \lambda \in \mathrm{U}(1) \right\}. \tag{59}$$

The element $t \in \mathsf{MCG}_\Sigma$ defined by twisting along one of the homologically non-trivial cycles is represented by the matrix $\mathbf{V}(t) = T = \mathrm{diag}(1, e^{4\pi i/5})$. We consider consistency condition (39) for the composition $st \in \mathsf{MCG}_\Sigma$,

$$(ST)\mathbf{\Pi D}(ST)^{-1} \in \Delta,$$

where $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_\tau)$ and $\lambda_a \in \mathrm{U}(1)$. Again, we consider the following two cases:

1. For $\mathbf{\Pi} = I$, we get

$$(ST)\mathbf{\Pi D}(ST)^{-1} = \frac{1}{\phi + 2} \begin{pmatrix} \lambda_1 + \lambda_\tau(\phi + 1) & (\lambda_1 - \lambda_\tau)\phi \\ (\lambda_1 - \lambda_\tau)\phi & \lambda_1(\phi + 1) + \lambda_\tau \end{pmatrix}.$$

This is identical to the first case above; thus, $\mathbf{\Pi D} = \lambda I$.

2. For $\mathbf{\Pi} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we get

$$(ST)\mathbf{\Pi D}(ST)^{-1} = \frac{\zeta}{\phi + 2} \begin{pmatrix} (\zeta^3 \lambda_1 - \lambda_\tau)\phi & \zeta^3 \lambda_1(\phi + 1) + \lambda_\tau \\ -\zeta^3 \lambda_1 - \lambda_\tau(\phi + 1) & -(\zeta^3 \lambda_1 - \lambda_\tau)\phi \end{pmatrix},$$

where $\zeta = e^{i\pi/5}$. Since $\phi/(\phi + 2) < 1/2$, the diagonal elements must vanish, that is, we have $\lambda_\tau = \zeta^3 \lambda_1$. This indeed then gives an element of Δ, and $\mathbf{\Pi D} = \lambda \begin{pmatrix} 0 & e^{3\pi i/5} \\ 1 & 0 \end{pmatrix}$.

In summary, we have shown that

$$\Delta_{st} = \left\{ \lambda I, \lambda \begin{pmatrix} 0 & e^{3\pi i/5} \\ 1 & 0 \end{pmatrix} \middle| \lambda \in \mathrm{U}(1) \right\}. \tag{60}$$

Combining (59) and (60), we conclude that

$$\Delta_s \cap \Delta_{st} = \left\{ \lambda I \mid \lambda \in \mathrm{U}(1) \right\},$$

and this means that $\Delta_{\mathsf{MCG}_\Sigma} \subset \Delta_s \cap \Delta_{st} = \{ \lambda I \mid \lambda \in \mathrm{U}(1) \}$. According to Theorem 4.1, this implies that there is no non-trivial protected gate on the torus.

Note that this conclusion is consistent with the form of a Dehn twist, given by the logical unitary $U = \mathrm{diag}(1, e^{4\pi i/5})$ (with the "topological" phases or twists on the diagonal): Dehn twists do *not* preserve locality! For example, for a Dehn twist along C_1, an operator supported on C_2 may end up with support in the neighborhood of the union $C_1 \cup C_2$ under conjugation by the unitary realizing the Dehn twist.

2. On the M-punctured sphere

We now provide a proof of Theorem 6.1. As already mentioned, braiding of $M \geq 4$ Fibonacci anyons is known to be universal;[21,20] hence, we could invoke Corollary 4.2. Instead, we give a different proof by exploiting the equivalence relation introduced in Section IV C and analyzing the

dimension of the associated spaces (i.e., using the constraints arising from the gluing postulate, see Section III B).

Consider the M-punctured sphere $\Sigma = S^2(\tau^M)$ corresponding to M Fibonacci anyons. We will use as our "standard" basis the one arising from the standard DAP decomposition C of the M-punctured sphere introduced in Section II E (see Fig. 5). We then have the following statement:

Lemma 6.3. There is only one equivalence class under the relation $\sim$. Furthermore, the set of braids $\{\sigma_j\}_{j=1}^{M-1}$ generates the relation $\sim$.

Proof. Let x and x' be two fusion-consistent labelings that are related by interchanging $\tau = x_j$ and $1 = x'_j$ (or vice versa) in the jth entry (but are otherwise the same). Fusion-consistency implies that $x_{j-1} = x'_{j-1} = x_{j+1} = x'_{j+1} = \tau$. In particular, the relevant braid matrix describing the action of $V(\sigma_j)$ is $B(\tau, \tau)$ which has non-zero entries everywhere. We conclude that

$$\langle x'|V(\sigma_j)|x\rangle \neq 0 \qquad \text{and} \qquad \langle x'|V(\sigma_j)|x'\rangle \neq 0 \ .$$

This implies that $x \Leftrightarrow_{\sigma_j} x'$. Since any fusion-consistent labeling can be obtained from the sequence $\tau^N = (\tau, \ldots, \tau)$ by such interchanges, we conclude that any two fusion-consistent labelings are equivalent. That is, there is only one equivalence class under $\sim$. $\qquad\square$

We will now argue that the conditions of Lemma 4.3 (ii) apply in this situation, that is, any protected gate U acts diagonally in any of the bases $\mathcal{B}_{\sigma_j(C)}$ obtained from the standard DAP-decomposition by applying a braid group generator σ_j. In fact, we will argue more generally that U acts diagonally in any basis defined by a DAP-decomposition.

To do so, consider first the standard DAP-decomposition and the spaces $\mathcal{H}_{\Sigma'_j(a,a)}$ for $j \in \{1, \ldots, M - 3\}$ and $a \in \{1, \tau\}$ (cf. (21)), where Σ'_j is obtained from Σ by cutting along the curve C_j which leaves a $j + 2$-punctured and a $(M - j)$-punctured sphere, respectively. Note that τ is its own antiparticle ($\bar{\tau} = \tau$), and hence it suffices to consider $\Sigma'_j(\tau, \tau)$ and $\Sigma'_j(1, 1)$. Our goal is to identify pairs $(a, \tilde{a})$ such that $\mathcal{H}_{\Sigma'_j(a,a)} \cong \mathcal{H}_{\Sigma'_j(\tilde{a}, \tilde{a})}$ are isomorphic, this being a necessary condition for a permutation satisfying $\pi^{C_j}(a) = \tilde{a}$ (see Proposition 3.3 and Eq. (35)). To compute $\dim \mathcal{H}_{\Sigma'_j(a,a)}$ for $a \in \{1, \tau\}$, we make use of the general fact that $\dim \mathcal{H}_{S^2(\tau^M)} = \Phi_{M-1}$ where Φ_M denotes the Mth Fibonacci number, starting with $\Phi_0 = 0$ and $\Phi_1 = 1$ and satisfying the recurrence relation $\Phi_{M+1} = \Phi_M + \Phi_{M-1}$. From (21), we obtain $\dim \mathcal{H}_{\Sigma'_j(1,1)} = \Phi_j \Phi_{M-j-2}$ and $\dim \mathcal{H}_{\Sigma'_j(\tau,\tau)} = \Phi_{j+1} \Phi_{M-j-1}$, excluding the case $j = 1 = M - 3$ which satisfies $\dim \mathcal{H}_{\Sigma'_1(1,1)} = \Phi_1 \Phi_{M-3} = \dim \mathcal{H}_{\Sigma'_{M-3}(1,1)}$ and $\dim \mathcal{H}_{\Sigma'_1(\tau,\tau)} = \Phi_2 \Phi_{M-2} = \dim \mathcal{H}_{\Sigma'_{M-3}(\tau,\tau)}$, it follows from the monotonicity and positivity of Φ that

$$\dim \mathcal{H}_{\Sigma'_j(1,1)} < \dim \mathcal{H}_{\Sigma'_j(\tau,\tau)} \qquad \text{for } M > 4, \text{ and all } j \in \{1, \ldots, M - 3\}. \tag{61}$$

Hence, according to consistency condition (35), for $M > 4$, we only get an isomorphism $\mathcal{H}_{\Sigma'(a,\bar{a})} \cong \mathcal{H}_{\Sigma'(\pi^C(a), \overline{\pi^C(a)})}$ with $\pi^C = \mathsf{id}$ being trivial for any internal loop C in a standard DAP decomposition. This shows that a protected gate acts diagonally in the standard basis.

Observe that this argument only involved the dimensions of the fusion spaces obtained by cutting along a curve C_j in the pants decomposition. Since it is generally true that cutting along a curve will decompose the M-punctured sphere into a $j + 2$-punctured and a $(M - j)$-punctured sphere, respectively (for some j), the argument extends to arbitrary DAP-decompositions. In particular, U is diagonal with respect to each of the bases $\mathcal{B}_{\sigma_j(C)}$, as claimed.

We have shown that the conditions of Lemma 4.3 apply. With Lemma 6.3, Theorem 6.1 is immediate.

B. The Ising model

The Ising anyon model has label set $\mathbb{A} = \{1, \psi, \sigma\}$ and non-trivial fusion rules

$$\psi \times \psi = 1, \ \psi \times \sigma = \sigma, \ \sigma \times \sigma = 1 + \psi.$$

1. On the 4-punctured sphere

Consider the possible spaces $\mathcal{H}_{S^2(\sigma,j,k,\sigma)}$ for $\{j,k\} \in \mathbb{A}$, and observe that fusion consistency implies

$$
\dim \mathcal{H}_{S^2(\sigma,j,k,\sigma)} = \begin{cases} 0 & \text{if } j \neq k = \sigma \text{ or } k \neq j = \sigma, \\ 1 & \text{if } j,k \in \{1,\psi\}, \\ 2 & \text{if } j = k = \sigma. \end{cases}
$$

Therefore, the only nontrivial case to consider is $\mathcal{H}_{S^2(\sigma,\sigma,\sigma,\sigma)} = \mathcal{H}_{S^2(\sigma^4)}$ with an ordered basis $\{|1\rangle, |\psi\rangle\}$. A locality-preserving automorphism of $\mathcal{H}_{S^2(\sigma^4)}$ will act as

$$
U|a\rangle = e^{i\eta} e^{if(a)} |\pi^C(a)\rangle, \quad \text{where } f \in \mathsf{Iso}\left(\begin{array}{c} \sigma \\ \sigma \; | \quad \cdot \quad | \; \sigma \end{array} \rightarrow \begin{array}{c} \sigma \quad \sigma \\ \sigma \; | \; \pi^C(\cdot) \; | \; \sigma \end{array} \right).
$$

A valid permutation π^C of $\{1,\psi\}$ that defines the action of U and the set of phases can be determined as follows. Let $\mathcal{B}_C = \{|1\rangle_C, |\psi\rangle_C\}$ and $\mathcal{B}_{C'} = \{|1\rangle_{C'}, |\psi\rangle_{C'}\}$ be the corresponding ordered bases of $\mathcal{H}_{S^2(\sigma^4)}$ for the two DAP-decomposition C and C', respectively. The F-matrix relating these two bases is given in the ordered basis $\mathcal{B}_C$ as

$$
F = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.
$$

Now consider some locality-preserving automorphism U expressed in the bases $\mathcal{B}_C$ and $\mathcal{B}_{C'}$ as $\mathbf{U} = \mathbf{\Pi D}$ and $\mathbf{U}' = \mathbf{\Pi' D'}$, respectively, for some 2×2 permutation matrices $\mathbf{\Pi}, \mathbf{\Pi}'$ and diagonal matrices $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_\psi)$ and $\mathbf{D}' = \mathrm{diag}(\lambda'_1, \lambda'_\psi)$ with phases $\lambda_a, \lambda'_a \in U(1)$. Then, the consistency relation takes the form $\mathbf{U}' = F\mathbf{U}F^{-1}$. Next, we find all consistent solutions for a given permutation $\mathbf{\Pi}$.

1. For $\mathbf{\Pi} = I$, we get

$$
F\mathbf{\Pi D}F^{-1} = \frac{1}{2} \begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ \lambda_1 - \lambda_\psi & \lambda_1 + \lambda_\psi \end{pmatrix} = \mathbf{\Pi' D'}. \tag{62}
$$

Suppose that $\mathbf{\Pi}' = I$. Then, the consistency relation (62) becomes

$$
\frac{1}{2} \begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ \lambda_1 - \lambda_\psi & \lambda_1 + \lambda_\psi \end{pmatrix} = \begin{pmatrix} \lambda'_1 & 0 \\ 0 & \lambda'_\psi \end{pmatrix},
$$

which implies $\lambda_1 = \lambda_\psi = \lambda'_1 = \lambda'_\psi =: e^{i\eta}$. Therefore, U expressed in the basis $\mathcal{B}_C$ is trivial up to a global phase,

$$
\mathbf{U} = e^{i\eta} I.
$$

Suppose instead that $\mathbf{\Pi}' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Consistency relation (62) then becomes

$$
\frac{1}{2} \begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ \lambda_1 - \lambda_\psi & \lambda_1 + \lambda_\psi \end{pmatrix} = \begin{pmatrix} 0 & \lambda'_\psi \\ \lambda'_1 & 0 \end{pmatrix},
$$

which implies $\lambda_1 = -\lambda_\psi$ and $\lambda'_1 = \lambda'_\psi = \lambda_1$. Setting $e^{i\eta} := \lambda_1$ implies that U expressed in the basis $\mathcal{B}_C$ is given by

$$
\mathbf{U} = e^{i\eta} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
$$

These two solutions of the consistency relation, for the case $\mathbf{\Pi} = I$, now determine the only two functions of the set

$$
\mathsf{Iso}\left(\begin{array}{c} \sigma \quad \sigma \\ \sigma \; | \quad \cdot \quad | \; \sigma \end{array} \rightarrow \begin{array}{c} \sigma \quad \sigma \\ \sigma \; | \; \mathrm{id}(\cdot) \; | \; \sigma \end{array} \right) = \{(f(1), f(\psi))\} = \{(0,0), (0,\pi)\}.
$$

2. For $\mathbf{\Pi} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, corresponding to the transposition $(\psi, 1)$, we get

$$F\mathbf{\Pi}DF^{-1} = \frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ -\lambda_1 + \lambda_\psi & -\lambda_1 - \lambda_\psi \end{pmatrix} = \mathbf{\Pi}'\mathbf{D}'. \tag{63}$$

By taking $\mathbf{\Pi}' = I$, this becomes

$$\frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ -\lambda_1 + \lambda_\psi & -\lambda_1 - \lambda_\psi \end{pmatrix} = \begin{pmatrix} \lambda_1' & 0 \\ 0 & \lambda_\psi' \end{pmatrix},$$

which implies $\lambda_1 = \lambda_\psi = \lambda_1' = -\lambda_\psi'$. Letting $e^{i\eta} := \lambda_1$ allows U to be expressed in the basis $\mathcal{B}_C$ by

$$\mathbf{U} = e^{i\eta}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Instead, suppose now that $\mathbf{\Pi}' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then, consistency relation (63) is of the form

$$\frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ -\lambda_1 + \lambda_\psi & -\lambda_1 - \lambda_\psi \end{pmatrix} = \begin{pmatrix} 0 & \lambda_\psi' \\ \lambda_1' & 0 \end{pmatrix},$$

implying that $\lambda_1 = -\lambda_\psi = -\lambda_1' = \lambda_\psi'$. Let $e^{i\eta} := \lambda_1$, then this shows that U expressed in the basis $\mathcal{B}_C$ is given by

$$\mathbf{U} = e^{i\eta}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Furthermore, these two solutions completely determine the relevant set of functions (which happens to be the same as the previous case for $\mathbf{\Pi} = I$),

$$\mathsf{Iso}\left(\begin{array}{c} \sigma \quad\quad \sigma \\ \sigma\ \rule[0.3ex]{0pt}{1.5ex}|\ \ \cdot\ \ |\ \sigma \end{array} \rightarrow \begin{array}{c} \sigma \quad\quad \sigma \\ \sigma\ \rule[0.3ex]{0pt}{1.5ex}|\ (\psi,1)(\cdot)|\ \sigma \end{array} \right) = \{(f(1), f(\psi))\} = \{(0,0),(0,\pi)\}.$$

By denoting the single qubit (logical) Pauli group as

$$\mathcal{P} := \left\{ \lambda\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \lambda\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \lambda\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \lambda\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \middle| \lambda \in \mathrm{U}(1) \right\},$$

these results can be summarized as follows: If U is a locality-preserving automorphism of the fusion space $\mathcal{H}_{S^2(\sigma^4)}$ of the 4-punctured sphere, then U expressed in the basis $\mathcal{B}_C$ is in $\mathcal{P}$.

2. On the M-punctured sphere

Let $M \geq 4$ and consider the $M = N + 3$-punctured sphere $S^2(\sigma^M)$ and corresponding space $\mathcal{H}_{S^2(\sigma^M)}$. For the "standard" DAP-decomposition C of $S^2(\sigma^M)$, a consistent labeling $\mathsf{L}(C)$ corresponds to a sequence $(\ell(C_1), \ldots, \ell(C_N)) =: (x_1, \ldots, x_N) =: x$. It is readily observed that $\dim \mathcal{H}_{S^2(\sigma^M)} = 0$ if M is odd, as there are no consistent labelings in this case.

Therefore, in what follows we will restrict our discussion to the $M = N + 3$-punctured sphere where N is any odd positive integer. In this case, any consistent labeling $\ell \in \mathsf{L}(C)$ yields a sequence $(x_1, \ldots, x_N)$ where $x_i \in \{1, \psi\}$ for odd i and $x_i = \sigma$ is fixed for even i. Actually any such labeling of this form is consistent, giving an isomorphism defined in terms of orthonormal basis elements by

$$\begin{aligned} W : \mathcal{H}_{S^2(\sigma^{N+3})} &\rightarrow (\mathbb{C}^2)^{(N+1)/2}, \\ |x\rangle &\mapsto |x_1\rangle \otimes |x_3\rangle \otimes \cdots \otimes |x_N\rangle. \end{aligned} \tag{64}$$

Lemma 6.4. Consider the "standard" basis of the M-punctured sphere $S^2(\sigma^M)$, where $M \geq 4$ is even. Then there is only one equivalence class under the relation $\sim$. Furthermore, the set of braids $\{\sigma_j\}_{j=1}^{M-1}$ generates the relation $\sim$.

Proof. If two fusion-consistent labelings x, x' differ only in location $2j+1$, they can be connected by σ_{2j+1}: the relevant braid matrix is

$$B(\sigma,\sigma) = \frac{e^{-3\pi i/8}}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}.$$

We have $x \Leftrightarrow_{\sigma_{2j+1}} x'$, and it follows that there is only one equivalence class under $\sim$. $\qquad\square$

Now consider a locality-preserving automorphism U of $\mathcal{H}_{S^2(\sigma^{N+3})}$ and its associated family $\vec{\pi} = \{\pi^{C_j}\}$ of permutations. Because only sequences x with $x_{2j} = \sigma$ for all j are fusion-consistent, and $\vec{\pi}$ is a permutation on $\mathsf{L}(C)$, we conclude that $\pi^{C_{2j}}(\sigma) = \sigma$ for all j. In other words, we can essentially ignore labels carrying even indices. For odd indices, only labels $x_{2j+1} \in \{1,\psi\}$ are allowed, which means that $\pi^{C_{2j+1}} \in \{\mathsf{id}, (\psi,1)\}$ either leaves the label invariant or interchanges ψ and 1. In conclusion, $\vec{\pi} = \{\pi^{C_j}\}_{j=1}^N$ are of the form $\pi^{C_j} \in \{\mathsf{id}, (\psi,1)\}$ for odd j, and $\pi^{C_j} = \mathsf{id}$ for even j.

For odd $j = 2k+1$, we obtain the constraint

$$\varphi(x) = \eta_{2k+1}(x_1,\ldots,\widehat{x_{2k+1}},\ldots,x_N) + f_{2k+1}(x_{2k+1}) \qquad \text{for } k = 0,\ldots,(N-1)/2,$$

where $f_{2k+1} \in \mathsf{Iso}\left(\begin{array}{c} \sigma \\ \sigma \;|\; \cdot \;|\; \sigma \end{array} \rightarrow \begin{array}{c} \sigma \qquad \sigma \\ \sigma \;|\; \pi^{C_{2k+1}}(\cdot) \;|\; \sigma \end{array} \right)$ given that for even labels $\pi^{C_{2m}}$ $(x_{2m}) = x_{2m} = \sigma$. Let us write

$$\varphi(x) = \eta(x) + \sum_{m=0}^{(N+1)/2} f_{2m+1}(x_{2m+1}) \tag{65}$$

and show that $\eta(x) = \eta$ is actually independent of the labeling x. Indeed, we can write

$$\eta(x) = \left(\varphi(x) - f_{2k+1}(x_{2k+1})\right) - \sum_{m,m\neq k}^{(N+1)/2} f_{2m+1}(x_{2m+1})$$

$$= \eta_{2k+1}(x_1,\ldots,\widehat{x_{2k+1}},\ldots,x_N) - \sum_{m,m\neq k}^{(N+1)/2} f_{2m+1}(x_{2m+1}).$$

Since this holds for all k, we conclude that $\eta(x) = \eta(\widehat{x_1},x_2,\widehat{x_3},x_4,\ldots)$ is a function of the even entries only. But the latter are all fixed as $x_{2m} = \sigma$, and hence $\eta(x) = \eta$ is simply a global phase.

We can now combine these results into a general statement concerning locality-preserving automorphisms of the M-punctured sphere $S^2(\sigma^M)$. Again, since $\dim \mathcal{H}_{S^2(\sigma^M)} = 0$ for odd M and $\dim \mathcal{H}_{S^2(\sigma^2)} = 1$, we are only concerned with the cases where $M = N + 3 \geq 4$ is even. Let $\{|x\rangle\}_{x \in \mathsf{L}(C)}$ be a basis of $\mathcal{H}_{S^2(\sigma^M)}$. Then such an automorphism must act on $\mathcal{H}_{S^2(\sigma^M)}$ as

$$U|x\rangle = e^{i\varphi(x)}|\vec{\pi}(x)\rangle, \qquad \text{where} \qquad \varphi(x) = \eta + \sum_{m=0}^{(N+1)/2} f_{2m+1}(x_{2m+1})$$

and

$$f_{2k+1} \in \mathsf{Iso}\left(\begin{array}{c} \sigma \qquad \sigma \\ \sigma \;|\; \cdot \;|\; \sigma \end{array} \rightarrow \begin{array}{c} \sigma \qquad \sigma \\ \sigma \;|\; \pi^{C_{2k+1}}(\cdot) \;|\; \sigma \end{array} \right) = \{(f(1), f(\psi))\} = \{(0,0),(0,\pi)\}.$$

More explicitly, we have

$$U|x\rangle = e^{i\eta}\left(\prod_{m=1}^{(N+1)/2} e^{if_{2m+1}(x_{2m+1})} \right) |\pi^{C_1}(x_1), x_2, \pi^{C_3}(x_3), x_4, \ldots, \pi^{C_N}(x_N)\rangle.$$

In particular, under isomorphism (64), we get

$$WUW^{-1} = e^{i\eta} \bigotimes_{m=1}^{(N+1)/2} U_m, \qquad \text{where} \qquad U_m|a\rangle = e^{if_{2m-1}(a)}|\pi^{C_{2m-1}}(a)\rangle.$$

From Section VI B 1, we know that U_m is a single-qubit Pauli for each m up to a global phase. This concludes the proof of Theorem 6.2.

VII. ABELIAN ANYON MODELS

Our goal in this section is to characterize topologically protected gates in general abelian anyon models. For simplicity, we will restrict our attention to closed 2-manifolds Σ (see Fig. 1). We have seen in Lemma 3.1 that in an arbitrary anyon model, protected gates permute the idempotents along closed loops. In this section, we show that for the case of abelian anyon models, the protected gates can only permute the labels of string operators along closed loops (up to phases), which refines Lemma 3.1 for abelian models. To formalize this notion, we introduce the generalized Pauli and Clifford groups in Section VII A. The main result of this section can then be stated as follows:

Theorem 7.1. *For an abelian anyon model, any locality-preserving unitary automorphism* U *acting on* $\mathcal{H}_\Sigma$ *has logical action* $[U] \in \mathsf{Clifford}^\star_\Sigma$.

For abelian anyon models, the set $\mathbb{A}$ of particles is an abelian group and the fusion rules (i.e., Verlinde algebra (7)) are given by the group product, $N^c_{ab} = 1$ if and only if $c = ab$ and $N^c_{ab} = 0$ otherwise. In other words, any two particles a and b fuse to a unique particle $c = ab$, and the identity element $1 \in \mathbb{A}$ is the only particle satisfying $1a = a$ for all $a \in \mathbb{A}$. Another requirement is that the S matrix is composed entirely of phases (divided by the quantum dimension $\mathcal{D}$), and $S_{1a} = S_{a1} = 1/\mathcal{D}$ for all $a \in \mathbb{A}$. Furthermore, the involution $a \mapsto \bar{a}$ defining the antiparticle associated to $a \in \mathbb{A}$ is simple as the inverse $\bar{a} = a^{-1}$ with respect to the group multiplication. Note that, by the fundamental theorem of finitely generated abelian groups, the group $\mathbb{A}$ is isomorphic to $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_r}$ for some prime powers N_j. The number $N = \mathsf{lcm}(N_1, \ldots, N_r)$ will play an important role in the following, determining, e.g., the order of a protected gate.

It is well known that for abelian anyons a and b, and two inequivalent loops C and C' whose intersection number is 1 in the manifold Σ the relation

$$[F_{\bar{b}}(C')][F_{\bar{a}}(C)][F_b(C')][F_a(C)] = \mathcal{D}S_{ab}[\mathsf{id}] \tag{66}$$

holds. As we will see, this provides an additional constraint on the logical action of a protected gate U. The following consistency condition must hold:

Lemma 7.2. Let C and C' be two loops on Σ which intersect once. Consider the action of a locality preserving unitary automorphism of the code on the string operators on C and C', that is,

$$\rho_U([F_b(C)]) = \sum_d \Lambda_{b,d}[F_d(C)], \qquad \rho_U([F_b(C')]) = \sum_d \Lambda'_{b,d}[F_d(C')]. \tag{67}$$

Then, the matrices Λ and Λ' must satisfy the following consistency condition:

$$\Lambda_{a,c}\, \Lambda'_{b,d}\, (S_{cd} - S_{ab}) = 0 \quad \forall a,b,c,d \in \mathbb{A}. \tag{68}$$

Proof. Since in an abelian anyon model every string operator $[F_a(C)]$ is unitary, relation (66) is equivalent to the commutation relation

$$[F_b(C')][F_a(C)] = \mathcal{D}S_{ab}[F_a(C)][F_b(C')].$$

Conjugating this by U and rearranging terms yields

$$0 = \sum_{c,d} \Lambda_{a,c}\, \Lambda'_{b,d}\, (\mathcal{D}S_{cd} - \mathcal{D}S_{ab})\, [F_c(C)][F_d(C')]. \tag{69}$$

The claim follows from linear independence of the logical operators $[F_c(C)][F_d(C')]$.   □

Invoking our previous result of Lemma 3.1, the following lemma is implied:

Lemma 7.3. The anyon labels of string *operators along the loop are permuted by U*

$$\Lambda_{b,d} = e^{i\phi_b}\delta_{d,\tilde{\pi}(b)}, \tag{70}$$

for some phase ϕ_b, and where $\tilde{\pi}$ is a permutation of anyon labels.

Proof. Recall from (29) that

$$\Lambda_{b,d} = \sum_a \frac{S_{b,a}}{S_{1,a}} S_{1,\pi^C(a)} \overline{S_{d,\pi^C(a)}} = \sum_a S_{b,a} \overline{S_{d,\pi^C(a)}}, \tag{71}$$

where π^C is the permutation of the central idempotents associated with loop C, where the second equality holds for abelian anyons. An analogous equation holds for loop C'. Now sum over all $a \in \mathbb{A}$ in (68). To evaluate the sum, we require $\sum_a \Lambda_{a,c}$ and $\sum_a \Lambda_{a,c} S_{ab}$. First,

$$\sum_a \Lambda_{a,c} = \sum_{a,g} S_{a,g} \overline{S_{c,\pi^C(g)}} = \mathcal{D} \sum_g \delta_{g,1} \overline{S_{c,\pi^C(g)}} = \mathcal{D} \overline{S_{c,\pi^C(1)}},$$

where we used unitarity of the S-matrix, $\delta_{1z} = \sum_x \overline{S_{x1}} S_{xz} = \sum_x S_{xz}/\mathcal{D}$. Second,

$$\sum_a \Lambda_{a,c} S_{ab} = \sum_{a,g} S_{a,g} \overline{S_{c,\pi^C(g)}} S_{ab} = \sum_{a,g} S_{a,g} \overline{S_{c,\pi^C(g)} S_{a\overline{b}}} = \sum_g \delta_{g,\overline{b}} \overline{S_{c,\pi^C(g)}} = \overline{S_{c,\pi^C(\overline{b})}}.$$

Therefore, (68) implies

$$\left(\mathcal{D} S_{cd} \overline{S_{c,\pi^C(1)}} - \overline{S_{c,\pi^C(\overline{b})}} \right) \Lambda'_{b,d} = 0 \qquad \forall b,c,d \in \mathbb{A}. \tag{72}$$

For any $B \in \mathbb{A}$, there must exist at least one anyon $D \in \mathbb{A}$ such that $\Lambda'_{B,D} \neq 0$. Then,

$$\mathcal{D} S_{cD} \overline{S_{c,\pi^C(1)}} - \overline{S_{c,\pi^C(\overline{B})}} = 0 \qquad \forall c \in \mathbb{A}. \tag{73}$$

For each $D' \neq D$, there must be some $C \in \mathbb{A}$ such that $S_{CD} \neq S_{CD'}$. Therefore, substituting into (72) the values $b = B, c = C$, and $d = D'$, the term in brackets must be non-zero, implying $\Lambda'_{B,D'} = 0$ for all $D' \neq D$. Unitarity of U yields the claim for loop C'. $\square$

A. The generalized Pauli and Clifford groups

Consider the case where $\mathbb{A} = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_r}$ and set $N = \mathsf{lcm}(N_1, \ldots, N_r)$. We define the following group associated with the surface Σ.

Definition 7.4 (Pauli group). Consider a genus-g surface Σ and let $\mathcal{G} = \{C_j\}_{j=1}^{3g-1}$ be the loops associated with generators of the mapping class group as in Fig. 1. The Pauli group Pauli_Σ *associated with Σ is*

$$\mathsf{Pauli}_\Sigma := \left\langle \left\{ \lambda[F_a(C)] \mid \lambda \in \langle e^{2\pi i/N} \rangle, a \in \mathbb{A}, C \in \mathcal{G} \right\} \right\rangle,$$

i.e., the set of logical operators generated by taking products of string-operators associated with $\mathcal{G}$, where $\langle e^{2\pi i/N} \rangle$ is the subgroup of $\mathrm{U}(1)$ consisting of Nth roots of unity.

According to Eq. (66), we can always reorder and write each element $P \in \mathsf{Pauli}_\Sigma$ in the standard form

$$P = \lambda[F_{a_1}(C_1)] \cdots [F_{a_{3g-1}}(C_{3g-1})] \qquad \text{for some } \lambda \in \langle e^{2\pi i/N} \rangle, \ a_j \in \mathbb{A}.$$

This shows that the group Pauli_Σ is finite. Furthermore, since $a^N = 1$ for every $a \in \mathbb{A}$, we conclude that $P^N = \lambda[\mathsf{id}]$ is proportional to the identity up to a phase $\lambda \in \langle e^{2\pi i/N} \rangle$. That is, every element of the Pauli group Pauli_Σ has order dividing N.

Given this definition, we can proceed to give the definition of the Clifford group.

Definition 7.5 (Clifford group). The Clifford group associated with Σ is the group of logical unitaries

$$\mathsf{Clifford}_\Sigma := \{ \lambda[U] \mid [U]\mathsf{Pauli}_\Sigma[U]^{-1} \subset \mathsf{Pauli}_\Sigma, \lambda \in \langle e^{2\pi i/N} \rangle \}.$$

In this definition, $[U]$ is any logical unitary on the code space.

We can define a "homology-preserving subgroup" of $\mathsf{Clifford}_\Sigma$. To do so, we first introduce the following subgroup of Pauli_Σ associated with a loop on Σ.

Definition 7.6 (Restricted Pauli group). Let $C \in \mathcal{G}$ be a single closed loop. We set

$$\mathsf{Pauli}_\Sigma(C) := \left\langle \left\{ \lambda[F_a(C)] \mid \lambda \in \langle e^{2\pi i/N} \rangle, a \in \mathbb{A} \right\} \right\rangle,$$

i.e., the subgroup generated by string-operators associated with the loop C.

It is straightforward to check that for any $C \in \mathcal{G}$, the subgroup $\mathsf{Pauli}_{\Sigma_g}(C) \subset \mathsf{Pauli}_{\Sigma_g}$ is normal; furthermore, any $P \in \mathsf{Pauli}_{\Sigma_g}(C)$ has the simple form of a product $P = \lambda[F_{a_1}(C)] \cdots [F_{a_r}(C)]$.

Given this definition, we can define a subgroup of Clifford group elements as follows:

Definition 7.7 (Homology-preserving Clifford group). The homology-preserving Clifford group associated with Σ is the subgroup

$$\mathsf{Clifford}_\Sigma^\star := \{\lambda[U] \mid [U]\mathsf{Pauli}_\Sigma(C)[U]^{-1} \subset \mathsf{Pauli}_\Sigma(C) \text{ for all } C \in \mathcal{G}, \ \lambda \in \langle e^{2\pi i/N} \rangle \}.$$

Note that this is a proper subgroup, i.e., $\mathsf{Clifford}_\Sigma^\star \subsetneq \mathsf{Clifford}_\Sigma$, as can be seen from the following example.

Example 7.8. Consider, for example, Kitaev's $D(\mathbb{Z}_2)$-code on a torus Σ_2 (cf. Example 2.1). In this case, there are two inequivalent homologically non-trivial cycles C_1 and C_2. In the language of stabilizer codes, the logical operators $(\bar{X}_1, \bar{Z}_1) = (F_e(C_1), F_m(C_2))$ and $(\bar{X}_2, \bar{Z}_2) = (F_e(C_2), F_m(C_1))$ are often referred to as the logical Pauli operators associated with the first and second logical qubits, respectively. Consider the logical Hadamard $\bar{H}_1$ on the first qubit, which acts as

$$\bar{H}_1 \bar{X}_1 \bar{H}_1^\dagger = \bar{Z}_1 \qquad and \qquad \bar{H}_1 \bar{Z}_1 \bar{H}_1^\dagger = \bar{X}_1$$

but leaves $\bar{X}_2$ and $\bar{Z}_2$ invariant. Then, $\bar{H}_1$ belongs to the Clifford group, $\bar{H}_1 \in \mathsf{Clifford}_\Sigma$. However, $\bar{H}_1 \notin \mathsf{Clifford}_\Sigma^\star$ because $\bar{X}_1$ and $\bar{Z}_1$ belong to different homology classes (specified by C_1 and C_2, respectively).

In the following, we make use of the existence of a loop C' which intersects with a given loop C exactly once. Note that this is not necessarily given, but works in the special case where C is one of the $3g - 1$ curves $\{C_j\}_{j=1}^{3g-1}$ associated with the generators of the mapping class group of the genus-g surface Σ_g (cf. Fig. 1). We are now ready to prove Theorem 7.1, i.e., that a protected gate U has logical action $[U] \in \mathsf{Clifford}_\Sigma^\star$.

Proof. By Lemma 7.3, we have that $\sum_c \Lambda_{a,c}[F_c(C)] = \lambda[F_b(C)]$ for some $\lambda \in \mathrm{U}(1)$ and $b \in \mathbb{A}$. It remains to show that λ is an Nth root of unity. We have

$$\lambda^N[\mathsf{id}] = \lambda^N[F_b(C)^N] = [\lambda F_b(C)]^N = [U][F_a(C)]^N[U^\dagger] = [\mathsf{id}]$$

because the string operators $F_a(C)$ have order dividing N, and thus we must have $\lambda^N = 1$. Because a and C were arbitrary, this concludes the proof that $[U] \in \mathsf{Clifford}_\Sigma^\star$. □

ACKNOWLEDGMENTS

APPENDIX: DENSITY ON A SUBSPACE AND PROTECTED GATES

Lemma 1.1. Let $\mathcal{H}_0$ be an invariant subspace under the mapping class group representation, and suppose the action of MCG_Σ is dense in the projective unitary group $\mathsf{PU}(\mathcal{H}_0)$. Let $\mathcal{H}_1$ be the orthogonal complement of $\mathcal{H}_0$ in $\mathcal{H}_\Sigma$. Assume that the decomposition $\mathcal{H}_0 \oplus \mathcal{H}_1$ stems from the gluing postulate in the sense that $\mathcal{H}_j = \bigoplus_{\vec{a} \in \Lambda_j} \mathcal{H}_{\Sigma'(\vec{a})}$ for $j = 0, 1$, where Λ_0, Λ_1 are disjoint set of labelings of the boundary components of the surface Σ' obtained by cutting Σ along a family $\vec{C}$ of pairwise non-intersecting curves. If $\dim \mathcal{H}_1 < \dim \mathcal{H}_0$ (or a similar assumption), then any protected gate U leaves $\mathcal{H}_0$ invariant and acts as a global phase on it.

Proof. Extending $\vec{C}$ to a DAP-decomposition $\mathcal{C}$, the unitary U expressed in the (suitably ordered) basis $\mathcal{B}_\mathcal{C}$ takes the form

$$
\mathbf{U} = \begin{pmatrix} \mathbf{U}_{00} & \mathbf{U}_{01} \\ \mathbf{U}_{10} & \mathbf{U}_{11} \end{pmatrix},
$$

where $\mathbf{U}_{jk}$ describes the operator $P_{\mathcal{H}_j} U P_{\mathcal{H}_k}$ obtained by projecting the domain and image of U to $\mathcal{H}_k$ and $\mathcal{H}_j$, respectively.

Consider the Schur decomposition $\mathbf{U}_{00} = \mathbf{W}_{00} \Gamma \mathbf{W}_{00}^\dagger$ of $\mathbf{U}_{00}$, i.e., $\mathbf{W}_{00}$ is a unitary matrix and Γ is upper triangular. There are different cases to consider:

(i)   If Γ is diagonal with a single eigenvalue λ, then

$$
\mathbf{U} = \begin{pmatrix} \lambda I & \mathbf{U}_{01} \\ \mathbf{U}_{10} & \mathbf{U}_{11} \end{pmatrix}.
$$

Assume for the sake of contradiction that $\lambda = 0$. Writing $d_j = \dim \mathcal{H}_j$, the $d_1 \times d_0$-matrix $\mathbf{U}_{10}$ must have exactly d_0 non-zero values, each in a different row because $\mathbf{U} \in \Delta$. This is only possible if $d_1 > d_0$, contradicting our assumption.

We conclude that $\lambda \neq 0$. But then the condition $\mathbf{U} \in \Delta$ requires that $\lambda \in U(1)$ and $\mathbf{U}_{01} = \mathbf{U}_{10} = 0$ (since we cannot have more than one non-zero entry in each column or row).

(ii) Γ has a non-zero off-diagonal element $\Gamma_{j,k}$, $j < k$. We will show that this is not consistent with the fact that U is a protected gate (i.e., leads to a contradiction). By reordering basis elements of $\mathcal{B}_\mathcal{C}$, we can assume without loss of generality that $\Gamma_{1,2} \neq 0$. By using, e.g., Solovay-Kitaev on $\mathcal{H}_0$, we find a product $\tilde{\mathbf{V}} = \mathbf{V}(\vartheta_1) \cdots \mathbf{V}(\vartheta_m)$ of images of mapping class group elements approximating $\mathbf{V} = \mathbf{W}_{00}^\dagger \oplus \mathbf{W}_{11}$, where $\mathbf{W}_{11}$ is an arbitrary unitary on $\mathcal{H}_1$.

Consider the matrix $\mathbf{V}\mathbf{U}\mathbf{V}^\dagger$. We have $(\mathbf{V}\mathbf{U}\mathbf{V}^\dagger)_{j,k} = \Gamma_{j,k}$ for $j, k = 1, \ldots, \dim \mathcal{H}_0$. In particular, $(\mathbf{V}\mathbf{U}\mathbf{V}^\dagger)_{1,2} \neq 0$ and $(\mathbf{V}\mathbf{U}\mathbf{V}^\dagger)_{2,1} = 0$.

We claim that we must have $(\mathbf{V}\mathbf{U}\mathbf{V}^\dagger)_{1,1} = (\mathbf{V}\mathbf{U}\mathbf{V}^\dagger)_{2,2} = 0$. To show this, assume for the sake of contradiction that one of these diagonal entries is non-zero. Then $\mathbf{V}\mathbf{U}\mathbf{V}^\dagger \notin \Delta$ since it has two non-zero entries in the same row or column. But this implies $\tilde{\mathbf{V}}\mathbf{U}\tilde{\mathbf{V}}^\dagger \notin \Delta$ since $\tilde{\mathbf{V}}\mathbf{U}\tilde{\mathbf{V}}^\dagger \approx \mathbf{V}\mathbf{U}\mathbf{V}^\dagger$, a contradiction to the fact that $\mathbf{U} \in \Delta_{\vartheta_1 \cdots \vartheta_m}$.

Now let $X_{j,k} = (\mathbf{V}\mathbf{U}\mathbf{V}^\dagger)_{j,k}$ for $j, k \in \{1, 2\}$ be the principal minor 2×2 submatrix. We have established that its only non-zero entry is $X_{1,2}$. Using the Hadamard matrix H, we then have $(HXH^\dagger)_{1,1} = X_{1,2}/2 \neq 0$ and $(HXH^\dagger)_{1,2} = -X_{1,2}/2 \neq 0$. Let $\mathbf{H} = H \oplus I_{(\dim \mathcal{H}_0 - 2)}$. By Solovay-Kitaev, we can find a product $\tilde{\mathbf{V}}' = \mathbf{V}(\vartheta_1') \cdots \mathbf{V}(\vartheta_\ell')$ of images of mapping class group elements approximating $\mathbf{V}' = \mathbf{H} \oplus \mathbf{W}_{11}'$, where $\mathbf{W}_{11}'$ is an arbitrary unitary on $\mathcal{H}_1$. Then, we have

$$
(\mathbf{V}'\mathbf{V}\mathbf{U}\mathbf{V}^\dagger(\mathbf{V}')^\dagger)_{1,1} = X_{1,2}/2 \neq 0,
$$

$$
(\mathbf{V}'\mathbf{V}\mathbf{U}\mathbf{V}^\dagger(\mathbf{V}')^\dagger)_{1,2} = -X_{1,2}/2 \neq 0,
$$

which shows that $\mathbf{V}'\mathbf{V}\mathbf{U}\mathbf{V}^\dagger(\mathbf{V}')^\dagger \notin \Delta$. By continuity, this shows that $\tilde{\mathbf{V}}'\tilde{\mathbf{V}}\mathbf{U}\tilde{\mathbf{V}}^\dagger(\tilde{\mathbf{V}}')^\dagger \notin \Delta$, contradicting the fact that $\mathbf{U} \in \Delta_{\vartheta_1' \cdots \vartheta_\ell' \vartheta_1 \cdots \vartheta_m}$.

(iii)   Γ is diagonal with distinct eigenvalues: In this case, we can apply the same kind of argument as in the proof of Corollary 4.2.

□

[1] Atiyah, M., "Topological quantum field theories," Publ. Math. Inst. Hautes Etud. Sci. **68**, 175–186 (1989).
[2] Beigi, S., Shor, P. W., and Whalen, D., "The quantum double model with boundary: Condensations and symmetries," Commun. Math. Phys. **306**(3), 663–694 (2011).
[3] Bombin, H., "Topological order with a twist: Ising anyons from an Abelian model," Phys. Rev. Lett. **105**, 030403 (2010).
[4] Bombin, H. and Martin-Delgado, M. A., "Topological quantum distillation," Phys. Rev. Lett. **97**, 180501 (2006).
[5] Bombin, H. and Martin-Delgado, M. A., "Family of non-Abelian Kitaev models on a lattice: Topological condensation and confinement," Phys. Rev. B **78**, 115421 (2008).
[6] Bombin, H. and Martin-Delgado, M. A., "Topological computation without braiding," Phys. Rev. Lett. **98**, 160502 (2007).
[7] Bravyi, S., Hastings, M., and Verstraete, F., "Lieb-Robinson bounds and the generation of correlations and topological quantum order," Phys. Rev. Lett. **97**(5), 050401 (2006).
[8] Bravyi, S. and Kitaev, A. Y., "Quantum codes on a lattice with boundary," e-print arXiv:quant-ph/9811052 (1998).
[9] Bravyi, S. and Kitaev, A. Y., "Universal quantum computation with ideal Clifford gates and noisy ancillas," Phys. Rev. A **71**, 022316 (2005).
[10] Bravyi, S. and König, R., "Classification of topologically protected gates for local stabilizer codes," Phys. Rev. Lett. **110**, 170503 (2013).
[11] Brell, C. G., Burton, S., Dauphinais, G., Flammia, S. T., and Poulin, D., "Thermalization, error correction, and memory lifetime for Ising anyon systems," Phys. Rev. X **4**(3), 031058 (2014).
[12] Burton, S., Brell, C. G., and Flammia, S. T., "Classical simulation of quantum error correction in a Fibonacci anyon code," e-print arXiv:1506.03815v1 [quant-ph].
[13] Chen, X., Gu, Z.-C., and Wen, X.-G., "Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order," Phys. Rev. B **82**(15), 155138 (2010).
[14] Eastin, B. and Knill, E., "Restrictions on transversal encoded quantum gate sets," Phys. Rev. Lett. **102**, 110502 (2009).
[15] Else, D. V., Schwarz, I., Bartlett, S. D., and Doherty, A. C., "Symmetry-protected phases for measurement-based quantum computation," Phys. Rev. Lett. **108**, 240505 (2012).
[16] Fowler, A. G., Mariantoni, M., Martinis, J. M., and Cleland, A. N., "Surface codes: Towards practical large-scale quantum computation," Phys. Rev. A **86**, 032324 (2012).
[17] Fowler, A. G., Stephens, A. M., and Groszkowski, P., "High threshold universal quantum computation on the surface code," Phys. Rev. A **80**, 052312 (2009).
[18] Freedman, M., Nayak, C., Walker, K., and Wang, Z., in *On Picture (2+1)-TQFTs* (World Scientific, 2008), Chap. 2, pp. 19–106.
[19] Freedman, M. H., Kitaev, A. Y., and Wang, Z., "Simulation of topological field theories by quantum computers," Commun. Math. Phys. **227**, 587–603 (2002).
[20] Freedman, M. H., Kitaev, A., Larsen, M. J., and Wang, Z., "Topological quantum computation," Bull. Am. Math. Soc. **40**, 31–38 (2003).
[21] Freedman, M. H., Larsen, M., and Wang, Z., "A modular functor which is universal for quantum computation," Commun. Math. Phys. **227**(3), 605–622 (2002).
[22] Haah, J., "Local stabilizer codes in three dimensions without string logical operators," Phys. Rev. A **83**, 042330 (2011).
[23] Haah, J., "An invariant of topologically ordered states under local unitary transformations," e-print arXiv:1407.2926 (2014).
[24] Hutter, A. and Wootton, J. R., "Continuous error correction for Ising anyons," e-print arXiv:1508.04033 [quant-ph].
[25] Walker, K., *On Witten's 3-Manifold Invariants*, Lecture Notes (1991), http://canyon23.net/math/1991TQFTNotes.pdf.
[26] Kitaev, A. and Preskill, J., "Topological entanglement entropy," Phys. Rev. Lett. **96**, 110404 (2006).
[27] Kitaev, A. Y., "Fault-tolerant quantum computation by anyons," Ann. Phys. **303**(1), 2 (2003).
[28] Kitaev, A. Y., "Anyons in an exactly solved model and beyond," Ann. Phys. **321**(1), 2 (2006).
[29] Kitaev, A. Y. and Kong, L., "Models for gapped boundaries and domain walls," Commun. Math. Phys. **313**(2), 351–373 (2012).
[30] Kong, L. and Wen, X.-G., "Braided fusion categories, gravitational anomalies, and the mathematical framework for topological orders in any dimensions," e-print arXiv:1405.5858 (2014).
[31] Lane, S. M., *Categories for the Working Mathematician*, Graduate Texts in Mathematics (Springer, New York, 1998).
[32] Levin, M. A. and Wen, X.-G., "String-net condensation: A physical mechanism for topological phases," Phys. Rev. B **71**, 045110 (2005).
[33] Levin, M. A. and Wen, X.-G., "Detecting topological order in a ground state wave function," Phys. Rev. Lett. **96**, 110405 (2006).
[34] Lieb, E. H. and Robinson, D. W., "The finite group velocity of quantum spin systems," Commun. Math. Phys. **28**(3), 251–257 (1972).
[35] Michnicki, K., "3-D topological quantum memory with a power-law energy barrier," Phys. Rev. Lett. **113**, 130501 (2014); e-print arXiv:1208.3496.
[36] Moore, G. and Seiberg, N., "Polynomial equations for rational conformal field theories," Phys. Lett. B **212**(4), 451–460 (1998).
[37] Pastawski, F. and Yoshida, B., "Fault-tolerant logical gates in quantum error-correcting codes," Phys. Rev. A **91**, 012305 (2015); e-print arXiv:1408.1720.
[38] Pedrocchi, F. L. and DiVincenzo, D. P., "Majorana braiding with thermal noise," Phys. Rev. Lett. **115**, 120402 (2015).

[39] Preskill, J., Lecture Notes on Quantum Computation (2004), available at http://www.theory.caltech.edu/people/preskill/ph229/lecture.

[40] Segal, G., *The Definition of Conformal Field Theory*, London Mathematical Society Lecture Note Series (Cambridge University Press, 2004), Vol. 308, preprint.

[41] Verlinde, E., "Fusion rules and modular transformations in 2D conformal field theory," Nucl. Phys. B **300**, 360–376 (1988).

[42] Wang, Z., *Topological Quantum Computation*, Regional Conference Series in Mathematics Vol. 112 (Conference Board of the Mathematical Sciences, 2010).

[43] Witten, E., "Quantum field theory and the Jones polynomial," Commun. Math. Phys. **121**(3), 351–399 (1989).

[44] In the language of this paper, braiding/mapping class group elements belong to locality-preserving unitaries if the model is abelian. However, for a general non-abelian model, braiding is not locality-preserving according to our definition.

[45] In principle, we could consider unitaries/isometries (or sequences thereof) of the form $U : \mathcal{H}_{\text{phys},\Sigma} \to \mathcal{H}'_{\text{phys},\Sigma'}$ which map between *different* systems $\mathcal{H}_{\text{phys},\Sigma}$ and $\mathcal{H}'_{\text{phys},\Sigma'}$. By a slight modification of the arguments here, we could then obtain restrictions on locality-preserving isomorphisms (instead of automorphisms, cf. Section III). Such a scenario was discussed in Ref. 10 in the context of stabilizer codes. Here, we restrict to the case where the systems (and associated ground spaces) are identical for simplicity, since the main conclusions are identical.

[46] As a side remark, we mention that our terminology is chosen with spin lattices in mind. However, the notion of locality-preservation can be relaxed. As will become obvious below, our results apply more generally to the set of *homology-preserving* automorphisms U. The latter can be defined as follows: if the support of an operator X is contained in a region $\mathcal{R} \subset \Sigma$ which deformation retracts to a closed curve C, then the support of $UXU^\dagger$ must be contained in a region $\mathcal{R}' \subset \Sigma$ which deformation retracts to a curve C' in the same homology class as C. For example, for a translation-invariant system, translating by a possibly extensive amount realizes such a homology-preserving (but not locality-preserving) automorphism.

[47] More precisely, for $B(x_{k-1}, x_{k+1})$, the relevant matrices are $\tilde{F}_{x',x} = F^{z x_{k-1} x_k}_{x_{k+1} z x'}$ and $\tilde{R}$ is diagonal with entries $\tilde{R}_{x,x} = R^{zz}_x$. Here, F is the F-matrix associated with basis changes on the four-punctured sphere (see Section V A), whereas R^{xy}_z determines an isomorphism between certain Hilbert spaces associated with the three-punctured sphere. We refer to, e.g., Ref. 39 (p. 48) for a derivation of these expressions.