PHYSICAL REVIEW A **67**, 022315 (2003)

Anyons from nonsolvable finite groups are sufficient for universal quantum computation

Carlos Mochon*

Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125

(Received 1 October 2002; published 28 February 2003)

We present a constructive proof that anyonic magnetic charges with fluxes in a nonsolvable finite group can perform universal quantum computations. The gates are built out of the elementary operations of braiding, fusion, and vacuum pair creation, supplemented by a reservoir of ancillas of known flux. Procedures for building the ancilla reservoir and for correcting leakage are also described. Finally, a universal qudit gate set, which is ideally suited for anyons, is presented. The gate set consists of classical computation supplemented by measurements of the X operator.

DOI: 10.1103/PhysRevA.67.022315 PACS number(s): 03.67.Lx, 05.30.Pr

I. INTRODUCTION

The discovery of the potential speedups offered by quantum computers launched an effort to find physical systems out of which these computers could be built. Researchers soon found that these systems are in short supply, as it is extremely difficult to isolate a quantum system from the environment, while maintaining enough control to perform operations on the encoded data. The advent of quantum error correction and fault-tolerant processing has drastically increased the tolerable error rates; nonetheless, physical systems with low enough error rates are still hard to come by.

One way to protect a Hilbert space from the environment is to encode the quantum data in nonlocal observables. These observables, which are constructed from topological invariants, cannot be measured or changed by any local operator. Therefore, because the environment generally acts locally, the physics of the system provides a form of fault tolerance.

In particular, consider the spectrum of electrically and magnetically charged particles that are obtained by breaking a gauge group to a finite subgroup. The finite group gauge theory is a particularly good system for quantum computing because it involves no gauge fields, and hence no long-range interactions except for those obtained by braiding. Furthermore, the Hamiltonian of the system respects the unbroken symmetry; therefore, Schur's lemma forbids the types of coupling to uncharged objects that can produce decoherence. Of course, the data could still decay by the exchange of a charged particle between two anyons, but this is a quantum tunneling event which is exponentially suppressed by the distance between the particles.

When the gauge theory is restricted to two spatial dimensions, the particles acquire topological long-range interactions, which can be be used to perform computations. The interactions occur when the particles are exchanged or braided, and depend only on the topological class of the path involved. Because of these interactions, the charged particles have quantum statistics that are more exotic than the standard fermions and bosons, and are known as anyons. The nonstandard statistics, though, only arise when clockwise rotations can be distinguished from counterclockwise rotations, which is why we impose the requirement of two spatial dimensions. While this two-dimensional model of the world seems somehow unphysical, there exist condensed-matter systems with quasiparticles that behave like anyons.

The original proposal for an anyon based quantum computer was made by Kitaev [1,2]. The first concrete description was done by Ogburn and Preskill in Refs. [3,4] for anyons in the group A_5, the even permutations of five elements. In our paper, we will generalize the work of Ogburn and Preskill to any nonsolvable finite group, which includes A_5 as the smallest case.

The paper is organized as follows: We begin by introducing some notation and reviewing the properties of the anyon model that will be used throughout this paper. Section III presents the universal gate set that will be employed to prove anyons can perform quantum computations. Sections IV–VI contain the main part of the paper, and discuss a concrete anyonic implementation of all the necessary gates. For pedagogical reasons, we first cover the easier subcase of simple perfect groups in Sec. IV, and then discuss the required generalizations for any nonsolvable group in Sec. VI. In Section V, we discuss how to make these computations fault tolerant by performing leakage correction. Finally, we discuss the conclusions and unsolved questions. There are also two Appendixes which include the mathematical proofs, and a technique for creating anyon ancillas.

II. REVIEW

In this section, we will review some of the braiding and fusion properties of our anyons. Our review will be rather abridged, but more details can be found in the excellent review of discrete gauge theories [5] (and the original work [6]). The paper by Ogburn and Preskill [3,4] also contains a good review with emphasis on the applications to quantum computing.

This section also establishes our notation for qudits, and reviews the phase estimation circuit, a highly useful trick that will be used often.

A. Magnetic charges

The main players throughout this paper will be the magnetic charges, also known as fluxes. For a field theory with

*Electronic address: carlosm@theory.caltech.edu

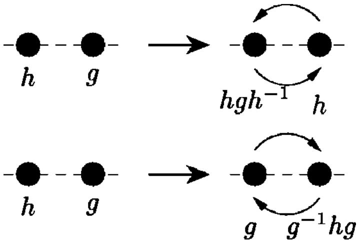


FIG. 1. Exchanging two anyons.

an unbroken finite group G, there is one magnetic charge for each element $g \in G$. Quantum mechanically, we can have superpositions of these states, giving a one-particle Hilbert space spanned by $|g\rangle \;\forall\; g \in G$ (though strictly speaking, superpositions of charges in different conjugacy classes are meaningless, as will be explained in the following section).

Specifying the exchange properties of the charges involves making a choice of gauge. The easiest choice, which will be used in this paper, is to keep all anyons ordered on a horizontal line. The exchange of particles, which can be clockwise or counterclockwise, is only allowed between adjacent pairs. In either case, the particle that passes below remains unchanged, while the particle that passes above gets conjugated. When the exchange is in the counterclockwise direction, the upper anyon gets conjugated by the flux of the lower one, whereas in the clockwise direction it gets conjugated by the inverse of the lower flux. This is depicted in Fig. 1.

One way to visualize these exchanges is to associate with each anyon a ray that is vertical in the plane, starting at the particle and proceeding upwards. Anyons are allowed to move freely through the plane, but every time an anyon crosses the ray of another particle, it gets conjugated by the flux of the owner of the ray (or by the inverse flux if crossing from left to right). Note that when a particle passes a group of anyons, it gets conjugated by the total flux of the anyons, which is given as the product from left to right of the individual fluxes.

Clearly, moving single anyons around can produce strange correlations throughout the system. However, moving a pair of anyons with a total flux that is trivial will not change the state of the system if the pair always passes below. This is why we will always be dealing with states of the form

$$\sum_g a_g |g\rangle \otimes |g^{-1}\rangle, \tag{1}$$

which correspond to a pair of anyons with trivial total flux. When dealing only with pairs of trivial total flux, we can swap any two pairs, or bring any two pairs together without affecting the state of the rest of the system.

We do want to allow controlled interaction between pairs, though, and this is accomplished by a pass-through operation. The idea is to have one pair circle one anyon from the other pair. This will conjugate the fluxes of the pair that circles, but leave the other pair invariant. This operation is depicted using elementary exchanges in Fig. 2.

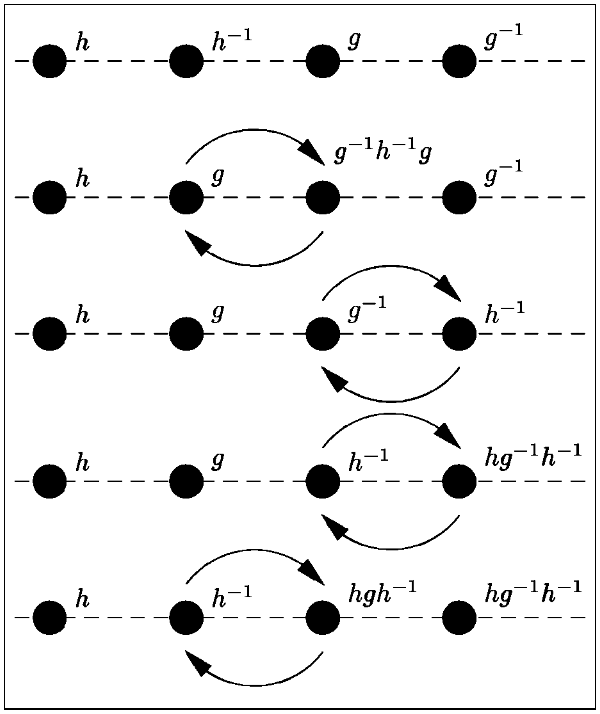


FIG. 2. Conjugating a pair of anyons.

The net result of the pictured operation is

$$|h\rangle \otimes |h^{-1}\rangle \otimes |g\rangle \otimes |g^{-1}\rangle \to |h\rangle \otimes |h^{-1}\rangle \otimes |hgh^{-1}\rangle \otimes |hg^{-1}h^{-1}\rangle, \tag{2}$$

which is a conjugation of the second pair by h. Conjugation by h^{-1} could be achieved by using counterclockwise exchanges in the picture.

For notational convenience, in this paper, we will generally only mention the flux of the left element of a pair. The above transformation will be written as

$$|h\rangle \otimes |g\rangle \to |h\rangle \otimes |hgh^{-1}\rangle, \tag{3}$$

leaving the compensating fluxes implicit. While we will exclusively deal in this paper with flux pairs with trivial flux, we will only explicitly refer to the second anyon when necessary to describe the operations.

B. Electric charges and vacuum pairs

We now wish to focus on the operations of creating pairs from the vacuum and fusing pairs back into the vacuum. However, we must first briefly discuss the complete spectrum of particles, and that involves electric charges.

An electric charge is a particle with no flux that transforms as some nontrivial irreducible representation of the group G. A useful analogy is to think of the representation of G as the total spin of the particle. The internal state of the particle is then equivalent to the direction in which the spin is pointing.

The electric charge states can be labeled as $|R,V\rangle$, where R is a representation of G and V is a vector that transforms in the representation R. The electric charges do not interact with each other, but when one of them circles a magnetic flux g, its state changes as

$$|R,V\rangle \rightarrow |R,U_R(g)V\rangle, \tag{4}$$

where $U_R(g)$ is the matrix corresponding to g in the representation R. This is known as the Aharonov-Bohm effect.

While we can transform the state of an electric charge within the subspace of a representation, there are no operations (other than fusion, which destroys the particle) that can change the representation of a particle. Furthermore, the phase between states of different representations cannot be measured. We can therefore effectively describe the electric charges as having decohered into the different representations. In particle physics, we would say that the different representations correspond to different superselection sectors.

The same thing happens to the magnetic charges. Different conjugacy classes live in different superselection sectors, so we can imagine that there is an automatic decoherence into different conjugacy classes. Superpositions of fluxes in different conjugacy classes are therefore meaningless.

The spectrum also contains particles with both electric and magnetic charge, which are called dyons. The only special feature is that the electric charge is a representation only of the subgroup of G that commutes with the flux. The aforementioned magnetic charges are just dyons with a trivial representation. The dyons also have superselection sectors that correspond to different conjugacy classes and representations.

The purpose of discussing the full spectrum, and the idea of superselection sectors, is to find out what kind of states we get when we create a pair of particles from the vacuum. The first thing to note is that each of the particles will instantly decohere into a specific conjugacy class and representation. Furthermore, because a pair created from the vacuum must have trivial total charge and flux, the conjugacy classes must be inverses, and the representations must be conjugate representations.

Consider the case that the pair decoheres into plain magnetic charges, with the first one contained in the conjugacy class C. Because the combined state still has vacuum quantum numbers, the state must transform trivially when another flux is dragged around it. That is, it must be invariant under conjugation. There is only one such state:

$$|\mathrm{vac}(C)\rangle = \frac{1}{\sqrt{|C|}} \sum_{g\in C} |g\rangle \otimes |g^{-1}\rangle. \tag{5}$$

The vacuum states for the other superselection sectors are also unique and have similar expressions. When a pair of anyons is created from the vacuum, it will start off in one of these states.

Another useful operation is to fuse two anyons together. Note that we are not talking about two anyon pairs, but rather two anyons, sometimes from the same pair, and sometimes from different pairs. The operation of fusion will turn the two particles into one, which must carry the total flux and charge of the two. It is also possible that the two anyons will have vacuum quantum numbers, and will fuse back into the vacuum. In this case, no particle will be left behind and their total mass will be transformed into some other medium, such as radiation. If $|\Psi\rangle$ is the combined state of the two anyons, and the first anyon is in the conjugacy class C, then the probability that the two will fuse into the vacuum is given by the standard rules of quantum mechanics:

$$P_{vacuum} = |\langle \mathrm{vac}(C)|\Psi\rangle|^2. \tag{6}$$

After fusing two particles of different pairs, the fused particle may carry some flux. However, since the total flux of the original four particles was trivial, the total flux of all the remaining particles (including the product of the fusion) will be trivial as well. Therefore, it is possible to safely move the group of particles away from the bulk of the computation without disturbing our quantum state.

C. Qudits

Throughout this paper it will be useful to perform computations with qudits rather than the usual qubits. We define our computational basis as the states $|i\rangle$ for $0 \leqslant i < d$, where we will assume that d is prime. The unitary Z and X gates can be defined as follows

$$Z|i\rangle = \omega^i |i\rangle, \tag{7}$$

$$X|i\rangle = |i+1\rangle, \tag{8}$$

where ω is a fixed nontrivial dth root of unity, and sums are understood to be modulo d. The operators satisfy the commutation relation

$$ZX = XZ\omega. \tag{9}$$

As usual, the eigenstates of Z correspond to the computational basis. We can also introduce the eigenstates of X:

$$|\tilde{i}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-ij} |j\rangle, \tag{10}$$

which have the following transformations under the action of our unitary gates:

$$Z|\tilde{i}\rangle = |\widetilde{i-1}\rangle, \tag{11}$$

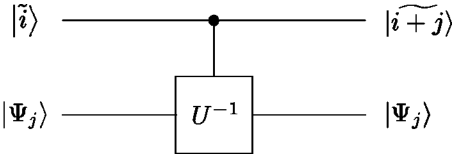
$$X|\tilde{i}\rangle = \omega^i |\tilde{i}\rangle. \tag{12}$$

D. Phase measurement

A very useful trick, used many times throughout this paper, is Kitaev's phase estimation technique [7]. In fact, we will only employ a special case of the technique which we describe below.

Assume that we are working in a system with qudits, and we have an operator U with eigenvalues that are dth roots of unity. We shall prove that being able to apply a controlled U gate, and measure in the X basis, is equivalent to being able to measure the operator U.

Consider applying the circuit below to an eigenstate $|\Psi_j\rangle$ of U with eigenvalue ω^j:

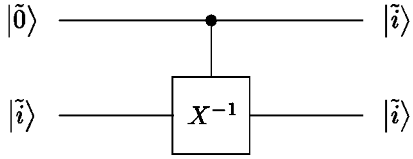


where the controlled U^{-1} gate can be applied as $d-1$ controlled U gates. The circuit works as described because the controlled U^{-1} gate leaves the bottom state invariant, but applies a Z^{-j} to the upper state. On a general state $|\phi\rangle = \Sigma_j c_j|\Psi_j\rangle$ expanded in terms of eigenvectors of U, the circuit produces the transformation

$$|\tilde{0}\rangle\otimes|\phi\rangle\rightarrow\sum_j c_j|\tilde{j}\rangle\otimes|\Psi_j\rangle. \qquad (13)$$

Clearly, a subsequent measurement of the first qudit in the X basis is equivalent to a nondestructive measurement of the original state in the U basis. We will use this technique in the following section to measure the operators X^aZ^b.

In a later section, we will employ the equivalent circuit



run in both the forward and backward directions, to change between the $|\tilde{i}\rangle$ states and the readily available $|\tilde{0}\rangle$ state which can be naturally produced from, and fused into the vacuum.

III. A UNIVERSAL GATE SET FOR ANYONS

A lot of the work in proving universality can be simplified by choosing a proper gate set. For this paper, we will employ a generalization of the gate set used by Ogburn and Preskill [3,4]. The gate set, which involves measurements as well as unitary gates, can be applied to qudits when d is prime, which is the only case considered in this paper.

The universal gate set is (1) Measure nondestructively Z, (2) Measure nondestructively X, and (3) Apply Toffoli operators (to any set of three qudits), where the qudit Toffoli operator is defined as

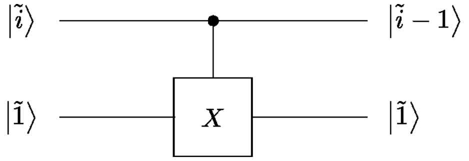
$$T|l,m,n\rangle=|l,m,lm+n\rangle. \qquad (14)$$

and all computations are done modulo d.

Though tangential to the main purpose of this paper, the above gate set is another answer to the question posed in Ref. [8]. That is, given a Toffoli gate, what extra gates are required to complete a universal set? Of course, the answer provided by the above gate set involves measurements in an integral way, and is therefore different from the one proposed in Ref. [8]. However, the above gate set also addresses the question: Given classical computation (i.e., Toffoli gate and measurements of Z), what gates are needed to complete the universal set?

We now turn our attention to the proof of universality for the gate set presented above. We note that Gottesman has already proven in Ref. [9] that for d prime, applying and measuring products of Z's and X's, plus a Toffoli gate, is universal for quantum computation. All we need to do in order to prove universality, is to show that we can apply and measure operators of the form X^aZ^b using the above gates.

Measurements of X followed by measurements of Z can produce $|i\rangle$ ancillas for any i. Similarly, we can obtain $|\tilde{i}\rangle$ ancillas from measurements of Z followed by measurements of X. A controlled sum gate can be made out of a Toffoli gate by fixing an input to a $|1\rangle$ ancilla. Because a controlled sum gate is really a controlled X gate, fixing the other input to $|1\rangle$ produces the X gate. On the other hand, a controlled sum gate from a state to a $|\tilde{1}\rangle$ ancilla, produces a Z gate on the state



The general case of applying X^aZ^b can be done by a series of X and Z gates. All that remains is to construct a method for measuring operators of the form X^aZ^b. First, we note that

$$(X^aZ^b)^d=\omega^{abd(d-1)/2}X^{ad}Z^{bd}=\begin{cases}1, & d\text{ odd}\\ -1^{ab}, & d=2.\end{cases} \qquad (15)$$

A. *d* odd case

The case $d=2$ is rather complicated and will be handled separately. The general case d odd (remember we required d prime) is easy because the eigenvalues of X^aZ^b are the dth roots of unity just like those of X and Z. As discussed in the review of phase estimation, being able to apply a controlled X^aZ^b gate, combined with measurements in the X basis (which includes preparation of X eigenstates) is sufficient to measure in the X^aZ^b basis.

All that remains is to construct the controlled X^aZ^b gate. That is, we need to be able to apply the gate

$$|n\rangle\otimes|\psi\rangle\rightarrow|n\rangle\otimes(X^aZ^b)^n|\psi\rangle=|n\rangle\otimes X^{an}Z^{bn}\omega^{abn(n-1)/2}|\psi\rangle, \qquad (16)$$

composed of a phase $|n,m\rangle\rightarrow\omega^{bnm+abn(n-1)/2}|n,m\rangle$ followed by controlled sums. The controlled sum gate is just a Toffoli gate with an input fixed to one. As for the phase, because we have a Toffoli gate, we have universal classical computation. We can thus compute $bnm+abn(n-1)/2$ in an ancilla, apply a Z gate to this ancilla, and then erase the computation.

B. $d=2$ case

The $d=2$ case is somewhat trickier because our gate set is invariant under complex conjugation, and thus there is no way of distinguishing the two eigenstates of $ZX=iY$. We will solve this problem by creating an ancilla that is an eigenstate of ZX, defining it to be the $+i$ eigenstate, and then using it to measure and build more eigenstates.

Assume, we were given a state

$$|\Psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle+\omega|1\rangle), \tag{17}$$

where $\omega^2=-1$. Clearly, the state is equal to one of the two ZX eigenstates: $|\pm_Y\rangle=(|0\rangle\pm i|1\rangle)/\sqrt{2}$.

Using a controlled ZX gate, which is built by the method described in the d odd case, we can produce copies of the state $|\Psi\rangle$. The idea, similar to the one used for phase estimation, is to apply the controlled ZX gate from a state $|\tilde{0}\rangle$ to a the state $|\Psi\rangle$. The target state is an eigenvector of ZX with eigenvalue ω, and therefore the relative phase is copied over to the first state:

$$|\tilde{0}\rangle\otimes|\Psi\rangle\rightarrow\frac{1}{\sqrt{2}}(|0\rangle+\omega|1\rangle)\otimes|\Psi\rangle=|\Psi\rangle\otimes|\Psi\rangle. \tag{18}$$

Notice that copying works independent of whether $|\Psi\rangle$ is the $+i$ or $-i$ eigenstate of ZX. Naturally, by subsequently applying a Z, we can also produce the orthogonal state $|\Phi\rangle=(|0\rangle-\omega|1\rangle)/\sqrt{2}$.

With our ancilla, we can also measure in this basis. This is done by applying a controlled ZX gate to the ancilla from the state we want to measure:

$$|\Psi\rangle\otimes|\Psi\rangle\rightarrow|\tilde{1}\rangle\otimes|\Psi\rangle, \tag{19}$$

$$|\Phi\rangle\otimes|\Psi\rangle\rightarrow|\tilde{0}\rangle\otimes|\Psi\rangle, \tag{20}$$

and then measuring in the X basis.

As long as we are consistent in always using the same ancilla $|\Psi\rangle$, we will have broken the conjugation symmetry, and found a way to label, create, and measure eigenstates of ZX. Of course, we should keep many copies of the ancilla, which can be prepared from the original state. The operations above also allow us to error correct our set of ancillas by copying each, comparing the copies, and using majority voting to discard the damaged ancillas. Thus, even if there are some errors in preparation, or some of the ancillas decay over time, computation will still be feasible.

All that remains to be explained is how to create the first copy of $|\Psi\rangle$. Because a state with a density-matrix proportional to the identity can be written as

$$\rho=\tfrac{1}{2}I=\tfrac{1}{2}|+_Y\rangle\langle+_Y|+\tfrac{1}{2}|-_Y\rangle\langle-_Y|, \tag{21}$$

it is equivalent to having prepared an eigenstate of $ZX=iY$ chosen at random. The state $\rho=I/2$ can be produced by discarding one qubit of a bell state, and a bell state can be produced with a controlled sum gate from a $|\tilde{0}\rangle$ ancilla to a $|0\rangle$ ancilla. Therefore, we have shown that we can produce the initial eigenstate of ZX, and we have completed the proof that the gate set presented at the beginning of this section is universal for quantum computation.

IV. UNIVERSAL COMPUTATION FOR SIMPLE PERFECT GROUPS

In this section, we will prove that a set of anyons based on certain groups can perform universal quantum computations. Instead of dealing first with the general case of nonsolvable groups, we will deal with the smaller set of groups that are both simple and perfect.

We remind the reader that nonsolvable groups are those that contain a perfect subgroup; and a perfect group is any nontrivial group, whose commutator subgroup equals the full group: $[G,G]=G$. The property of simplicity means that the group has exactly two subgroups that are invariant under conjugation: the trivial group and the whole group. Because the commutator subgroup is invariant under conjugation, it should be clear that any simple non-Abelian group is perfect. However, we shall refer to these groups as simple and perfect to remind the reader that we are dealing with a subcase of the general nonsolvable case.

The set of simple perfect groups, which includes the groups A_n for $n>4$, is powerful for computing because in some sense we can get from one nontrivial element to any other using operations that fix the identity. The general case of nonsolvable groups will be deferred to Sec. VI, where we will show that a simple perfect group can be extracted from a nonsolvable group.

A. Requirements for the physical system

Here, we list the operations, ancillas, and measurements that we assume are available on any realistic anyonic system, and which we will use to build our quantum gate set:

(1) We can braid or exchange any two particles.

(2) We can fuse a pair of anyons and detect whether there is a particle left behind or whether they had vacuum quantum numbers.

(3) We can produce a pair of anyons in a state that is chosen at random from the two particle subspace that has vacuum quantum numbers.

(4) We have ancilla pairs of the form $|g\rangle\otimes|g^{-1}\rangle$ for any $g\in G$, where the individual anyons have trivial electric charge.

We remind the reader again that even though all our anyons are used in pairs of trivial total flux, we will generally only mention one of the anyons of the pair. These conventions also apply to ancillas, which means that we will refer to the $|g\rangle\otimes|g^{-1}\rangle$ state as an ancilla of flux g.

While the first three requirements are natural operations for a laboratory system, it is not clear where the ancillas would come from. Depending on the physical realization there may be many ways of obtaining the ancilla reservoir. We discuss one such scheme in Appendix A.

B. Computational basis

Let G be a simple and perfect finite group. Let a and b be two noncommuting elements of G. Let d be the smallest integer such that $a^d b a^{-d} = b$. We can assume that d is prime, otherwise we could replace a by $a^{d/p}$ where p is some prime that divides d.

It turns out that every simple non-Abelian group has even order. This was first conjectured by Burnside [10] in 1911, and proven by Feit and Thompson [11] in 1963 (in fact, the complete classification of simple finite groups was completed in the early 1980's, see for instance Ref. [12]). Using Sylow's theorems, the fact that every simple group has even order means that they all include a nontrivial element a such that $a^2 = 1$. Therefore, we could always work with a basis of qubits. However, we will present the general qudit case both for its elegance, and because in some instances a basis of qudits is more convenient.

We will work with a basis of qudits of trivial net flux

$$|n\rangle = |a^n b a^{-n}\rangle \otimes |a^n b^{-1} a^{-n}\rangle \tag{22}$$

for $0 \leqslant n < d$, where we have explicitly described both anyons of the pair.

It should be clear that we can initialize the computer by filling up the computational space with $|0\rangle$ ancillas. We turn now to the task of constructing the gates presented in Sec. III.

C. Conjugation by a function

We begin by describing the technique of conjugation by a function, which is especially powerful for simple perfect groups. In Sec. II A, we showed that we could perform the transformation

$$|h\rangle \otimes |g\rangle \rightarrow |h\rangle \otimes |hgh^{-1}\rangle, \tag{23}$$

where we conjugate the second anyon by the flux of the first, while the first anyon remains invariant. We can also conjugate an anyon by a product $h_1 h_2 \cdots h_n$

$$|g\rangle \rightarrow |h_1 h_2 \cdots h_n g h_n^{-1} \cdots h_2^{-1} h_1^{-1}\rangle, \tag{24}$$

where the $\{h_i\}$ are fluxes of other anyons which remain unchanged throughout this process. The procedure is done by first conjugating by h_n, then by h_{n-1}, and proceeding leftward until we finally conjugate by h_1.

The above procedure is not terribly useful if all the $\{h_i\}$ are fluxes of fixed ancillas, because we could have equivalently conjugated by a single ancilla of flux $h = h_1 h_2 \cdots h_n$. However, some of the fluxes in the product could correspond to anyons that represent qubits of unknown state. In this case we can think of the above operation as conjugation by a function of the fluxes of certain qubits.

Let's consider what kind of functions can be applied in this way. Clearly we are speaking about functions that can be written as products of elements of G. The elements can include known constants if we use our ancillas to conjugate. We can also include the flux of a qubit, which will be of the form $a^i b a^{-i}$ if the qubit is in the computational basis (though this may not be the case when we are trying to correct leakage). Finally, we can include in the product the inverse of the flux of a qubit, as discussed in Sec. II A.

In conclusion, given n qubits with fluxes g_1 through g_n, and a function $f(g_1, \ldots, g_{n-1})$ of the first $n-1$ qubits, we can conjugate the last qubit by f

$$|g_n\rangle \rightarrow |f(g_1, \ldots, g_{n-1}) g_n f(g_1, \ldots, g_{n-1})^{-1}\rangle, \tag{25}$$

provided that the function f can be written in product form. By product form, we mean that f is a product of the inputs $\{g_i\}$, their inverses $\{g_i^{-1}\}$, and fixed elements of G, each of which may appear more than once, or not at all. For example, a valid function would be $f(g_1, g_2) = a g_2 b g_1^{-1} c g_1^{-1} d$ with $a,b,c,d \in G$. Furthermore, this transformation does not change the flux of the first $n-1$ qubits, though it may entangle them with the last qubit.

D. Toffoli Gate

To build the Toffoli gate we must be able to conjugate the third qubit by the function $f(g_1, g_2)$, which depends on the fluxes of the first two qubits as

$$f(a^i b a^{-i}, a^j b a^{-j}) = a^{ij}, \tag{26}$$

and is arbitrary for values of g_1 and g_2 that are not in the computational basis. If the third qubit is in the state $a^k b a^{-k}$, conjugation by f produces the transformation

$$|a^k b a^{-k}\rangle \rightarrow |a^{ij+k} b a^{-ij-k}\rangle, \tag{27}$$

which is the desired Toffoli gate.

Given the discussion in the preceding section, we are left with the task of expressing the function f in product form. However, it turns out that for simple and perfect groups every function has such an expression.

Theorem: If G is a simple and perfect finite group, then any function $f(g_1, \ldots, g_n): G^n \rightarrow G$ can be expressed as a product of the inputs $\{g_i\}$, their inverses $\{g_i^{-1}\}$, and fixed elements of G, any of which may appear multiple times in the product.

Not only does the above theorem prove that Toffoli gates are possible for any simple and perfect group, but it directly proves that any classical function can be computed.

The proof of the theorem, which is mostly constructive, is somewhat long and will be deferred to Appendix B. However, to make this seem plausible to the casual reader, we would like to illustrate the basic steps needed to build a Toffoli gate for qubits.

The main idea behind the construction is that the function f is basically a logical AND of the inputs. A commutator makes a good logical AND because it equals the identity if either of its inputs are the identity. Furthermore, the commutator function can be expanded as a product of its inputs. Therefore, we would like the first input to take values 1 or c and the second input to take values 1 or d, with the requirement that d not commute with c, so that we can put them into a commutator.

Let g_1 denote the flux of the first qubit, and g_2 the flux of the second qubit. Each takes values $g_i \in \{b, aba^{-1}\}$. Define the new variables $g_i' = g_i b^{-1} \in \{1, c\}$, where $c \equiv [a,b] \equiv aba^{-1}b^{-1}$. It is sufficient to show that we can express the Toffoli function as a product of g_1', g_2', their inverses and fixed ancillas.

Choose an element d that does not commute with c and define $e \equiv [c,d]$. Imagine we could find two functions of one element, that can be expressed in product form, such that

$$h_1(c) = d, \quad h_1(1) = 1, \tag{28}$$

$$h_2(e) = a, \quad h_2(1) = 1. \tag{29}$$

Using these functions, the Toffoli function can be written as

$$f(g_1, g_2) = h_2([g_1', h_1(g_2')]), \tag{30}$$

which when expanded out is a product of the correct form.

The existence of the functions h_i, which is discussed in more detail in the full proof of the theorem, is a consequence of G being simple. For any element $c \in G$, the group generated by its conjugacy class $C(c)$ is a normal subgroup. Because G is simple, this subgroup must equal the full group. Therefore, every element $d \in G$ has an expression of the form $d = x_1 c x_1^{-1} x_2 c x_2^{-1} \cdots x_n c x_n^{-1}$ for some n and some elements $\{x_i\} \in G$. We can use the expression to construct h_1,

$$h_1(g) = x_1 g x_1^{-1} x_2 g x_2^{-1} \cdots x_n g x_n^{-1}, \tag{31}$$

and a similar construction builds h_2.

For a concrete example, we can work with $G = A_5$. We begin by choosing an element a, which must satisfy $a^2 = I$, if we wish to work with qubits $(d = 2)$. Because of the symmetries of the group, all choices are equivalent to $a = (12)(34)$. The next step would involve choosing an element b that does not commute with a, and an element d that does not commute with $c \equiv [a,b]$. While any choice can produce a Toffoli gate, the required h_1 function will be simplified if we can make c and d fall in the same conjugacy class. The same can be said for h_2 if $e \equiv [c,d]$ and a are in the same conjugacy class.

At this point, a little trial and error yield $b = (345)$ and $d = (234)$. The computational basis is now defined as

$$|0\rangle = |b\rangle = |(345)\rangle,$$
$$|1\rangle = |aba^{-1}\rangle = |(435)\rangle, \tag{32}$$

and the remaining group elements are fixed as

$$c = (aba^{-1})b^{-1} = (435)(435) = (345),$$
$$e = (cdc^{-1})d^{-1} = (245)(324) = (25)(34). \tag{33}$$

The h_i functions, which are the only nonconstructive part of the proof, can be built as simple conjugations because of the choices we made earlier:

$$h_1(g) = h_2(g) = (521)g(125), \tag{34}$$

where both happen to be the same function by coincidence. Putting all the steps together, we have a function

$$\begin{aligned} f(g_1, g_2) &= \{(521)[g_1(435), (521)g_2(435)(125)](125)\} \\ &= \{(521)g_1(435)(521)g_2(435)(125) \\ &\quad \times (345)g_1^{-1}(521)(345)g_2^{-1}(125)(125)\} \\ &= \{(521)g_1(14352)g_2(124)g_1^{-1}(15342)g_2^{-1}(521)\}, \end{aligned}$$

which can be applied with nine elementary conjugations.

E. Measuring *Z*

The basic idea behind measuring in the computational basis is that if we fuse a flux with another flux of the inverse group element, there is a finite chance that they will have vacuum quantum numbers and disappear. On the other hand, if the product of the two fluxes is not unity then there must be a particle left behind to carry the remaining flux (i.e., the total flux is always conserved).

At this point it might be useful to remind the reader why a fusion of g with g^{-1} will not always turn into the vacuum. The short story is that the combined state is not invariant when another flux encircles them, implying that they have an electric charge component. The state that has vacuum quantum numbers is invariant under the effect of all fluxes, and hence is the sum of all the states in the conjugacy class of g, with the same phase. We can figure out the probability of fusion into the vacuum by calculating the overlap of the vacuum state with the state of two anyons to be fused. The result is

$$P = |\langle \mathrm{vac}(C)|(|g\rangle \otimes |g^{-1}\rangle)|^2 = \frac{1}{|C(g)|}, \tag{35}$$

where $C(g)$ is the conjugacy class of g, and the vacuum state was defined in Sec. II B.

Because one fusion will only probabilistically tell us the desired result, we should repeat the measurement many times to obtain a sufficient degree of accuracy. Besides, if we are working with qudits with $d > 2$ we need to test fusion with at least two different fluxes. We therefore need to have many copies of the state to be measured.

Because of the no-cloning theorem, copying can not be done exactly, but the transformation

$$\sum_i C_i |i\rangle \rightarrow \sum_i C_i |i\rangle \otimes |i\rangle \otimes |i\rangle \otimes \cdots \otimes |i\rangle \tag{36}$$

means that we can measure each of the separate copies in the Z basis and expect to get the same answer. The above transformation can be done with a controlled sum gate (Toffoli gate with one input fixed to $|1\rangle$) from the original state to a $|0\rangle$ ancilla. Repeating this controlled sum gate with many target ancillas will produce the above entangled state.

To summarize, the procedure for measuring in the Z basis is first to create an entangled state using a controlled sum gate. Then try to fuse each of the qudits with one of the inverses of the fluxes that are Z eigenstates. Eventually, one will disappear into the vacuum, and the inverse of the flux of that ancilla is the result. Even in the presence of errors, this measurement will have a good fidelity because the probability of failure is exponentially small in the number of fusions.

A final note is that, because we are always dealing with pairs of fluxes, what fusion really means is that we fuse the first element of our qubit with the first element of the ancilla.

F. Constructing the zero eigenvector of X

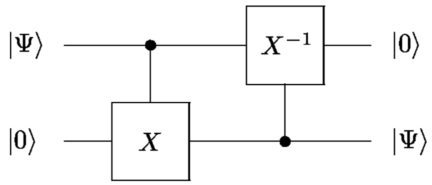
For the next gates, we are going to need a supply of states that are eigenvectors of X with zero eigenvalue:

$$|\tilde{0}\rangle=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle. \tag{37}$$

We will produce them out of pairs of anyons with vacuum quantum numbers. As usual we will just discuss one member of the pair, and assume that the equivalent operations are being performed on the other anyon.

One of the possible states that (when paired) have vacuum quantum numbers is the sum of fluxes in the conjugacy class of b. This is approximately what we want. Sadly, in general, a state created from the vacuum will be a mix of this desired state plus other states, including states that involve dyonic particles (particles with both electric and magnetic charge). We will have to filter through all this noise to get our X eigenstate.

The procedure that we will describe below is effectively an incomplete swap, that has been extended to the full Hilbert space in a logical way. In the computation basis, the operations act as



which performs a swap provided that the second qubit started in the $|0\rangle$ state. Outside of the computational basis, though, the operations are chosen so that we can detect whether we obtained the desired $|\tilde{0}\rangle$ state or not.

We start with two qubit states, one created from the vacuum and one which is a $|0\rangle$ ancilla:

$$|\text{vac}\rangle\otimes|0\rangle=(C|\tilde{0}\rangle+D|\Psi_{\perp}\rangle)\otimes|0\rangle, \tag{38}$$

where $|\Psi_{\perp}\rangle$ is a state orthogonal to the computational subspace. If the vacuum pair decohered into a superselection sector other than the one that contains the computational basis, the constant C will be zero. This will not be a problem as we will be able to detect this case, and then start again from this step.

Using the theorem from Sec. IV D, we can conjugate the $|0\rangle$ ancilla by a function of the flux of the vacuum pair that has the following form:

$$f(a^iba^{-i})=a^i,$$

$$f(\text{anything else})=I, \tag{39}$$

which is essentially a controlled sum gate that has been properly defined outside the computational basis.

The state of the combined system after conjugation will be

$$\frac{C}{\sqrt{d}}\sum_{i=0}^{d-1}|a^iba^{-i}\rangle\otimes|a^iba^{-i}\rangle+\sum_{i=0}^{d-1}D_i|\Psi_{i\perp}\rangle\otimes|a^iba^{-i}\rangle, \tag{40}$$

where $\{D_i\}$ are some constants, and $\{|\Psi_{i\perp}\rangle\}$ are states perpendicular to the computational basis. Note that the states $|\Psi_{i\perp}\rangle$ for $i\neq 0$ are the ones that have flux a^iba^{-i} but have nontrivial charge. The state $|\Psi_{0\perp}\rangle$ includes all the other fluxes and charges. Depending on the superselection sector in which the vacuum state was created, many of the constants C and $\{D_i\}$ will be zero.

Now we conjugate by f^{-1} from the ancilla to the vacuum state yielding

$$C|b\rangle\otimes|\tilde{0}\rangle+\sum_{i=0}^{d-1}D_i|\Psi'_{i\perp}\rangle\otimes|a^iba^{-i}\rangle, \tag{41}$$

where $\{|\Psi'_{0\perp}\rangle\}=\{|\Psi_{0\perp}\rangle\}$ and the states $\{|\Psi'_{i\perp}\rangle,i>0\}$ have flux b but nontrivial charge.

Now we try to fuse the first qubit with an ancilla of flux b^{-1} and trivial charge. The only state that can fuse into the vacuum with the ancilla is $|b\rangle$, and this will happen with finite probability. Note that the ancilla can never vanish into the vacuum with a state with charge because there is no way of extending the basis to be invariant under the stabilizer group of the flux.

In the end, if the particles disappear into the vacuum, the ancilla is left in the desired X eigenstate. Otherwise, we repeat the procedure from the beginning until eventually the state appears.

G. Choosing a dth root of unity

Before we continue building our gate set, we have to address a problem that appears for $d>2$, similar to the problem that occurred for $d=2$ when proving that the gate set is universal.

So far, we have defined everything in terms of ω, a nontrivial dth root of unity. But there are $d-1$ of these, and there is a symmetry which interchanges them. We will have to break this symmetry by using an ancilla.

In particular, we need an ancilla that is an eigenstate of X with eigenvalue not equal to 1. We will then define this state to be the $|\tilde{1}\rangle$ state in the X basis, i.e.,

$$|\tilde{1}\rangle=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}\omega^{-i}|i\rangle, \tag{42}$$

which has eigenvalue ω, thus, fixing our root of unity. We then define the other X eigenstates by

$$|\tilde{n}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \omega^{-ni}|i\rangle, \tag{43}$$

and the operator Z by $|\tilde{n}\rangle \rightarrow |\widetilde{n-1}\rangle$.

How do we produce the first $|\tilde{1}\rangle$ in terms of which everything is defined? We start with a $|\tilde{0}\rangle$ (which is always well defined and which we know how to construct from the preceding section), and we apply a controlled X^{-1} gate (which is a classical function, and thus computable from the Toffoli operator) from this ancilla to a $|0\rangle$ ancilla, which produces the output

$$|\tilde{0}\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{d}} \sum_i |\tilde{i}\rangle \otimes |\tilde{i}\rangle. \tag{44}$$

If we discard the second state, we will have a mixed state that is a combination of the different X eigenstates. This is equivalent to being handed an arbitrarily chosen X eigenstate, which we will call $|\tilde{i}\rangle$.

We can obtain copies of this state by applying a controlled X^{-1} gate from a $|\tilde{0}\rangle$ ancilla to this state, which applies the transformation

$$|\tilde{0}\rangle \otimes |\tilde{i}\rangle \rightarrow |\tilde{i}\rangle \otimes |\tilde{i}\rangle. \tag{45}$$

We can thus build arbitrarily many copies of the state. We still have to worry that this might be the $|\tilde{0}\rangle$ state. However, below in the section for measuring X, we will give a procedure to detect the $|\tilde{0}\rangle$ which does not rely on having $|\tilde{1}\rangle$ ancillas. If we determine that $i=0$, we throw away all the copies and start over (this will only happen with probability $1/d$). Otherwise, we relabel our state as $|\tilde{1}\rangle$, fixing a value for ω.

Because we can copy the $|\tilde{1}\rangle$ state, and below we will also show how to measure it, we can build a reservoir of ancillas in this state, which will be used for all future computations. We can even use copying, comparing, and majority voting to error correct our reservoir, thus allowing for computation even in the presence of noise.

H. Measuring *X*

The last gate needed for universality is the measurement of X. The basic idea is to fuse the pair of anyons that form the state to be measured. The $|\tilde{0}\rangle$ eigenstate will have some overlap with the vacuum, and will vanish with probability $p=d/|C(b)|$, where $C(b)$ is the conjugacy class of b.

The other X eigenstates have zero probability of vanishing because $|\tilde{i}\rangle = 1/\sqrt{d}\Sigma_i \omega^{-i}|a^i b a^{-i}\rangle$ is orthogonal to the vacuum for $i>0$. To detect the state $|\tilde{i}\rangle$, we first apply a Z^i and then use the above fusion procedure. The Z gate can be applied as a controlled sum gate with a $|\tilde{1}\rangle$ target as discussed in Sec. III.

Of course, the above will require us to have many copies on which to measure, which means we need to perform the transformation

$$\sum_i C_i|\tilde{i}\rangle \rightarrow \sum_i C_i|\tilde{i}\rangle \otimes |\tilde{i}\rangle \otimes |\tilde{i}\rangle \otimes \ldots \otimes |\tilde{i}\rangle, \tag{46}$$

which is done using a controlled X^{-1} gate with a $|\tilde{0}\rangle$ ancilla as control and the state to be copied as target.

To perform the measurement nondestructively, we can fuse all but one of the copies of the state. Alternatively, using the Z gate and $|\tilde{0}\rangle$ ancillas, we can always produce the rest of the $|\tilde{i}\rangle$ states. The rest of the logic is similar to the Z measurement procedure.

Having completed the construction of the universal gates, we have proven that universal quantum computation can be performed with anyons from simple and perfect finite groups. We now turn to the question of whether these operations can be performed in a fault-tolerant fashion.

V. LEAKAGE CORRECTION

In this section, we will discuss both the motivation and the techniques needed to implement error correction and fault tolerance in the software of an anyonic computer. The main result will be the construction of a leakage correction circuit for anyons, which enables the use of the standard techniques for handling errors.

A. Motivation

Any quantum system that uses nonlocality to protect its data will be susceptible to errors if a large number of its local components are damaged simultaneously. The probability for failure is generally exponentially small in the size of the system, and is zero in the theoretical limit of an infinite system. However, all physical systems are finite. Furthermore, practical considerations may force a given setup to have a size such that the error of probability is small but nonnegligible.

In the case of anyons, errors can occur due to quantum tunneling, which is an effect of the high-energy degrees of freedom that were frozen out to obtain a two-dimensional discrete gauge theory. The probability of this type of error goes as e^{-mL}, where m is the mass of the lightest particle that can mediate a charge interaction and L is the separation between anyons.

Finite temperature effects are another source of error. These effects involve the creation of charge pairs from the vacuum. Because these pairs have trivial total charge, even if they braid with a computational anyon, the net charges of the collective three particle excitation will still be correct. However, if one of these particles separates from the group, or separately braids with another anyon, then errors will be introduced. The density of the thermal excitations goes as $e^{-\Delta/T}$, where Δ is the mass gap and T is the temperature.

A good anyonic quantum computer should therefore have $L \gg m$ and $T \ll \Delta$. In some implementations, however, it may be more practical to accept a small error rate from the hardware, and then correct it using standard quantum error correction techniques. For such cases, we present below the necessary steps needed to implement software based error correction for anyons.

While any of the error correcting codes can be used, most techniques require embedding a code space inside a Hilbert space on which we can do universal quantum computation. However, in the case at hand, our computational states are embedded in a Hilbert space (the states with arbitrary flux and charge) in which we cannot perform universal quantum computation. Therefore, before starting the recovery protocol, we must first deal with states that have leaked out of the computational subspace (the subspace in which we can perform universal computations).

B. Implementation

To deal with leakage errors we can construct a version of the swap-if-leaked gate described by Kempe *et al.* [13]. The idea behind the gate is to implement a projective measurement that can distinguish the computational subspace from its complement. If a state if found to be in the computational subspace, it is left alone. Otherwise, it is replaced with an arbitrary ancilla that is in the computational subspace. The ancilla will still be an error, but one that is correctable by standard quantum error correcting codes. In fact, the general methods of quantum error correction and fault-tolerant computation can be applied to anyons as long as we can reliably project leaked qubits into a state in the computational subspace.

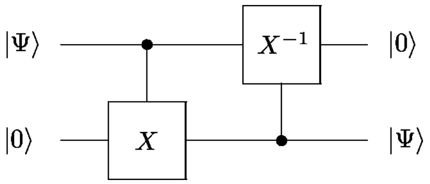
We again focus on the case of simple and perfect groups, and defer the general case to the following section. In the current formalism, the computational basis is the set of states of a pair of anyons with zero total magnetic charge, where each anyon has zero electric charge and a magnetic flux of the form $a^i b a^{-i}$ or its inverse.

The first type of error that we will deal with, is when the total magnetic flux of the pair is nontrivial. This is a particularly grievous error because, if we drag around a pair with a nontrivial net flux, we could be introducing errors into all the other qubits. Furthermore, our assumption that we can perform the operation $h,g \rightarrow h,hgh^{-1}$ relied on the fact that the second pair had zero net magnetic flux, so it is important that we detect and fix this error first.

To detect a net flux, we take an ancilla $|g\rangle \otimes |g^{-1}\rangle$ and encircle it by the qudit we are performing the leakage correction on. The ancilla will get conjugated by the net flux of the qudit, and the qudit will get conjugated by the net flux of the ancilla which should be zero. We then fuse the ancilla with a pair with opposite flux. If the net flux of the qudit is in the stabilizer of g, the fusion will have vacuum quantum numbers with a finite probability, whereas if the conjugation changed the flux of the ancilla, there will always be a particle left behind. If we repeat this many times with many different ancillas $|g\rangle \otimes |g^{-1}\rangle$, with good statistical confidence we will be able to tell if the net flux of the qudit is in the stabilizer of g. Because G has no center, the intersection of all stabilizers is the identity, and hence repeating the above with sufficiently many different elements g, we can detect a nonzero net magnetic charge.

If we detected a net flux, we replace the state with an ancilla in the state $|0\rangle$. Of course, we must be very careful when moving the damaged ancilla pair out of the region of qubits, so as not to damage other states. That is, when moving past other anyons, we always do so in the direction in which the damaged pair gets conjugated and the good qubits are unaffected.

In the case when the qubit passes the above test, then we have projected into the zero net flux subspace, but otherwise left the state unchanged. The next step is to deal with electric charge. Because it is very difficult to measure the electric charge of a single anyon, we will start with a fresh ancilla $|0\rangle$, made from two anyons neither of which have electric charge, and copy the state over. Once again we will be using the incomplete swap circuit,



when acting on the computational basis. Of course, the heart of a leakage detection algorithm is how to extend the operations outside of the computational subspace. The procedure cannot be described simply by a circuit, and therefore we will present a way of completing the controlled sum gate so that the above operation will always yield a state that is in the computational subspace.

The following procedure is almost identical to the one used to produce $|\tilde{0}\rangle$ states. This is because $|\tilde{0}\rangle$ states are obtained by taking a vacuum state and projecting to the computational basis, which is primarily leakage detection. The main difference is that when doing leakage detection, we only get one chance of using the qubit (because of the no-cloning theorem), but if the state leaked, it is acceptable to replace it by anything in the computational basis. The latter is clearly not acceptable when creating $|\tilde{0}\rangle$ ancillas.

We will use the incomplete swap procedure for the second round of leakage detection. Recall that by this point we have projected the qubit into the zero net flux subspace. Take the qubit and a $|0\rangle$ ancilla, and conjugate the ancilla by a function of the qubit's flux:

$$f(a^i b a^{-i}) = a^i,$$

$$f(\text{anything else}) = I. \tag{47}$$

This is the same extension of a controlled sum that was used to produce $|\tilde{0}\rangle$ ancillas.

Afterward, we conjugate the original qubit by $f(g)^{-1}$, where g is the flux of the ancilla. Note that because we know at this point that the original qubit has net flux zero, the state of the ancilla will not exit the computational basis during this operation (though it might change within the computational basis if the original state had nonzero electric charge). The result of the past two controlled sums gate is

$$|\psi_{\parallel}\rangle \otimes |0\rangle + |\psi_{\perp}\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |\psi_{\parallel}\rangle + \sum_{i=0}^{d-1} |\psi_{\perp i}\rangle \otimes |i\rangle, \tag{48}$$

where parallel and perpendicular refer to inside and outside the computational basis, and none of the ψ states are normalized. Finally, we replace the original pair with the ancilla pair and discard the original pair.

Clearly, the new state will be in the computational basis. Furthermore, if the original state was in the computational basis, then the new state will be equal to the old state, and unentangled with the old anyons.

Having complemented our gate set with a leakage correction scheme, we have proven not only that we can do universal quantum computation with anyons, but that these computations can be made fault tolerant.

VI. UNIVERSAL COMPUTATION FOR NONSOLVABLE GROUPS

We will now generalize the results of the preceding section to any nonsolvable group. Unfortunately, in our proofs for the simple perfect case, we made extensive use of the fact that we can compute any classical function simply by multiplying the inputs with ancillas. This is no longer true, even if we restrict ourselves just to perfect groups that are not simple. The quickest example is $A_5 \times A_5$ which is perfect, but has two normal subgroups given by each of the A_5 factors. Thus, if our two inputs are 1×1 and $g\times 1$, there is no expression made out of products in which the results differ in the second factor.

The above example can easily be fixed by working within one A_5 subgroup. In general, though, even this is not possible, as not all perfect groups have a perfect and simple subgroup. However, the following theorem comes to the rescue.

Theorem: If G is a nonsolvable finite group, then there exists a normal subgroup P of G and a subgroup N, normal in P, such that P/N is perfect and simple.
Once again we defer the proof to the Appendix.

What the theorem tells us is that we want to work with cosets of N in P. That is, we would like to replace our old flux eigenstates with states that are labeled by elements in P/N and invariant under N. A good guess would be

$$|x\rangle = \frac{1}{\sqrt{|N|}} \sum_{n\in N} |x'n\rangle, \tag{49}$$

where x is an element of P/N, and x' is an element in the coset that x represents. More specifically, if $f:P\rightarrow P/N$ is the canonical epimorphism that maps elements to cosets, then we require that $f(x')=x$. The particular choice of x' has no effect on the above definition.

The above is a good guess but not quite right. A given coset may intersect many different conjugacy classes of G, each of which lies in a different superselection sector. Thus, we are effectively working with mixed states.

Remembering that we really want to keep our anyons in pairs of zero net flux, the right choice for the new states is

$$\rho_x = \frac{1}{|N|} \sum_{C\in\mathcal{C}(G)} \left[\left(\sum_{x'\in[C\cap f^{-1}(x)]} |x'\rangle \otimes |x'^{-1}\rangle \right) \otimes \left(\sum_{x'\in[C\cap f^{-1}(x)]} \langle x'| \otimes \langle x'^{-1}| \right) \right], \tag{50}$$

where again x is an element of P/N and $\mathcal{C}(G)$ is the set of conjugacy classes of G.

These states have the nice property that when conjugated by any element $h'\in P$ (or equivalently, when a flux $h'\in P$ is dragged around them), the effect only depends on the coset $f(h')$ of h', and generates the transformation

$$\rho_g \rightarrow \rho_{f(h')gf(h')^{-1}}. \tag{51}$$

Because of this, if we use the usual scheme of passing one pair of anyons in between another, and they are both prepared in states of the above form, the net effect is that the inner pair will get conjugated by the outer pair as

$$\rho_h \otimes \rho_g \rightarrow \rho_h \otimes \rho_{hgh^{-1}}, \tag{52}$$

keeping the pair unentangled.

A. New requirements for the physical system

While the operations of braiding, fusion, and vacuum pair creation described in Sec. IV A all seem like reasonable requirements to demand from the physical system, the requirement of flux ancillas is somewhat harder to justify.

In particular, take the case of a group that has a nontrivial center, which can occur even if the group is perfect. Consider two fluxes g and cg that differ by multiplication of an element c in the center. These two fluxes cannot be distinguished by conjugation, since $cgx(cg)^{-1}=gxg^{-1}$. Thus, it may be a difficult problem to distill these flux eigenstates from the vacuum.

A more reasonable assumption is to require the existence of ancillas only for the fluxes in the perfect subgroup. Another improvement might be to assume that we only have ancillas in the mixed states ρ_x defined above, where $x\in P/N$. These states might be easier to produce because they are obtained from the vacuum by first throwing away the anyons with flux not in P or with nontrivial charge, and then projecting to a definite coset of N in P. Therefore, we will replace our old requirement for the existence of flux ancillas by

$(4')$ We have ancillas in the state ρ_x for any $x\in P/N$.

It would be highly desirable to be able to prove that requirements (1)–(4) are sufficient to create the states in $(4')$. Unfortunately, it appears that requirements (1)–(3) combined with $(4')$ may neither be a subset nor a superset of requirements (1)–(4). Thus, in a sense, we are imposing a different set of requirements for this section. One ameliorating fact is that in the case when P is simple, the states ρ_x are just flux eigenstates. We therefore could have used requirement $(4')$ for all sections of this paper. We will not attempt to describe in the Appendix a protocol by which these generalized ancillas can be created, however.

B. Universal computation

As in Sec. IV B, we choose two elements $a,b\in P/N$ such that $a^{d}ba^{-d}=b$ for some prime d, and $a^{i}ba^{-i}\neq b$ for $0<i<d$. We then define our computational basis states as

$$\rho_i=\rho_{a^{i}ba^{-i}}, \tag{53}$$

which we define as eigenstates of the Z operator. The X operator is defined by the action $X(\rho_i)\equiv X\rho_i X^{\dagger}=\rho_{i+1}$ and its eigenstates can be obtained using the projection operators $P_i=\Sigma_{j=0}^{d-1}\omega^{-i}X^{i}/d$ by

$$\rho_{\tilde{i}}=d\times P_i\rho_0 P_i^{\dagger}=\frac{1}{d}\left(\sum_{j=0}^{d-1}\ \omega^{-i}X^{i}\right)\rho_0\left(\sum_{j=0}^{d-1}\ \omega^{i}X^{i\dagger}\right). \tag{54}$$

At this point proving that universal quantum computation can be achieved is fairly straightforward, and is almost identical to the discussion in Sec. IV. The major differences occur when we have to deal with states outside of the computational basis, that is, when creating $\rho_{\tilde{0}}$ states and when dealing with leakage correction. Both of these issues will be dealt with in the following section. As for the rest of the operations, we will only give a very brief discussion.

Because the ρ_x states have the same braiding properties as those of the fluxes of a group P/N (and, in particular two Z eigenstates remain unentangled after braiding), the same method for producing a Toffoli gate applies to them.

Measuring Z is easy because the ρ_i states have support in orthogonal subspaces. The copy (using the Toffoli gate) and fuse with ancillas procedure will work just as well as before.

For the interested reader, we will carry out below some of the calculations needed to deal with X eigenstates and prove universality. Most of the results seem almost miraculous when expressed in the language of density operators. However, the reader should bear in mind that we are only using density operators to account for the different superselection sectors. If we just fixed a superselection sector for each particle, we would be dealing with pure states, and all of the proofs from the past section would carry through.

We begin by studying the action of the controlled X^{-1} gate on X eigenstates:

$$\begin{aligned}\rho_{\tilde{m}}\otimes\rho_{\tilde{n}}&=\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\ \omega^{-im+jm}X^{i}\rho_0X^{j\dagger}\otimes\rho_{\tilde{n}}\\ &\rightarrow\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\ \omega^{-im+jm}X^{i}\rho_0X^{j\dagger}\otimes X^{-i}\rho_{\tilde{n}}X^{-j\dagger}\\ &=\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\ \omega^{-im+jm}X^{i}\rho_0X^{j\dagger}\otimes\omega^{-in}\rho_{\tilde{n}}\omega^{jn}\\ &=\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\ \omega^{-i+j(m+n)}X^{i}\rho_0X^{j\dagger}\otimes\rho_{\tilde{n}}\\ &=\rho_{\widetilde{m+n}}\otimes\rho_{\tilde{n}},\end{aligned} \tag{55}$$

which is equivalent to its action on pure states. Therefore, once we have $\rho_{\tilde{0}}$ states, we can use the same trick as before to break the symmetry and obtain a dth root of unity. That is, we use a controlled X^{-1} gate from the $\rho_{\tilde{0}}$ with a ρ_0 target to create the state

$$\begin{aligned}\rho_{\tilde{0}}\otimes\rho_0&=\left(\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\ X^{i}\rho_0X^{j\dagger}\right)\otimes\left(\sum_{n=0}^{d-1}\sum_{m=0}^{d-1}\ P_n\rho_0P_m^{\dagger}\right)\\ &\rightarrow\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\sum_{n=0}^{d-1}\sum_{m=0}^{d-1}\ X^{i}\rho_0X^{j\dagger}\otimes\omega^{-in+jm}P_n\rho_0P_m^{\dagger}\\ &=d\sum_{n=0}^{d-1}\sum_{m=0}^{d-1}\ (P_n\rho_0P_m^{\dagger})\otimes(P_n\rho_0P_m^{\dagger})\end{aligned} \tag{56}$$

and then discard (trace out) the first state to get the state $\rho=\Sigma_nP_n\rho_0P_n=\Sigma_n\rho_{\tilde{n}}/d$, which gives us an unknown eigenstate of X as before. We then discard and repeat if we obtained the $\rho_{\tilde{0}}$ state, and otherwise we relabel the state as $\rho_{\tilde{1}}$.

Once the $\rho_{\tilde{1}}$ state is available, we can use a controlled sum gate to produce the Z gate, which will allow us to produce any X ancilla including more $\rho_{\tilde{1}}$ states.

Finally, measuring X works by fusing the pair of anyons, because the $\rho_{\tilde{i}}$ are orthogonal to the vacuum for $i>0$. The full measurement proceeds as before by copying, permuting states using the Z gate, and then fusing.

C. Leakage detection and $\rho_{\tilde{0}}$ generation

One final issue remains: How do we measure whether a state is in the computational subspace? Projecting onto the computational subspace is useful because a $\rho_{\tilde{0}}$ is just the projection of a vacuum state to the computational basis. Furthermore, this projection will allow us to perform leakage correction.

One of the new issues that arises for general nonsolvable groups is that if we have a state in the computational basis, and we braid it with an electric charge carrying a nontrivial representation of the subgroup N, then the state will move outside the computational basis. The other issue is that the conjugacy class of an element in G might be larger than the conjugacy class of the element in P, though given that P is normal, the first set will be entirely contained in P.

Let us begin by examining how the leakage correction algorithm must be changed. The first step is to detect whether the net flux or charge of the pair of anyons we are working on has a nontrivial effect on the states ρ_x. The procedure is to braid the pair around the ancilla pair and then fuse the ancilla with another ancilla in the state $\rho_{x^{-1}}$. If the anyon pair has an effect on the ancilla states ρ_x, then the fusion statistics will be altered, and this will be detectable after many repetitions. If our state is found defective we discard it as usual, and replace it by a state in the computational basis. Otherwise, we move on to the next step. Note that if the anyon pair had a net flux in the subgroup N, or in some element outside of P that commutes with P, then the state will still advance to the next round of error correction. However, this anomalous flux or charge will not affect the usual braiding properties.

The second round of error correction is a swap with an ancilla in the ρ_0 state. Note that using our universal classical computation in P we can guarantee that if the original state was in P, the ancilla ends up in the computational basis. However, if the original anyons are outside of P, we will get a state that is within P (because P is normal) but not necessarily in the computational subspace. The final step is to perform a swap with a second ancilla in the ρ_0 state, where now we know that the first ancilla had to be composed of anyons with no charge, and fluxes only in P. This guarantees that the final state of the second ancilla is in the computational basis, and equals the original state if it did not leak, completing the leakage correction procedure.

To create $\rho_{\tilde{0}}$ we also use a swap, this time between a pair created from the vacuum and a ρ_0 ancilla. We then try to fuse the leftover vacuum state with a $\rho_{b^{-1}}$. If they fuse into the vacuum, then the ancilla is in a ρ_0 state. The logic is as follows: if the vacuum pair had electric charge when created, then the swap will not change the charge, and hence it cannot disappear into the vacuum. If the vacuum pair has no electric charge but is outside of P, then the ancilla is still guaranteed to be in P. Furthermore, when conjugating the vacuum state, we will be conjugating by an element in P. The vacuum state will end in a flux state outside of P, which is orthogonal to $\rho_{b^{-1}}$. Finally, if the vacuum pair is a pair of fluxes in P, then it will be of the form $\rho_{\tilde{0}}$, possibly superposed with other states ρ_x outside the computational basis. But the generalized swap can guarantee that a state in P outside of the computational basis, will remain outside of the computational basis (just like in the simple perfect case). Only when the ancilla is in the state $\rho_{\tilde{0}}$ can the fusion into the vacuum occur.

The above procedure for producing $\rho_{\tilde{0}}$ ancillas completes the gate set for nonsolvable groups, and proves the main result of this paper: that anyons with fluxes in a nonsolvable group can perform universal quantum computation.

VII. CONCLUSIONS AND OUTLOOK

While we have shown that universal quantum computation is theoretically feasible for any nonsolvable group, it is still not yet clear whether we will ever be able to build an anyon based computer. First of all there is the fact the smallest nonsolvable group is A_5 which has 60 elements. Obtaining such a group from symmetry breaking seems problematic.

One may wonder whether we can do computation with solvable groups. For Abelian groups, each superselection sector consists of just one state, so it is not possible to encode quantum data in a topologically invariant fashion. Attempts such as [14] encode the quantum data in a superposition of position eigenstates, but this has no more robustness than using superpositions of positions of any other neutral particle of the same mass.

Hope still remains for solvable non-Abelian groups. While producing Toffoli gates using conjugation as in this paper will most likely no longer be feasible, Toffoli gates might still be performed by employing magic states. In fact, Kitaev has such a procedure for the group S_3 [15]. The full set of groups which can perform universal quantum computation remains unknown, but we believe it does not include every non-Abelian group.

Furthermore, there are anyons that are not based on the electric and magnetic charge model (quantum double of a group) presented here. Some of the more exotic anyons are likely to be good quantum computers, but in general, their computational power remains unknown.

We have also neglected to present, in this paper, an account of the resources used to perform computations. While it should be clear that computations can be done with at worst a polynomial overhead in the size of the input, some gates (in particular those that require calculations of arbitrary functions over the group) may require resources that are exponential in the size of the group. A lot of the wasted resources may come from the description in terms of general groups, though. For a fixed group, the resources can probably be significantly reduced.

Finally, there remains the question of physical systems which contain anyons. Because of the requirement of two dimensions, we must look for quasiparticles in some two dimensional medium. There are some indications that non-Abelian anyons may arise in the fractional quantum Hall effect (see Refs. [3,4] and references therein). However, at the moment, there are no physical systems out of which the anyonic computer may be built. Even if no physical implementations are ever found, though, this subject will hopefully still be interesting because of its beautiful mix of computation, particle physics and group theory.

ACKNOWLEDGMENTS

The idea for universal classical computation with simple and perfect groups was initially suggested by Alexei Kitaev, to whom I am highly grateful. The author would also like to thank John Preskill, Jim Harrington, Meg Wessling, and James Chakan.

This work was supported in part by the National Science Foundation under Grant No. EIA-0086038 and by the Department of Energy under Grant No. DE-FG03-92-ER40701.

APPENDIX A: CREATING THE ANCILLAS

As discussed in the main text, the requirement of a supply of calibrated flux ancillas needs further justification. In this section, we will show that for a perfect and simple group, the requirements of braiding, fusion, and vacuum pair creation can be supplemented by one extra measurement to allow the distillation of flux ancillas. We will not cover the general nonsolvable case, though.

The new measurement involves determining whether a single anyon has trivial flux or not. Indeed, this measurement may even be done destructively. The plausibility of this measurement relies on the fact that nonzero flux charges are topologically nontrivial configurations that often have much higher masses than their electric charge counterparts. Naturally, dyons also have large masses and will be detected as having nontrivial flux.

Step 1. Creating electric ancilla pairs. The procedure for creating flux ancillas begins by creating single anyons with zero flux. These are obtained by creating a vacuum pair, measuring the flux of the first particle of the pair, and discarding the second one if the first one had nontrivial flux.

The next step is to create pairs of anyons, where each anyon has zero flux and unknown charge, but the pair has vacuum quantum numbers. Of course, if we could nondestructively distinguish trivial from nontrivial flux, we could skip this step, as the vacuum pairs always have vacuum quantum numbers.

Take two of the single electric charges we have produced. We are going to try to project this state onto the desired state with vacuum quantum numbers. Consider the process of creating a pair of anyons from the vacuum, braiding one of them around the pair of charges, and then fusing the vacuum pair. If the pair of charges had vacuum quantum numbers, then the vacuum pair will remain in the vacuum state throughout this process, and fuse into the vacuum at the end with unit probability. On the other hand, if the pair of charges does not have vacuum quantum numbers, then there will be a finite probability that the pair created from the vacuum will leave a particle behind after fusion (since the vacuum is the only state that is left invariant by the action of every flux).

Repeated application of this process will be a projective measurement which determines whether the pair of charges has vacuum quantum numbers. If we project onto a vacuum pair, then we have found a good charge ancilla pair. If the pair does not project onto the vacuum state (because the two anyons do not transform in conjugate representations, or because we projected to a state orthogonal to the vacuum), then we pair them up with other charges and repeat the process. While slow, this process will eventually yield as many electric charge pairs with vacuum quantum numbers as needed.

Step 2: Identifying the magnetic charges. The electric ancilla pairs are useful because they can perform a nondestructive measurement of magnetic flux. The procedure is to take a member of the electric charge pair, drag it around the anyons or group of anyons whose total flux we want to measure, and then fuse it with its pair.

To describe the effect of the fluxes, let $R(g)$ be the representation of the first electric charge of the pair. Let $|n\rangle$ be an orthonormal basis for the space on which R acts, and let $|n^*\rangle$ be the dual basis for the conjugate representation R^* under which the second charge transforms. The effect of a flux g is then

$$\sum_n |n\rangle\otimes|n^*\rangle\rightarrow\sum_n [R(g)|n\rangle]\otimes|n^*\rangle. \tag{A1}$$

Just as before, if the total flux is nontrivial, there will be a good chance that the fusion of the electric charges will leave a particle behind. On the other hand, if the total flux is trivial, even if the total charge is not, the pair of electric charges will always fuse into the vacuum.

Repeated application of this procedure will determine whether the total flux is trivial or not. Furthermore, this procedure will at worst introduce decoherence in the flux basis, but will leave all flux eigenstates unchanged.

We can use this procedure to compare the fluxes of two anyons. In particular, consider two pairs created from the vacuum. Measure the total flux of the first anyon of the first pair combined with the second anyon of the second pair. If the combined flux is trivial, the first anyon of each pair has the same flux; otherwise the flux is different. The procedure is depicted in Fig. 3.

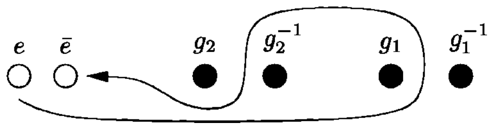


FIG. 3. Using electric charges to check if $g_1 = g_2$.

The above procedure allows us to sort the flux pairs into "bins" that depend on the total flux of the first anyon of the pair. We will get as many bins as elements of G, each containing an unlimited supply of vacuum pairs which carry the same flux in the first anyon of the pair. At this point, if the fluxes have not decohered in the flux basis, then we must have an entangled state involving all anyons in a given bin. Throwing away a single flux from each bin will produce the desired decoherence, just as it did when breaking the various symmetries in the main part of this paper.

All that remains is to identify each bin with an element of G. Assume that we were given an assignment of an element of G to each bin. The assignment could be checked by using the following procedure. First, we note that any finite group G may be described by a set of elements $\{g_i\}$ and a set of relations of the form $g_{i_1}\cdots g_{i_n}=1$ which they obey. To check that the assignment is correct, we just need to check all the relations (supplemented by the trivial one element relations $g_i^n g_i^m = g_i^{nm}$). These can be checked again with the electric charge ancillas, using a loop that circles each of the fluxes in the relation in the correct sequence.

To generate guesses, we could just randomly assign to each bin an element of g, which gives us a probability of success of at least $1/(|G|)!$. Of course, we can be a lot smarter, as the above procedure can help us figure out the powers of a given element (including its inverse) and even the elements in its conjugacy class. Thus, the need for guesswork is minimal, and some of the choices correspond to different valid assignments (i.e., automorphisms) of the group.

Analysis of the produced ancillas. At this point we have almost produced the desired ancillas, with one caveat: the individual anyons do not have trivial charge (i.e., they may be dyons). However, all we have done to the pairs, after creating them from the vacuum, is to measure the flux of one of the anyons. That means that the electric charge portion of the state is still in the vacuum state. More technically, if the ancilla pair circles a flux that commutes with the flux of one anyon of the ancilla, then the state remains unaltered. This is the same behavior that the pure magnetic charges would have.

Some careful thought at this point shows that these states are good enough for the quantum computation procedure presented in the bulk of the paper. Indeed, going back and repeating all the steps with these generalized ancillas would require very few modifications. The fusion to measure in the Z basis would now have a lower success probability, which is compensated by a higher rate of producing acceptable $|\tilde{0}\rangle$

states, but otherwise most gates remain unaltered. We have therefore succeeded in constructing an ancilla reservoir, which, while slightly different then the one initially desired, is useful for universal quantum computation.

APPENDIX B: MATHEMATICAL THEOREMS

This appendix proves the major mathematical theorems needed in the bulk of the paper. We begin by stating the definitions of some of the mathematical terms used.

Perfect group. A nontrivial group G such that $[G,G]=G$. Note that $[G,G]$ is not the set of elements of the form $[g_1,g_2]\equiv g_1g_2g_1^{-1}g_2^{-1}$ but rather the group generated by these elements. Even if G is perfect, there may not be a commutator expression for every element.

Nonsolvable group. A group that has a perfect subgroup.

Normal subgroup. A subgroup H of a group G such that $ghg^{-1}\in H$ for every $h\in H$ and $g\in G$.

Simple group. A group with no normal subgroups other than the whole group and the trivial group.

Before we get to our main theorem, we will prove a theorem that will allow us to deal with general nonsolvable groups. We intend to show that we can extract from nonsolvable groups a simple and perfect group. The simple perfect groups (which can also be described as the simple non-Abelian groups) are the ones on which we can perform universal classical computation and are therefore important for this paper.

We begin by defining the nth derived subgroups by the relations $G^{(n)}=[G^{(n-1)},G^{(n-1)}]$ and $G^{(1)}=[G,G]$. A solvable group is one for which $G^{(i)}=\{1\}$ for some i. A nonsolvable group must have an i such that for every $j>i$, $G^{(i)}=G^{(j)}$ and $G^{(i)}$ is nontrivial. The group $G^{(i)}$ is perfect, thus the definition for solvable groups is consistent with the definition for nonsolvable groups given above.

Furthermore, all the groups $G^{(n)}$ are normal subgroups of G. This can be proven by recalling the property $g[g_1,g_2]g^{-1}=[gg_1g^{-1},gg_2g^{-1}]$. The rest follows by induction because $G^{(1)}$ is normal in G, and $G^{(i)}$ is normal in G if $G^{(i-1)}$ is. We have therefore shown that every nonsolvable group G has a perfect normal subgroup P.

Sadly, this subgroup is not necessarily simple. However, we can prove that every perfect group P has a normal subgroup N such that P/N is perfect and simple. We choose N to be a normal proper subgroup of P such that no other normal proper subgroup of P has more elements, which is well defined because P is finite. Let f be the canonical epimorphism $P\rightarrow P/N$ which maps elements into cosets. Because f is surjective we have $[P/N,P/N]=[f(P),f(P)]=f([P,P])=f(P)=P/N$, which, combined with the fact that P/N is nontrivial, shows that P/N is perfect.

Finally, assume that P/N has a normal, nontrivial proper subgroup A. Then $B=f^{-1}(A)$ is a normal subgroup of P, because for any elements $b_1,b_2\in B$ and $p\in P$, we have $f(b_1b_2)=f(b_1)f(b_2)\in A$ and $f(pb_1p^{-1})=f(p)f(b_1)f(p)^{-1}\in A$. Furthermore, B is a proper subgroup of P, and $N=f^{-1}(1)$ is smaller than $B=f^{-1}(A)$, leading to a contradiction. Therefore, P/N is simple, and we have finished proving the following theorem.

Theorem. If G is a nonsolvable finite group, then there exists a normal subgroup P of G and a subgroup N, normal in P, such that P/N is perfect and simple.

Proof. Shown by the above text.

We now turn our attention to using our groups to compute classical functions. We shall prove that the set of functions that can be written in product form is complete, in the sense that it includes every function from $G^n\rightarrow G$, if G is simple and perfect (or equivalently simple and non-Abelian). This was first proven in the mathematical literature by Maurer in 1965 [16]. In the computer science literature, a related result was proven by Barrington [17]. In this paper, we will provide our own constructive proof for the following theorem.

Theorem. If G is a simple and perfect finite group, then any function $f(g_1,\ldots,g_n):G^n\rightarrow G$ can be expressed as a product of the inputs $\{g_i\}$, their inverses $\{g_i^{-1}\}$ and fixed elements of G, any of which may appear multiple times in the product.

Proof. Throughout this proof, we will refer to the set of functions that can be expressed in the above form as "computable." Proving the above statement is equivalent to showing that all functions are computable. The proof consists of building a series of computable δ functions that map most elements to the identity, and then expressing arbitrary functions as a product of these δ functions.

Step 1. Given a group element a not equal to the identity, let $C(a)$ denote its conjugacy class. Then the subgroup generated by the elements of $C(a)$ is equal to G. This is because the subgroup is a nontrivial, normal subgroup of G and G is simple.

Step 2. Fix two disjoint subsets A and B of G. Define a family of functions $\{\delta_c^{A,B}(g):A\cup B\rightarrow G\}$ with elements labeled by $c\in G$:

$$\delta_c^{A,B}(g)=\begin{cases}1 & \forall\ g\in A\\ c & \forall\ g\in B.\end{cases}\tag{B1}$$

If the function $\delta_c^{A,B}$ is computable for some $c\neq 1$, then every function in the family is computable. To prove this choose any $d\in G$. By step 1 there is an expression for d as a product of elements in the conjugacy class of c (for instance, $d=g_1cg_1^{-1}g_2cg_2^{-1}c$). Then $\delta_d^{A,B}$ is obtained by substituting $\delta_c^{A,B}$ for c in the expression.

Step 3. Fix a set A, an element b not in A, and an element $x\neq b$. If a function $\delta_c^{A,B}$ is computable for some B such that $b\in B$, then there exists a computable function $\delta_c^{A',B'}$ with two new sets such that $A\cup\{x\}\subset A'$ and $b\in B'$. The function can be obtained from

$$\delta_e^{A',B'}(g)=[\delta_d^{A,B}(g),gx^{-1}]\tag{B2}$$

using Step 2. The above equation assumes that we have extended the domain of $\delta_d^{A,B}$ to G, which can be done in a natural way once we have fixed a product representation for $\delta_d^{A,B}$. The element d was chosen not to commute with bx^{-1}. Such an element must exist because G is simple and non-Abelian, and hence has no center. The element e is just $e=[d,bx^{-1}]$.

Step 4. The functions defined by $\delta_c^b(g)\equiv\delta_c^{A,B}$, with $A=G-\{b\}$ and $B=\{b\}$, are computable. To prove this start with $A_1=\{1\}$ and $B_1=\{b\}$. The function $\delta_c^{A_1,B_1}$ is computable because it is in the same family as $f(g)=g=\delta_g^{A_1,B_1}$. Then proceed by induction, using Step 3, on the elements in $G-\{b\}$ that are not included in A_i.

Step 5. For a fixed set of ordered elements $b_1,\ldots,b_i$ define a family of functions labeled by c:

$$\delta_c^{b_1,\ldots,b_i}(g_1,\ldots,g_i)=\begin{cases} c & \text{for } g_1=b_1,\ldots, \text{ and } g_i=b_i, \\ 1 & \text{otherwise.}\end{cases} \tag{B3}$$

The same proof in Step 2 shows that if any function of the family with $c\neq 1$ is computable, then the entire family is computable.

Step 6: Fix $i\in Z^+$ and elements $b_1,\ldots,b_{i+1}\in G$. If the function $\delta_c^{b_1,\ldots,b_i}(g_1,\ldots,g_i)$ is computable, then so is the function $\delta_c^{b_1,\ldots,b_{i+1}}(g_1,\ldots,g_i,g_{i+1})$. By Step 5 it is sufficient to be able to compute

$$\delta_e^{b_1,\ldots,b_{i+1}}(g_1,\ldots,g_{i+1}) =[\delta_c^{b_1,\ldots,b_i}(g_1,\ldots,g_i),\delta_d^{b_{i+1}}(g_{i+1})], \tag{B4}$$

where the function $\delta_d^{b_{i+1}}(g_{i+1})$ is computable by Step 4, and d is chosen so that $e=[c,d]\neq 1$.

Step 7. Using induction on the number of inputs of the function, and starting from the base case $\delta_c^{b_1}(g_1)$, it is clear that all the functions defined in Step 5 are computable.

Step 8. Every function is computable because

$$f(g_1,\ldots,g_i)=\prod_{b_1\in G}\ldots\prod_{b_i\in G}\delta_{f(b_1,\ldots,b_i)}^{b_1,\ldots,b_i}(g_1,\ldots,g_i).$$

Q.E.D.

[1] A.Yu. Kitaev, e-print quant-ph/9707021.

[2] M. Freedman, A. Kitaev, M. Larsen, and Z. Wang, e-print quant-ph/0101025.

[3] R.W. Ogburn and J. Preskill, *Topological Quantum Computation*, in Proceeding of *QCQC '98*, edited by Colin P. Williams (Springer-Verlag, Berlin, 1999), pp. 341–356.

[4] J. Preskill, e-print quant-ph/9712048.

[5] M. de Wild Propitius and F.A. Bais, e-print hep-th/9511201.

[6] F.A. Bais, P. van Driel, and M. de Wild Propitius, Phys. Lett. B **280**, 63 (1992).

[7] A.Yu. Kitaev, e-print quant-ph/9511026.

[8] Y. Shi, e-print quant-ph/0205115.

[9] D. Gottesman, e-print quant-ph/9802007.

[10] W. Burnside, *Theory of Groups of Finite Order*, 2nd ed. (Dover, New York, 1955), Note M.

[11] W. Feit and J.G. Thompson, Pac. J. Math **13**, 775 (1963).

[12] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups* (AMS, Providence, RI, 1994).

[13] J. Kempe, D. Bacon, D.P. DiVincenzo, and K.B. Whaley, Quantum Information Comput **1**, 33 (2001).

[14] S. Lloyd, e-print quant-ph/0004010.

[15] A.Yu. Kitaev (private communication).

[16] W.D. Maurer and J.L. Rhodes, Proc. Am. Math. Soc. **16**, 552 (1965).

[17] D.A. Barrington, J. Comput. Syst. Sci. **38**, 150 (1989).