Universal quantum computation with the $\nu=5/2$ fractional quantum Hall state

Sergey Bravyi
IBM Watson Research Center, Yorktown Heights, New York 10598, USA
and Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA

(Received 6 January 2006; published 12 April 2006)

We consider topological quantum computation (TQC) with a particular class of anyons that are believed to exist in the fractional quantum Hall effect state at Landau-level filling fraction $\nu=5/2$. Since the braid group representation describing the statistics of these anyons is not computationally universal, one cannot directly apply the standard TQC technique. We propose to use very noisy nontopological operations such as direct short-range interactions between anyons to simulate a universal set of gates. Assuming that all TQC operations are implemented perfectly, we prove that the threshold error rate for nontopological operations is above 14%. The total number of nontopological computational elements that one needs to simulate a quantum circuit with L gates scales as $L(\ln L)^3$.

DOI: 10.1103/PhysRevA.73.042313 PACS number(s): 03.67.Lx

I. INTRODUCTION

One of the most important results in the theory of fault-tolerant quantum computation is the threshold theorem. It asserts that ideal quantum circuits can be efficiently simulated by noisy circuits if an error rate of individual gates is smaller than a certain constant threshold value δ; see [1–4]. Estimates of δ vary from $10^{-7}-10^{-4}$ for a local architecture [5,6] to $10^{-5}-10^{-2}$ for nonlocal gates [4,7]. With the present technology these rates are hardly achievable by any real device. Moreover, for practical computations it is desirable to have an error rate much smaller than δ; otherwise, one may need too many concatenation levels and the simulation overhead may become too large.

These challenges can be overcomed (at least partially) in the *topological quantum computation* (TQC) scheme developed by Kitaev and co-workers [8–10]. It makes use of the fact that elementary excitations of some two-dimensional (2D) many-body quantum systems are *anyons*—spatially localized quasiparticles with unusual exchange statistics described by nontrivial representations of the braid group. For the purposes of TQC one needs *non-Abelian anyons* (corresponding to multidimensional braid group representations). A computation is carried out by creating pairs of anyons from the ground state, separating them far apart, transporting individual anyons adiabatically around each other, and finally fusing pairs of anyons together. A list of particle types produced in the fusion is the classical outcome of the computation. An error rate of individual gates in TQC is expected to be much smaller than δ.

A physical system that may serve as a platform for TQC is a two-dimensional electron gas in the fractional quantum Hall effect (FQHE) regime. The FQHE plateau at the filling fraction $\nu=5/2$ was observed by Willett *et al.* [11] in the late 1980s. Shortly after that Moore and Read [12] developed a theory predicting that elementary excitations of the $\nu=5/2$ state are non-Abelian anyons. The corresponding braid group representation was found by Nayak and Wilczek [13]. For the sake of brevity we shall refer to the anyons existing in the $\nu=5/2$ state as *Ising anyons* (their exchange statistics can be described by monodromy of holomorphic correlation functions of the 2D Ising model [12]).

From the experimental point of view, Ising anyons have many favorable properties. A large quasiparticles gap (estimated as $\Delta \geqslant 100$ mK in [14]) suppresses thermal creation of "stray" particles, while nonzero electric charge permits control of anyons using electrostatic gates. Besides, one can take advantage of the well-developed FQHE experimental technology. An experimental setup for controlling Ising anyons and testing their statistics has been recently proposed by several authors [15–18]. An error rate for the one-qubit σ^x operation has been estimated as 10^{-30} in [15].

The only fact that prevents one from using Ising anyons for TQC is that the braid group representation describing their statistics is not computationally universal. We shall see that one can easily compute an amplitude of any braiding process; see Sec. III. Loosely speaking, TQC with Ising anyons is an intersection of two computational models known to be classically simulatable: quantum circuits with Clifford gates [19–21] and fermionic linear optics [22–24]. Therefore, Ising anyons offer only reliable storage of quantum information and reliable implementation of a certain nonuniversal gate set; see Sec. III for details.

The goal of the present paper is to argue that this drawback is not as serious as it might seem. We show that a universal gate set can be simulated by standard TQC operations—i.e., adiabatic transport and fusion of anyons—and very noisy nontopological operations, such as direct short-range interaction of anyons. The latter can be thought of as a tunneling process in which two anyons exchange a virtual quasiparticle. It can be implemented by transporting two anyons sufficiently close to each other, waiting for an appropriate period of time, and then returning the anyons to the original positions. Another example of a nontopological computational element is a two-point contact interferometer proposed in [16–18]. It has the geometry of a Hall bar with two constrictions, such that quasiparticle tunneling occurs between two edge currents on the opposite edges of the bar. The tunneling current is sensitive to the total topological charge of anyons trapped inside the interferometer loop. We will show that the short-range interaction and two-point contact interferometer together with TQC operations provide a universal gate set.

1050-2947/2006/73(4)/042313(16)/$23.00

Our main result concerns the threshold error rate of nontopological operations. To avoid propagation of errors we apply all nontopological operations before the computation itself to prepare a supply of "computationally universal" ancillary states from the vacuum. In our scheme there will be two types of ancillary states: a four-particle state $|a_4\rangle$ and an eight-particle state $|a_8\rangle$. From the computational perspective, $|a_4\rangle$ can be identified with a one-qubit state $2^{-1/2}(|0\rangle + e^{i\pi/4}|1\rangle)$ (we represent a qubit by four quasiparticles). Analogously, $|a_8\rangle$ can be identified with a two-qubit state $2^{-1/2}(|0,0\rangle + |1,1\rangle)$. One copy of $|a_8\rangle$ together with TQC operations allows the implementation of the conrolled-NOT (CNOT) gate. One copy of $|a_4\rangle$ together with TQC operations and CNOT gates allows one to implement the one-qubit $\pi/8$ rotation. Summarizing, universal computation can be carried out by TQC operations if a supply of states $|a_4\rangle$ and $|a_8\rangle$is available.

Since nontopological operations are not perfect, in practice one can prepare only some very noisy ancillary states ρ_4 and ρ_8 approximating $|a_4\rangle$ and $|a_8\rangle$ up to some precision. We characterize this precision by two parameters

$$\epsilon_4 = 1 - \langle a_4|\rho_4|a_4\rangle \quad \text{and} \quad \epsilon_8 = 1 - \langle a_8|\rho_8|a_8\rangle .$$

We prove that the ideal states $|a_4\rangle$ and $|a_8\rangle$ can be distilled from many copies of ρ_4 and ρ_8 by TQC operations provided that (i) all TQC operations are perfect, (ii) $\epsilon_4 < 0.14$, and (iii) $\epsilon_8 < 0.38$.

A distillation method that we use is a combination of "magic states distillation" proposed in [25] and a slightly modified version of the entanglement purification protocol of Bennett *et al.* [26,27].

Summarizing, if one can prepare the states $|a_4\rangle$, $|a_8\rangle$ accurately enough, such that the conditions above are satisfied, then any quantum computation can be efficiently simulated by Ising anyons. The overall simulation requires only polylogarithmic overhead. Specifically, the number of noisy ancillas ρ_4 and ρ_8 and the number of TQC operations that one needs to simulate a quantum circuit with L gates scales as $L(\ln L)^3$.

In the case when one can meet only the condition $\epsilon_8 < 0.38$, TQC operations allow one to implement any Clifford gates (i.e., the CNOT gate, the Hadamard gate, and the one-qubit $\pi/4$ rotation). Though these gates do not constitute a universal set, they are sufficient to implement any error correction scheme based on stabilizer codes [28]. Error correction might be needed if one takes into account finite error rate of TQC operations (which is neglected throughout this paper).

Our derivation of the threshold conditions (ii) and (iii) is based on a single assumption regarding the error model characterizing nontopological operations—they must obey the superselection rules of Ising anyons. Accordingly, we assume that matrix elements of ρ_4 and ρ_8 are nonzero only for the vacuum sector (recall that each ancilla is prepared from the vacuum).

The rest of the paper is organized as follows. Section II provides the necessary background on Ising anyons. In Sec. III a TQC with Ising anyons is discussed and its classical simulatibility is proved. Section IV describes a distillation method for the state $|a_8\rangle$. We show how to use ancillas $|a_8\rangle$ to implement Clifford group gates in Sec. V. Finally, in Sec. VI we make use of the magic-states distillation protocol to simulate universal computation. Also the efficiency of the simulation is analyzed. Some particular nontopological ancilla preparation methods are discussed in Sec. VII.

II. ISING ANYONS

A complete specification of any class of anyons is rather complicated and involves a lot of data including a list of particle types, their fusion and braiding rules, S matrices, etc.; see [29] for a comprehensive review and [16] for a detailed discussion of Ising anyons in the context of the FQHE. In this section we briefly outline the properties of Ising anyons, focusing on those relevant for quantum computation.

A. Particle types and fusion rules

There are two nontrivial particle types in the class of Ising anyons. We shall label them by $\boldsymbol{\sigma}$ and $\boldsymbol{\psi}$. Particles of different types cannot be converted to one another (or to the vacuum) by a local operator, thus describing superselection sectors of the model. However, if one brings two particles close to each other, they can fuse into a single one or annihilate each other, forming a topologically trivial particle (belonging to the vacuum sector). Admissible interconversions of particles are formally described by the fusion rules

$$\psi \times \psi = \mathbf{1}, \quad \psi \times \sigma = \sigma, \quad \sigma \times \sigma = \mathbf{1} + \psi. \tag{1}$$

Here **1** stands for the vacuum sector. The most important for us is the last rule. It implies that a pair of σ particles can be prepared in two orthogonal states that differ by the total topological charge. Computing a product $\sigma \times \cdots \times \sigma$ for $2n$ σ particles one can easily get

$$\sigma^{\times 2n} = 2^{n-1}\mathbf{1} + 2^{n-1}\psi. \tag{2}$$

Thus, if one creates $2n$ σ particles from the vacuum, there is a 2^{n-1}-dimensional subspace of states that can be distinguished by fusing some pairs of particles together and observing the type of resulting particles. It is used as a computational space in the TQC scheme.

B. Braid group representation

Recall that the exchange statistics of particles residing in the $(2+1)$-dimensional space-time is described by unitary representations of the braid group rather than the symmetric group (because the clockwise and counterclockwise exchanges are not equivalent). The braid group $\mathcal{B}_n$ with n strings can be formally described by the generators b_j, b_j^{-1}, $j=1,\ldots,n-1$ (see Fig. 1), which obey the Yang-Baxter relations

$$b_j b_k = b_k b_j \quad \text{for } |j-k| > 1,$$

$$b_j b_{j+1} b_j = b_{j+1} b_j b_{j+1} \quad \text{for } j = 1, \ldots, n-2. \tag{3}$$

The strings can be thought of as world lines of particles, whose initial and final positions are chosen on the x axis.

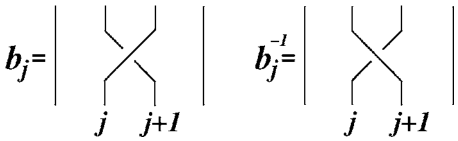

FIG. 1. Braid group generators.

The exchange statistics of σ particles is described by the *spinor representation* of the braid group [13]:

$$\varphi:\mathcal{B}_{2n} \to U(2^n).$$

It is constructed using the spinor representation of the orthogonal group SO$(2n)$. Let us introduce the Pauli operators σ_j^x, σ_j^y, and σ_j^z on n qubits and auxiliary *Majorana operators* $\hat{c}_1, \hat{c}_2, \ldots, \hat{c}_{2n}$ defined as

$$\hat{c}_{2j-1} = \sigma_1^z \otimes \cdots \otimes \sigma_{j-1}^z \otimes \sigma_j^x \otimes I_{j+1} \otimes \cdots \otimes I_n,$$

$$\hat{c}_{2j} = \sigma_1^z \otimes \cdots \otimes \sigma_{j-1}^z \otimes \sigma_j^y \otimes I_{j+1} \otimes \cdots \otimes I_n, \tag{4}$$

where I stands for the one-qubit identity operator and j runs from 1 to n. The Majorana operators obey commutation rules

$$\hat{c}_p\hat{c}_q + \hat{c}_q\hat{c}_p = 2\delta_{pq}I, \quad \hat{c}_p^\dagger = \hat{c}_p, \quad \text{for any } p,q.$$

Then the spinor representation of the braid group generators $b_1, \ldots, b_{2n-1}$ is defined as

$$\varphi(b_p) = \exp\left(-\frac{\pi}{4}\hat{c}_p\hat{c}_{p+1}\right) = \frac{1}{\sqrt{2}}(I - \hat{c}_p\hat{c}_{p+1}).$$

[We have omitted the overall phase of $\varphi(b_p)$, since it is irrelevant for quantum computation purposes.]

The Yang-Baxter relations can be easily verified using the following identity:

$$\varphi(b_p)\hat{c}_q\varphi(b_p)^\dagger = \begin{cases} \hat{c}_q, & \text{if } q \notin \{p,p+1\}, \\ \hat{c}_{p+1}, & \text{if } q = p, \\ -\hat{c}_p, & \text{if } q = p+1. \end{cases}$$

It says that an exchange of adjacent σ particles is equivalent to an exchange of the corresponding Majorana operators (up to a sign).

C. Topological charge measurements

The multidimensionality of the braid group representation accounts for the fact that there is more than one way to fuse $2n$ σ particles into the vacuum (or into ψ particles). A process in which two adjacent σ particles p and $p+1$ are fused together and then a type of the resulting particle (**1** or ψ) is observed can be described as a projective measurement of an observable

$$F_p = -i\hat{c}_p\hat{c}_{p+1}.$$

The eigenvalues +1 and −1 correspond to the resulting particle's type **1** and ψ, respectively.

A type of a particle that one would obtain by fusing together all $2n$ σ particles is measured by a *parity operator*

$$Q = \sigma_1^1 \otimes \cdots \otimes \sigma_n^z = (-i)^n\hat{c}_1\hat{c}_2\cdots\hat{c}_{2n}. \tag{5}$$

Note that Q commutes with the action of any braid group element, as well as with observables F_p. This is a manifestation of the superselection rules—any local operator preserves the total topological charge. Any state $|\Psi\rangle$ of $2n$ σ particles that can be created from the vacuum obeys $Q|\Psi\rangle = +|\Psi\rangle$. Analogously, $|\Psi\rangle$ can be prepared starting from a single $\boldsymbol{\psi}$ particle iff $Q|\Psi\rangle = -|\Psi\rangle$.

Remark. Strictly speaking, fusion is a process reducing the Hilbert space of states, since it replaces two particles by one. To simplify the notation we describe fusion as a projective measurement. This is justified, since a fusion can always be followed by an auxiliary fission process in which the resulting **1** or $\boldsymbol{\psi}$ particle is split into a pair of σ particles.

III. TOPOLOGICAL QUANTUM COMPUTATION WITH ISING ANYONS

The goal of this section is to introduce a computational model that captures all features of TQC with Ising anyons. We will show that any computation within this model can be efficiently simulated classically. Finally, we describe a natural encoding of a qubit by σ particles.

A. Formal computational model

To define a formal model we just need to extract its constituents from Sec. II—the computational Hilbert space with a fiducial initial state, a set of unitary gates, and a set of admissible measurements.

The computational Hilbert space of n qubits,

$$\mathcal{F}_n = (\mathbb{C}^2)^{\otimes n},$$

will be represented by $2n$ σ particles. The initial state $|\mathbf{0}\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$ is prepared by preparing pairs of σ particles, $(1,2), \ldots, (2n-1,2n)$, from the vacuum.

A set of elementary unitary gates includes nearest-neighbor exchange operations

$$B_p \equiv \varphi(b_p) = \exp\left(-\frac{\pi}{4}\hat{c}_p\hat{c}_{p+1}\right).$$

For any $p < q$ define a nonlocal exchange operation

$$B_{p,q} = \exp\left(-\frac{\pi}{4}\hat{c}_p\hat{c}_q\right). \tag{6}$$

Its conjugated action on the Majorana operators is

$$B_{p,q}\hat{c}_r B_{p,q}^\dagger = \begin{cases} \hat{c}_r, & \text{if } r \notin \{p,q\}, \\ \hat{c}_q, & \text{if } r = p, \\ -\hat{c}_p, & \text{if } r = q. \end{cases} \tag{7}$$

One can easily verify that a nonlocal exchange is a composition of $O(n)$ nearest-neighbor exchanges; namely, for any $p \leq q-2$ one has

$$B_{p,q} = B_{q-1}\cdots B_{p+1}B_pB_{p+1}^\dagger\cdots B_{q-1}^\dagger.$$

The operations $B_{p,q}$ constitute a set of elementary unitary gates in our model. We shall refer to them as *braid gates*.

Finally, a set of measurements includes nearest-neighbor two-particle fusion processes—i.e., nondestructive projective measurements of observables $F_p=-i\hat{c}_p\hat{c}_{p+1}$. For any $p<q$ define an observable

$$F_{p,q} = -\, i\hat{c}_p\hat{c}_q.$$

Taking into account that $F_{p,q}=B_{p+1,q}F_pB^\dagger_{p+1,q}$, we can also measure eigenvalues of any observable $F_{p,q}$. Summarizing, the formal computational model is as follows: (i) the Hilbert space $\mathcal{F}_n=(\mathbb{C}^2)^{\otimes n}$, (ii) the initial state $|\mathbf{0}\rangle=|0\rangle\otimes\cdots\otimes|0\rangle$, (iii) Braid gates $B_{p,q}=\exp\left(-\frac{\pi}{4}\hat{c}_p\hat{c}_q\right)$, and (iv) measurable observables $F_{p,q}=-i\hat{c}_p\hat{c}_q$.

We shall refer to this list as a TQC model. It will be assumed throughout this paper that TQC operations are implemented perfectly (a storage of quantum states in $\mathcal{F}_n$ is also assumed to be perfect).

B. Classical simulation of TQC with Ising anyons

The fact that any computation in the TQC model can be simulated classically follows easily from the Gottesman-Knill theorem; see [19]. Indeed, taking into account the relation, Eq. (4), between the Pauli matrices and the Majorana operators and the conjugated action of the braid gates, Eq. (7), one can easily prove that any braid gate maps Pauli operators to Pauli operators under a conjugation. Thus all braid gates belong to the Clifford group. Since the set of measurable observables includes only Pauli operators, we can directly apply the stabilizer formalism [20,21] to simulate the TQC.

Another way to deduce the same result is to relate the TQC model and the fermionic linear optics (FLO); see [22–24]. A theorem proved in these papers asserts that any computation within the FLO model can be efficiently simulated classically. In terms of FLO operations, the initial state $|\mathbf{0}\rangle$ is the Fock vacuum and the braid gates, Eq. (6), are just special case of Bogolyubov canonical transformations, while the observables $F_{p,q}$ measure single-mode occupation numbers. Then the classical simulatibility of the TQC model follows directly from [24].

Loosely speaking, TQC with Ising anyons is an intersection of two computational models known to be classically simulatable: the Clifford group and stabilizer formalism model and the FLO. This is the reason why we need two types of "computationally universal" ancillary states. The ancilla $|a_4\rangle$ takes us beyond the Clifford group model, while the ancilla $|a_8\rangle$ introduces a nonlinearity necessary to go beyond the FLO model.

In the remainder of this subsection we explicitly describe a set of unitary operators and a set of quantum states that can be achieved by TQC operations.

Let $G\subset U(2^n)$ be a group generated by braid gates $B_{p,q}$ for $2n$ σ particles. To describe G note that a subgroup $H\subset G$ generated by double exchanges $B_p^2=-\hat{c}_p\hat{c}_{p+1}$, $p=1,\ldots,2n-1$, coincides with the set of all *even* products of Majorana operators (we do not care about the overall phase of operators). Thus, if one parametrizes a product of Majorana operators $\hat{c}_1^{x_1}\cdots\hat{c}_{2n}^{x_{2n}}$ by a binary $2n$-bit string $(x_1,\ldots,x_{2n})$, we get $H\cong(\mathbb{Z}_2)^{2n-1}$. Moreover, the subgroup H is normal:$B_pHB_p^\dagger=H$ for any p. One can easily check that the factor group G/H coincides with the permutation group S_{2n} of $2n$ objects. Thus G can be represented as a semidirect product:

$$G=(\mathbb{Z}_2)^{2n-1}\rtimes S_{2n}.$$

To characterize the set of quantum states that can be prepared by TQC operations, note that the initial state $|\mathbf{0}\rangle$ is a stabilizer state with a stabilizer group

$$S=(\hat{c}_1\hat{c}_2,\hat{c}_3\hat{c}_4,\ldots,\hat{c}_{2n-1}\hat{c}_{2n}).$$

Applying any sequence of braid gates $B_{p,q}$ to this state is equivalent to updating the stabilizer group according to Eq. (7). A new stabilizer group is

$$S'=(\hat{c}_{p(1)}\hat{c}_{p(2)},\hat{c}_{p(3)}\hat{c}_{p(4)},\ldots,\hat{c}_{p(2n-1)}\hat{c}_{p(2n)}), \qquad (8)$$

where p is a permutation of the numbers $\{1,2,\ldots,2n\}$.

Let $|\psi\rangle$ be any state with a stabilizer group S' as above. A measurement of an observable $F_{p,q}$ has nontrivial effect on $|\psi\rangle$ only if $\hat{c}_p\hat{c}_q$ is not a stabilizer of $|\psi\rangle$. In this case p and q must belong to different pairs; i.e., $\hat{c}_r\hat{c}_p$ and $\hat{c}_q\hat{c}_s$ are stabilizers of $|\psi\rangle$ for some integers $r\neq s$. Moreover, these are the only generators of S'that anticommute with $F_{p,q}$. Therefore, measuring eigenvalue of $F_{p,q}$ is equivalent to updating the stabilizer group according to

$$(\ldots,\hat{c}_r\hat{c}_p,\hat{c}_q\hat{c}_s,\ldots)\rightarrow(\ldots,\hat{c}_r\hat{c}_s,\hat{c}_p\hat{c}_q,\ldots).$$

We conclude that any state one can get from the initial state $|\mathbf{0}\rangle$ by TQC operations can be described by a stabilizer group, Eq. (8) for some permutation $p\in S_{2n}$.

Remark. In the arguments above we have ignored eigenvalues associated with stabilizer operators which may be either $+i$ or $-i$. Naturally, after each transformation one has to update the eigenvalues as well. For simplicity we skip these details.

C. Representation of a qubit

So far we represented a single qubit by a pair of σ particles. Although this is the most efficient representation in terms of resources, it has some serious drawbacks. Since a pair of σ particles prepared in the basis states $|0\rangle$ and $|1\rangle$ has the total topological charge $\mathbf{1}$ and ψ, respectively, a qubit cannot be prepared in a superposition of the basis states—e.g., $|0\rangle\pm|1\rangle$—because they violate the superselection rules.

For this reason we shall represent a logical qubit by a group of four σ particles. The basis states $|\bar{0}\rangle$ and $|\bar{1}\rangle$ of a logical qubit will be identified with physical states $|0,0\rangle\in\mathcal{F}_2$ and $|1,1\rangle\in\mathcal{F}_2$. Both these states have trivial total charge. A computational subspace spanned by $|0,0\rangle$ and $|1,1\rangle$ can be specified by an eigenvalue equation

$$-\,\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4|\psi\rangle=|\psi\rangle. \qquad (9)$$

Logical Pauli operators $\bar{\sigma}^x$, $\bar{\sigma}^y$, and $\bar{\sigma}^z$ acting on the computational subspace can be chosen as

$$\bar{\sigma}^z=-\,i\hat{c}_1\hat{c}_2,$$

$$\bar{\sigma}^x = -i\hat{c}_2\hat{c}_3,$$

$$\bar{\sigma}^y = -i\hat{c}_1\hat{c}_3. \tag{10}$$

Clearly, logical Pauli operators can be implemented by braid gates—for example, $\bar{\sigma}^z$ corresponds to winding the particle 1 around the particle 2. Besides, TQC operations allow one to measure an eigenvalue of the logical one-qubit Pauli operators.

Note that any four-particle braid gate commutes with the parity operator $\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$; i.e., it implements some logical one-qubit gate. To find a subgroup of U(2) generated by these gates, it suffices to consider the braid gates $B_{1,2}$, $B_{2,3}$, and $B_{3,4}$. In terms of logical Pauli operators one has

$$B_{1,2} = B_{3,4} = \exp\left(-i\frac{\pi}{4}\bar{\sigma}^z\right) = e^{-i\pi/4}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix},$$

$$B_{2,3} = \exp\left(-i\frac{\pi}{4}\bar{\sigma}^x\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}.$$

(By abuse of notation, we identify a braid gate and the corresponding logical operator.) These gates generate the one-qubit Clifford group $\mathrm{Cl}(1)\subset \mathrm{U}(2)$.

The four-particle qubit representation also has some drawbacks which come out if one considers two logical qubits. Let us show that any two-qubit logical state

$$|\psi\rangle = a|\bar{0},\bar{0}\rangle + b|\bar{0},\bar{1}\rangle + c|\bar{1},\bar{0}\rangle + d|\bar{1},\bar{1}\rangle \in \mathcal{F}_4$$

that can be prepared by TQC operations has a product form

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Here $|\psi_1\rangle$ and $|\psi_2\rangle$ are some logical one-qubit states. Indeed, we already know that $|\psi\rangle$ obeys stabilizer equations

$$\hat{c}_{p(1)}\hat{c}_{p(2)}|\psi\rangle = \pm i|\psi\rangle, \ldots, \hat{c}_{p(7)}\hat{c}_{p(8)}|\psi\rangle = \pm i|\psi\rangle, \tag{11}$$

for some permutation $p\in S_8$; see Eq. (8). On the other hand, the assumption that $|\psi\rangle$ is a logical two-qubit state implies that

$$-\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4|\psi\rangle = -\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8|\psi\rangle = |\psi\rangle. \tag{12}$$

Obviously, Eqs. (11) and (12) are consistent with each other iff for any $1\leqslant j\leqslant 4$ one has

$$p(2j-1), p(2j) \in \{1,2,3,4\},$$

or

$$p(2j-1), p(2j) \in \{5,6,7,8\}.$$

In other words, each stabilizer $\hat{c}_{p(2j-1)}\hat{c}_{p(2j)}$ of the state $|\psi\rangle$ is composed either from generators $\hat{c}_1,\hat{c}_2,\hat{c}_3,\hat{c}_4$ or from the generators $\hat{c}_5,\hat{c}_6,\hat{c}_7,\hat{c}_8$. It means that $|\psi\rangle$ has a product structure $|\psi\rangle=|\psi_1\rangle\otimes|\psi_2\rangle$.

Summarizing, the four-particle qubit representation allows one to prepare qubits in a superposition, but no entangled states can be prepared topologically.

No-entanglement rule. The only logical states that can be prepared by TQC operations from the initial state $|\mathbf{0}\rangle$ are products of one-qubit states.

IV. PURIFICATION OF THE EIGHT-PARTICLE ANCILLAS

One way to get around the no-entanglement rule is to use some very noisy nontopological operations to prepare a state ρ that approximates some logical entangled "target" state. Then one can try to improve accuracy of the approximation by running a purification protocol involving only TQC operations. This is the strategy that we shall follow in this section.

A. Outline

A target state which we would like to purify is the maximally entangled two-qubit logical state

$$|a_8\rangle = \frac{1}{\sqrt{2}}(|\bar{0},\bar{0}\rangle + |\bar{1},\bar{1}\rangle) = \frac{1}{\sqrt{2}}(|0,0,0,0\rangle + |1,1,1,1\rangle). \tag{13}$$

It consists of eight σ particles.[1] The quasiparticles 1,2,3,4 and 5,6,7,8 represent the first and second logical qubits, respectively.

Let us denote $D(\mathcal{H})$ the set of all (mixed) quantum states on the Hilbert space $\mathcal{H}$. Let $\rho\in D(\mathcal{F}_4)$ be eight-particle mixed state that we can prepare by nontopological operations. A precision up to which ρ approximates $|a_8\rangle$ can be characterized by a parameter

$$\epsilon = 1 - \langle a_8|\rho|a_8\rangle.$$

It will be referred to as an *error rate*.

The only assumption we made about ρ is that it has a support only on the even subspace of $\mathcal{F}_4$—i.e.,

$$Q\rho = \rho Q = \rho, \tag{14}$$

where Q is the total parity operator,

$$Q = \hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8 = \sigma_1^z\otimes\sigma_2^z\otimes\sigma_3^z\otimes\sigma_4^z.$$

This assumption is justified if ρ is prepared starting from the vacuum by a local operator. As was mentioned in Sec. II, the operator Q measures the total topological charge ($\mathbf{1}$ or $\boldsymbol{\psi}$), so Eq. (14) is a consequence of the superselection rules.

An orthogonal projector onto $|a_8\rangle$ looks as

$$|a_8\rangle\langle a_8| = \frac{1}{16}(I+S_1)(I+S_2)(I+S_3)(I+Q),$$

where

$$S_1 = -\hat{c}_1\hat{c}_2\hat{c}_5\hat{c}_6,$$

$$S_2 = -\hat{c}_2\hat{c}_3\hat{c}_6\hat{c}_7,$$

[1] Under certain natural assumptions, 8 is the minimal number of σ particles one has to start with to prepare an entangled logical state. The reason is that any state $|\psi\rangle\in\mathcal{F}_k$, $k\leqslant 3$, with a trivial total charge is a Gaussian fermionic state; see [31] for a proof. The arguments used to prove the no-entanglement rule can be easily generalized to any Gaussian state since it also possesses a paired structure.

$$S_3 = - \hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4. \tag{15}$$

Given a binary string $\mathbf{s}=(s_1,s_2,s_3)$, $s_j \in \{0,1\}$, consider a normalized vector $|\Psi_{\mathbf{s}}\rangle \in \mathcal{F}_4$ such that

$$S_j|\Psi_{\mathbf{s}}\rangle = (-1)^{s_j}|\Psi_s\rangle, \quad j=1,2,3, \quad Q|\Psi_{\mathbf{s}}\rangle = |\Psi_{\mathbf{s}}\rangle.$$

Notice that $|a_8\rangle = |S_{000}\rangle \equiv |S_{\mathbf{0}}\rangle$. Obviously, $\{|\Psi_{\mathbf{s}}\rangle\}$ constitute an orthonormal basis of the even subspace of $\mathcal{F}_4$. Therefore, ρ can be written as

$$\rho = \sum_{\mathbf{s},\mathbf{t}} \rho_{\mathbf{st}}|\Psi_{\mathbf{s}}\rangle\langle\Psi_{\mathbf{t}}|, \quad \rho_{\mathbf{00}} = 1-\epsilon. \tag{16}$$

By analogy with quantum error correcting codes, the operators S_j and the string $\mathbf{s}$ will be referred to as *stabilizers* and a *syndrome*, respectively.

The goal of a purification is to prepare one copy of $|a_8\rangle$ with an arbitrarily small error rate ϵ' starting from n noisy copies of $|a_8\rangle$ with an error rate ϵ. The performance of a purification protocol can be characterized by a threshold value of ϵ below which the purification is possible and efficiency—i.e., an asymptotic behavior of $n=n(\epsilon,\epsilon')$ for $\epsilon' \to 0$. We shall describe a protocol for which the threshold error rate is

$$\delta_8 \approx 0.384 \tag{17}$$

and

$$n(\epsilon,\epsilon') \approx C(-\ln \epsilon')^3 \tag{18}$$

for any fixed $\epsilon < \delta_8$ and $\epsilon' \to 0$. Here C is a function of ϵ only. The protocol succeeds with a probability at least 1/2 and there is a flag that tells us when it fails.

The protocol involves the following steps.

(i) Dephasing: make ρ diagonal in the basis $\{|\Psi_{\mathbf{s}}\rangle\}$.

(ii) Syndrome whirling: make the probability distribution of the nonzero syndromes $\mathbf{s} \neq 0$ uniform.

(iii) Purification: convert two noisy copies of $|a_8\rangle$ into one clean copy by postselective measurements on four pairs of σ particles.

In order to achieve an arbitrarily small error rate, these steps have to be repeated sufficiently many times in a recursive fashion. Below we describe the protocol on a more technical level.

B. Dephasing

Let S be a group generated by S_1, S_2, and S_3. It consists of eight elements. Consider a quantum operation

$$\Phi_S(\rho) = \frac{1}{8}\sum_{U\in S} U\rho U^\dagger.$$

It symmetrizes a state over the group S, thus implementing a dephasing in the basis $\{|\Psi_{\mathbf{s}}\rangle\}$. The stabilizer operators S_j themselves can be implemented using braid gates—for instance, $S_1 = -B_{1,2}^2 B_{5,6}^2$. Accordingly, Φ_S can be implemented using braid gates, if $U \in S$ is drawn randomly according to the uniform distribution. Obviously, for any state ρ one has

$$\Phi_S(\rho) = \sum_{\mathbf{s}} p(\mathbf{s})|\Psi_{\mathbf{s}}\rangle\langle\Psi_{\mathbf{s}}|, \quad p(\mathbf{s}) \equiv \langle\Psi_{\mathbf{s}}|\rho|\Psi_{\mathbf{s}}\rangle. \tag{19}$$

We shall assume that each ancilla is acted on by Φ_S before it is fed into the purification protocol. It allows one to identify quantum states with probability distributions of syndromes.

C. Syndrome whirling

A probability distribution of syndromes $p(\mathbf{s})$ can be brought by braid gates into the standard bimodal form

$$p(\mathbf{s}) = \begin{cases} 1-\epsilon & \text{if } \mathbf{s}=(0,0,0), \\ \epsilon/7 & \text{if } \mathbf{s} \neq (0,0,0). \end{cases} \tag{20}$$

To achieve this, we will first show how to implement a cyclic shift on the set of seven nonzero syndromes $\mathbf{s} \neq \mathbf{0}$. Then we shall implement a random cyclic shift.

Consider a braid gate

$$U_{12} = B_{2,3}B_{6,7}^\dagger. \tag{21}$$

Its conjugated action is as follows (only nontrivial part of the action is shown):

$$U_{12}\cdot U_{12}^\dagger = \begin{cases} \hat{c}_2 \to \hat{c}_3, \\ \hat{c}_3 \to -\hat{c}_2, \\ \hat{c}_6 \to -\hat{c}_7, \\ \hat{c}_7 \to \hat{c}_6. \end{cases}$$

Accordingly, a conjugated action of U_{12} on the stabilizers S_j is

$$U_{12}\cdot U_{12}^\dagger = \begin{cases} S_1 \to S_1S_2, \\ S_2 \to S_2, \\ S_3 \to S_3. \end{cases}$$

Therefore, U_{12} implements an exclusive-OR-(XOR)-like transformation

$$U_{12}|\Psi_{s_1,s_2,s_3}\rangle = |\Psi_{s_1\oplus s_2,s_2,s_3}\rangle,$$

where $\oplus$ stands for the addition by modulo 2. Analogously, one can check that braid gates

$$U_{23} = B_{1,2}^\dagger B_{3,4} \quad \text{and} \quad U_{31} = B_{1,5}B_{2,6}$$

implement XOR-like transformations

$$U_{23}|\Psi_{s_1,s_2,s_3}\rangle = |\Psi_{s_1,s_2\oplus s_3,s_3}\rangle,$$

$$U_{31}|\Psi_{s_1,s_2,s_3}\rangle = |\Psi_{s_1,s_2,s_1\oplus s_3}\rangle. \tag{22}$$

Consider now a braid gate

$$U = U_{31}U_{23}U_{12}.$$

One can easily check that U implements a cyclic shift of nonzero syndromes:

$$U|\Psi_{\mathbf{s}}\rangle = |\Psi_{\eta(\mathbf{s})}\rangle, \quad \eta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 3 & 7 & 4 & 5 & 6 & 2 & 1 \end{pmatrix}.$$

Here η is a permutation of the numbers $\{0,1,\ldots,7\}$, and the syndromes are represented by integers according to $\mathbf{s}=4s_1$

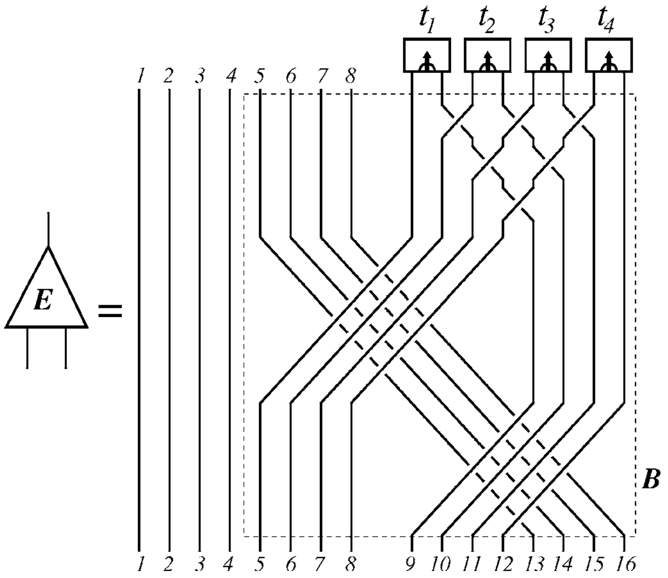

FIG. 2. The elementary purification round.

$+2s_2+s_3$. Consider a symmetrization Φ_U over the cyclic group generated by U (it is the cyclic group $\mathbb{Z}_7$, since $U^7=I$)—i.e.,

$$\Phi_U(\eta) = \frac{1}{7}\sum_{p=0}^{6} U^p \eta U^{-p}.$$

An application of Φ_U to a state $\rho=\Sigma_{\mathbf{s}} p(\mathbf{s})|\Psi_{\mathbf{s}}\rangle\langle\Psi_{\mathbf{s}}|$ transforms the probability distribution $p(\mathbf{s})$ into the standard form Eq. (20), where

$$\epsilon = 1 - p(\mathbf{0}) = 1 - \langle\Psi_{\mathbf{0}}|\rho|\Psi_{\mathbf{0}}\rangle.$$

By construction, Φ_U is a probabilistic mixture of braid gates.

D. Elementary purification round

Suppose we are given a supply of states

$$\rho = \sum_{\mathbf{s}} p(\mathbf{s})|\Psi_{\mathbf{s}}\langle\Psi_{\mathbf{s}}|.$$

Here $p(\mathbf{s})$ is some fixed probability distribution of syndromes (which may or may not have the standard bimodal form).

Consider a state $\rho\otimes\rho$ where the first and second copies are composed from generators $\hat{c}_1,\ldots,\hat{c}_8$ and $\hat{c}_9,\ldots,\hat{c}_{16}$, respectively. Let us reshuffle the generators by a braid gate B shown in Fig. 2 (inside the dashed rectangle) and then measure eigenvalues of four operators

$$T_1 = -i\hat{c}_9\hat{c}_{10}, \quad T_2 = -i\hat{c}_{11}\hat{c}_{12},$$

$$T_3 = -i\hat{c}_{13}\hat{c}_{14}, \quad T_4 = -i\hat{c}_{15}\hat{c}_{16}. \tag{23}$$

Let $t_1,t_2,t_3,t_4\in\{0,1\}$ be the measurement outcomes, such that T_j has an eigenvalue $(-1)^{t_j}$. Since the input state $\rho\otimes\rho$ is a probabilistic mixture of pure states $|\Psi_{\mathbf{r}}\rangle\otimes|\Psi_{\mathbf{s}}\rangle$, it suffices to analyze the effect of the braiding+measurement operation on these input states. For any string of outcomes $\mathbf{t}=(t_1,t_2,t_3,t_4)$ consider the final (unnormalized) state

$$|F_{\mathbf{t}|\mathbf{trs}}\rangle = P_{\mathbf{t}}B|\Psi_{\mathbf{r}}\otimes\Psi_{\mathbf{s}},$$

where

$$P_{\mathbf{t}} = \frac{1}{16}\prod_{j=1}^{4}(I+(-1)^{t_j}T_j)$$

is the projector corresponding to the outcomes $\mathbf{t}$. Taking into account an identity

$$(\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8)(\hat{c}_9\hat{c}_{10}\hat{c}_{11}\hat{c}_{12}) = B^\dagger(T_1T_2T_3T_4)B \tag{24}$$

and the fact that $|\Psi_{\mathbf{r}}\rangle$ and $|\Psi_{\mathbf{s}}\rangle$ are even states, we conclude that

$$|F_{\mathbf{t}|\mathbf{rs}}\rangle = 0 \quad \text{unless} \quad r_3\oplus s_3 = t_1\oplus t_2\oplus t_3\oplus t_4. \tag{25}$$

Thus a bit

$$t \equiv t_1\oplus t_2\oplus t_3\oplus t_4$$

can be regarded as a check sum for the syndrome bits r_3 and s_3. If $t=0$, then either both syndrome bits are correct, $r_3=s_3=0$, or both of them are wrong, $r_3=s_3=1$. If the input state ρ has a sufficiently small error rate [the probability distribution $p(\mathbf{s})$ is concentrated at $\mathbf{s}=\mathbf{0}$], the former possibility is more likely than the latter one. As we shall see now, one can enhance a probability of states with a correct eigenvalue of S_3 by discarding the final state whenever the outcome $t=1$ is observed.

Indeed, suppose we have measured $t=0$ and $|F_{\mathbf{t}|\mathbf{rs}}\rangle\neq 0$. After some algebra one gets

$$|F_{\mathbf{t}|\mathbf{rs}}\rangle = |\Psi_{\mathbf{u}}\rangle\otimes|t_1,t_2,t_3,t_4\rangle \tag{26}$$

(up to a normalization), where

$$u_1 = r_1\oplus s_1\oplus t_1\oplus t_2\oplus 1,$$

$$u_2 = r_2\oplus s_2\oplus t_2\oplus t_3\oplus 1,$$

$$u_3 = r_3 = s_3. \tag{27}$$

Note that the syndrome bit u_3 depends only upon $\mathbf{r}$ and $\mathbf{s}$, while u_1 and u_2 depend also upon $\mathbf{t}$. Let us apply additional braid gates

$$\hat{c}_2\hat{c}_3:|\Psi_{u_1,u_2,u_3}\rangle \rightarrow |\Psi_{u_1\oplus 1,u_2,u_3}\rangle,$$

$$\hat{c}_1\hat{c}_2:|\Psi_{u_1,u_2,u_3}\rangle \rightarrow |\Psi_{u_1,u_2\oplus 1,u_3}\rangle,$$

conditioned on bits $t_1\oplus t_2\oplus 1$ and $t_2\oplus t_3\oplus 1$, respectively. These braid gates flip the bits u_1 and u_2, so we get

$$u_1 = r_1\oplus s_1, \quad u_2 = r_2\oplus s_2, \quad u_3 = r_3 = s_3. \tag{28}$$

(To avoid clutter, the additional braid gates are not shown in Fig. 2.) Summarizing, the output state of the elementary purification round is $|\Psi_{\mathbf{u}}\rangle$ with $\mathbf{u}$ determined by Eq. (28).

For the mixed input state $\rho\otimes\rho$ the syndromes $\mathbf{r}$ and $\mathbf{s}$ are drawn from a product distribution $p(\mathbf{r})p(\mathbf{s})$, so the output (normalized) state is

$$\rho_{out} = \sum_{\mathbf{u}} p_{out}(\mathbf{u}) |\Psi_{\mathbf{u}}\rangle\langle\Psi_{\mathbf{u}}|,$$

where

$$p_{out}(\mathbf{u}) = Z^{-1} \sum_{\mathbf{r},\mathbf{s}} \Gamma^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} p(\mathbf{r}) p(\mathbf{s}) \tag{29}$$

and

$$\Gamma^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} = \delta_{r_3,u_3} \delta_{s_3,u_3} \delta_{r_1 \oplus s_1,u_1} \delta_{r_2 \oplus s_2,u_2}.$$

Normalizing ρ_{out} one gets

$$Z = \sum_{\mathbf{r},\mathbf{s},\mathbf{u}} \Gamma^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} p(\mathbf{r}) p(\mathbf{s}) = \sum_{\mathbf{r},\mathbf{s}} \delta_{r_3,s_3} p(\mathbf{r}) p(\mathbf{s}).$$

Note that Z is equal to the probability to observe $t=0$—i.e., a success probability of the elementary purification round.

E. Protocol

Let $\epsilon^{(j)}$ and $\epsilon^{(j)}_{out}$ be a probability to observe $s_j=1$ for the distribution $p(\mathbf{s})$ and $p_{out}(\mathbf{s})$, respectively $(j=1,2,3)$. They can be regarded as error rates for the individual syndrome bits. If $p(\mathbf{s})$ has the standard bimodal form, Eq. (20), then $\epsilon^{(j)}=4\epsilon/7$. On the other hand, for $\epsilon \ll 1$ one can easily find from Eq. (29) that

$$\epsilon^{(3)}_{out} \approx 16\epsilon^2/49, \quad \epsilon^{(1)}_{out} = \epsilon^{(2)}_{out} \approx 4\epsilon/7.$$

It tells us that the error rate $\epsilon^{(3)}$ is suppressed quadratically, $\epsilon^{(3)}_{out} \approx (\epsilon^{(3)})^2$, while the error rates $\epsilon^{(1)}$ and $\epsilon^{(2)}$ remain practically unchanged, $\epsilon^{(1)}_{out} \approx \epsilon^{(1)}$ and $\epsilon^{(2)}_{out} \approx \epsilon^{(2)}$. For this reason we shall iterate the elementary purification round shown in Fig. 2 three times to purify all three syndrome bits s_1, s_2, and s_3. The iterations are interlaced with an additional braid gate C which shifts the syndrome bits cyclically—i.e.,

$$CS_1C^\dagger = S_2, \quad CS_2C^\dagger = S_3, \quad CS_3C^\dagger = S_1.$$

These equations can be satisfied if C transforms the generators $\hat{c}_1, \ldots, \hat{c}_8$ according to

$$C: \begin{cases} \hat{c}_1 \to \hat{c}_6, & \hat{c}_5 \to -\hat{c}_7, \\ \hat{c}_2 \to \hat{c}_2, & \hat{c}_6 \to \hat{c}_3, \\ \hat{c}_3 \to \hat{c}_1, & \hat{c}_7 \to -\hat{c}_4, \\ \hat{c}_4 \to \hat{c}_5, & \hat{c}_8 \to \hat{c}_8. \end{cases}$$

An explicit implementation of C is shown in Fig. 3.

A single round of a_8-purification protocol is shown in Fig. 4. Its input consists of eight copies of a noisy $|a_8\rangle$ state in the standard bimodal form with an error rate ϵ:

$$\rho = (1-\epsilon)|\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| + \frac{\epsilon}{7} \sum_{\mathbf{s}\neq\mathbf{0}} |\Psi_{\mathbf{s}}\rangle\langle\Psi_{\mathbf{s}}|.$$

The protocol outputs a single copy of a noisy $|a_8\rangle$ state in the standard bimodal form with an error rate ϵ_{out}. The triangles labeled by E denote the elementary purification rounds shown in Fig. 2. The boxes labeled by C denote the braid gate shown in Fig. 3. The circle labeled by W stands for the syndrome whirling transformation. Each line in the figure represents eight σ particles.

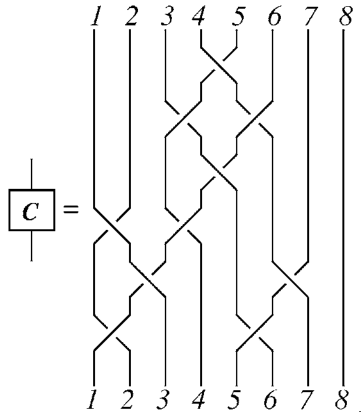

FIG. 3. A braid gate C implementing a cyclic shift of stabilizers $S_1 \to S_2 \to S_3 \to S_1$.

The corresponding recursive flow equation $\epsilon_{out}(\epsilon)$ can be found by iterating Eq. (29) three times with an additional cyclic shifts inserted after each iteration. Equivalently, $\epsilon_{out}(\epsilon)$ is implicitly defined by equations

$$\epsilon_{out} = 1 - Z^{-1} p_1(\mathbf{0}),$$

$$p_1(\mathbf{u}) = \sum_{\mathbf{r},\mathbf{s}} \Theta^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} p_2(\mathbf{r}) p_2(\mathbf{s}),$$

$$p_2(\mathbf{u}) = \sum_{\mathbf{r},\mathbf{s}} \Delta^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} p_3(\mathbf{r}) p_3(\mathbf{s}),$$

$$p_3(\mathbf{u}) = \sum_{\mathbf{r},\mathbf{s}} \Gamma^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} p(\mathbf{r}) p(\mathbf{s}),$$

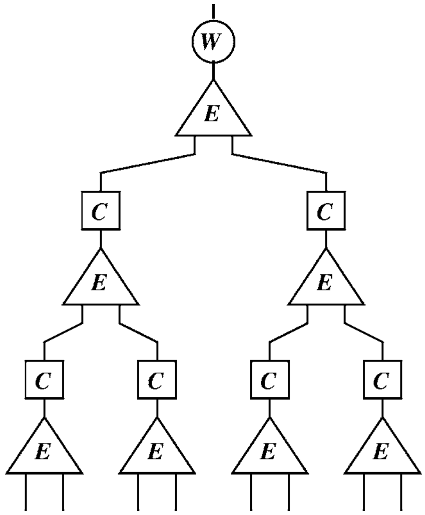

FIG. 4. A single round of a_8-purification protocol. Time flows upwards. Each line represents one copy of the noisy $|a_8\rangle$ state (eight σ particles). Each triangle E corresponds to the elementary purification round shown in Fig. 2. Each rectangle C represents a braid gate that shifts the generators S_1, S_2, and S_3 cyclically; see Fig. 3. Finally, a circle W stands for the syndrome whirling transformation.

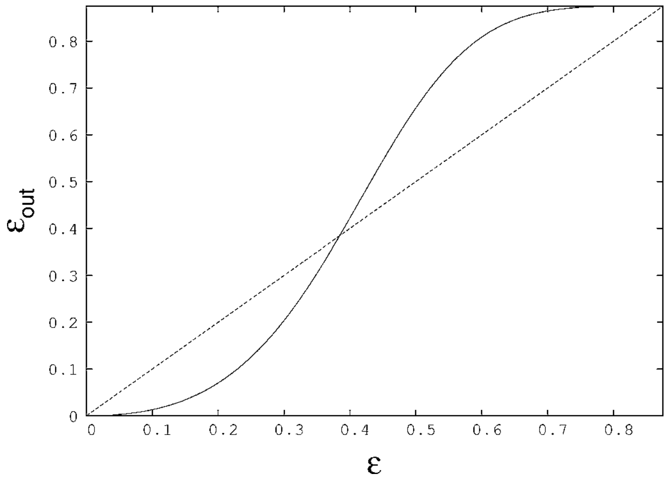

FIG. 5. Input and output error rates for a single round of a_8-purification protocol.

$$Z = \sum_{\mathbf{u}} p_1(\mathbf{u}). \tag{30}$$

The initial distribution $p(\mathbf{s})$ has the standard bimodal form, Eq. (20), with the error rate ϵ. The coefficients $\Theta^{\mathbf{u}}_{\mathbf{r},\mathbf{s}}$ and $\Delta^{\mathbf{u}}_{\mathbf{r},\mathbf{s}}$ are obtained from $\Gamma^{\mathbf{u}}_{\mathbf{r},\mathbf{s}}$ by a cyclic shift of indices,

$$\Theta^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} = \delta_{r_1,u_1}\delta_{s_1,u_1}\delta_{r_2\oplus s_2,u_2}\delta_{r_3\oplus s_3,u_3},$$

$$\Delta^{\mathbf{u}}_{\mathbf{r},\mathbf{s}} = \delta_{r_2,u_2}\delta_{s_2,u_2}\delta_{r_1\oplus s_1,u_1}\delta_{r_3\oplus s_3,u_3}.$$

The final cyclic shift can be discarded because it is followed by the syndrome whirling. We have found a solution of Eq. (30) using MAPLE. A plot of a function $\epsilon_{out}(\epsilon)$ is shown in Fig. 5.

The threshold error rate δ_8 satisfying $\epsilon_{out}(\delta_8) = \delta_8$ turns out to be $\delta_8 \approx 0.384$. If the initial error rate is below the threshold, $\epsilon < \delta_8$, one can invoke the protocol recursively to achieve arbitrarily small error rates. For $\epsilon \ll 1$ one can easily get

$$\epsilon_{out}(\epsilon) = \frac{48}{49}\epsilon^2 + O(\epsilon^3).$$

A probability for all elementary purification rounds in Fig. 4 to succeed is given by the normalizing coefficient Z in Eq. (30). For small ϵ one has

$$Z = 1 - 8\epsilon + O(\epsilon^2). \tag{31}$$

The function $Z(\epsilon)$ is monotone decreasing in the interval $0 \leq \epsilon \leq \delta_8$ and $Z(\delta_8) \approx 0.04$.

The initial supply of states $|a_8\rangle$ with an error rate $\epsilon_0 \equiv \epsilon$ will be called level-0 ancillas. Accordingly, level-k ancillas are obtained from the level-0 ancillas by iterating the protocol, shown in Fig. 4, k times. Let ϵ_k and n_k be an error rate and the total number of level-k ancillas. The numbers ϵ_{k+1}, n_{k+1} and ϵ_k, n_k are related by the recursive flow equations

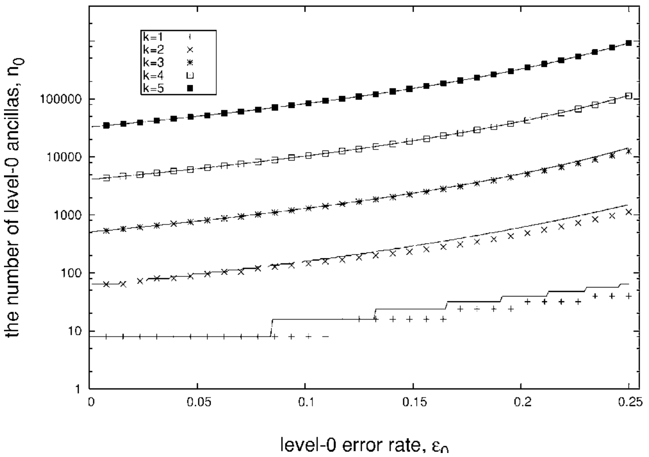

FIG. 6. The graph shows the number of level-0 ancillas, n_0, that one needs to prepare one level-k ancilla ($k=1,\ldots,5$) with a success probability 1/2. The success probability has been evaluated using Monte Carlo simulation of the protocol with 10^5 trials. Solid lines show the dependence $n_0(\epsilon_0)$ that one gets using a naive equation $n_0 = 8^k \prod_{j=0}^{k-1} Z(\epsilon_j)^{-1}$ (it neglects fluctuations of n_k).

$$n_{k+1} \approx \frac{Z(\epsilon_k)}{8} n_k, \quad \epsilon_{k+1} \approx \frac{48}{49}\epsilon_k^2. \tag{32}$$

Here fluctuations of the quantity n_k are neglected. Monte Carlo simulation of the a_8-purification protocol shows that taking into account fluctuations does not change the answer significantly; see Fig. 6.

If one needs to prepare one copy of $|a_8\rangle$ with an error rate ϵ', the required number of levels k can be found from an equation

$$2^k \approx \frac{\ln(C\epsilon')}{\ln(C\epsilon_0)}, \quad C \equiv \frac{48}{49}.$$

The corresponding number of level-0 ancillas is

$$n_0 \approx 8^k \prod_{j=0}^{k-1} Z(\epsilon_j)^{-1}. \tag{33}$$

Assuming that $k \gg 1$ and denoting $p(\epsilon_0) = \prod_{j=0}^{\infty} Z(\epsilon_j)$ (one can easily check that this product is convergent), we get

$$n_0 \approx \frac{\ln^3(C\epsilon')}{p(\epsilon_0)\ln^3(C\epsilon_0)}.$$

To find the probability for the protocol to convert n_0 copies of the level-0 ancillas into one (or larger number) level-k ancilla, we used numerical simulations; see Fig. 6. The success probability $P_s = \mathrm{Prob}(n_k > 0)$ was calculated as a function of n_0 using the Monte Carlo method. For each particular $k=1,\ldots,5$ an equation $P_s(n_0) = 1/2$ has been solved to find n_0 as a function of ϵ_0. As one can see from the figure, the scaling of n_0 is pretty well described by Eq. (33).

The operational cost of the purification—i.e., the total number of braid gates and fusions needed to achieve an error rate ϵ'—has the same scaling as n_0; i.e., it is proportional to $(-\ln \epsilon')^3$.

Suppose we have to prepare a large number L of ancillas $|a_8\rangle$. Let us first prepare $n=3Ln_0(\epsilon_0,\epsilon')$ level-0 ancillas, split them into $3L$ groups, and then perform the a_8-purification protocol independently in each group. If the purification succeeds in each group with a probability $1/2$, the average number of successful group is $3L/2$. Using the Chernoff bound one can easily show that the probability for the number of successful group to be smaller than L is at most $\exp(-L/12)$. Thus one can say that a preparation of a single ancilla $|a_8\rangle$ with an accuracy ϵ' costs about $(-\ln\epsilon')^3$ elementary operations (TQC operations and preparations of ρ_8).

This observation also shows that the purification can be described by a trace-preserving completely positive linear map (in the exponentially rare events when the purification fails, one can output an arbitrary state). Accordingly, we can generalize all above results to the case when the preparation of the level-0 ancillas is a stochastic process that outputs a state ρ_α with a probability p_α, such that $\Sigma_\alpha p_\alpha\rho_\alpha=\rho$.

V. IMPLEMENTATION OF THE CLIFFORD GROUP GATES

Having prepared a supply of clean ancillas $|a_8\rangle$ one can proceed to the next goal—implementation of entangling two-qubit gates. We shall now explain how to implement a two-qubit controlled σ^z gate

$$\Lambda(\sigma^z):|\bar{a},\bar{b}\rangle \to (-1)^{ab}|\bar{a},\bar{b}\rangle$$

acting on the logical qubits. Together with logical one-qubit Clifford gates which can be implemented by braid gates (see Sec. III) it will allow us to execute any Clifford group computation (on the level of logical qubits). We shall need the following technical result.

Lemma 1. The following operations can simulate one another with assistance of TQC operations: $(O1)$ a preparation of $|a_8\rangle$, $(O2)$ a nondestructive measurement of an observable $\hat{c}_p\hat{c}_q\hat{c}_r\hat{c}_s$ (all four labels are distinct), and $(O3)$ a unitary gate $\exp\left(i\frac{\pi}{4}\hat{c}_p\hat{c}_q\hat{c}_r\hat{c}_s\right)$,

Remarks. (i) It is meant that one copy of any operation can be exactly simulated by one copy of any other operation. (ii) The operator $\hat{c}_p\hat{c}_q\hat{c}_r\hat{c}_s$ has eigenvalues ±1, so $O2$ can be described by orthogonal projectors $(1/2)(I\pm\hat{c}_p\hat{c}_q\hat{c}_r\hat{c}_s)$. (iii) If $O1$ is not ideal, so that $|a_8\rangle$ has an error rate ϵ, then $O2$ and $O3$ can be executed with an error probability $O(\epsilon)$. (iv) Explicit simulation protocols are given in the proof of the lemma.

The controlled σ^z can be easily reduced to $O3$. Indeed, suppose the first qubit is encoded by $\hat{c}_1,\ldots,\hat{c}_4$, while the second qubit is encoded by $\hat{c}_5,\ldots,\hat{c}_8$. Then $\Lambda(\sigma^z)=\exp\left[i\frac{\pi}{4}(I-\bar{\sigma}_1^z)(I-\bar{\sigma}_2^z)\right]$, where $\bar{\sigma}_j^z$ are the logical Pauli operators defined as $\sigma_1^z=-i\hat{c}_3\hat{c}_4$ and $\sigma_2^z=-i\hat{c}_5\hat{c}_6$; see Sec. III. Therefore,

$$\Lambda(\sigma^z) = e^{i\pi/4}\exp\left(-i\frac{\pi}{4}\hat{c}_3\hat{c}_4\hat{c}_5\hat{c}_6\right)\exp\left(-\frac{\pi}{4}\hat{c}_3\hat{c}_4\right)$$
$$\times\exp\left(-\frac{\pi}{4}\hat{c}_5\hat{c}_6\right). \qquad (34)$$

The last two exponents in Eq. (34) are braid gates, so the controlled σ^z gate is equivalent to $O3$ (we disregard the overall phase). One remains to prove the lemma.

2. Proof of lemma 1

O3 can simulate O1. Using solely braid gates one can prepare a state with a stabilizer group

$$S=(-i\hat{c}_1\hat{c}_7,-i\hat{c}_2\hat{c}_8,-i\hat{c}_3\hat{c}_5,-i\hat{c}_4\hat{c}_6)$$

(all eigenvalues are +1). Let this state be acted upon by an operator

$$U\equiv\exp\left(i\frac{\pi}{4}\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_6\right).$$

The conjugated action of U on the Majorana operators is as follows:

$$U\cdot U^\dagger:\begin{cases}\hat{c}_1\to -i\hat{c}_2\hat{c}_3\hat{c}_6, & \hat{c}_5\to\hat{c}_5,\\ \hat{c}_2\to i\hat{c}_1\hat{c}_3\hat{c}_6, & \hat{c}_6\to i\hat{c}_1\hat{c}_2\hat{c}_3,\\ \hat{c}_3\to -i\hat{c}_1\hat{c}_2\hat{c}_6, & \hat{c}_7\to\hat{c}_7,\\ \hat{c}_4\to\hat{c}_4, & \hat{c}_8\to\hat{c}_8.\end{cases}$$

Accordingly, the stabilizer group S is mapped onto

$$S'=(-\hat{c}_2\hat{c}_3\hat{c}_6\hat{c}_7,\hat{c}_1\hat{c}_3\hat{c}_6\hat{c}_8,-\hat{c}_1\hat{c}_2\hat{c}_5\hat{c}_6,-\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4).$$

It coincides with the stabilizer group (S_1,S_2,S_3) of the state $|a_8\rangle$; see Eq. (15). Therefore the state stabilized by S' coincides with $|a_8\rangle$ up to an overall phase.

O2 can simulate O1. (This part is not necessary for the proof, but we shall use this result later.) Using solely braid gates one can prepare a state with a stabilizer group

$$S=(-i\hat{c}_1\hat{c}_5,i\hat{c}_2\hat{c}_6,-i\hat{c}_3\hat{c}_7,i\hat{c}_4\hat{c}_8).$$

Let us measure an eigenvalue of $-\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8$ on this state. To find the final stabilizer group, choose generators of S as

$$S=(-\hat{c}_1\hat{c}_2\hat{c}_5\hat{c}_6,-\hat{c}_2\hat{c}_3\hat{c}_6\hat{c}_7,-\hat{c}_3\hat{c}_4\hat{c}_7\hat{c}_8,i\hat{c}_4\hat{c}_8).$$

After the measurement the last generator is replaced by $-\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8$ (may be with the opposite sign), which is equivalent to a generator $-\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$. The resulting stabilizer group coincides with the one of $|a_8\rangle$. (The preparation of $|a_8\rangle$ by measuring $\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8$ is illustrated by Fig. 8 below.)

O1 can simulate O2. Assume that one copy of $|a_8\rangle$ is available. A sequence of braidings and fusions that allows one to measure an eigenvalue of $\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$ is shown in Fig. 7. The particles labeled by 1, 2, 3, and 4 in the figure are prepared in an arbitrary initial state $|\psi_{in}\rangle$. The state $|a_8\rangle$ is described by generators $\hat{c}_5,\ldots,\hat{c}_{12}$. Accordingly, the circuit shown in Fig. 7 is applied to a state $|\psi_{in}\otimes a_8\rangle$. The particles are reshuffled by a braid operator, and then observables $T_1=-i\hat{c}_1\hat{c}_2$,$T_2=-i\hat{c}_3\hat{c}_4$, $T_3=-i\hat{c}_5\hat{c}_6$, and $T_4=-i\hat{c}_7\hat{c}_8$ are measured. The final state $|\psi_f\rangle$ is read out from the particles 9, 10, 11, and 12.

Let $(-1)^{t_j}$ be the measured eigenvalue of T_j. We shall consider in details only the case $t_1\oplus t_2\oplus t_3\oplus t_4=0$. Let $|\Phi_{\mathbf{t}}\rangle$ be the final state corresponding to outcomes $\mathbf{t}=(t_1,t_2,t_3,t_4)$. Using the stabilizer description of $|a_8\rangle$ [see Eq. (15)], one can easily check that

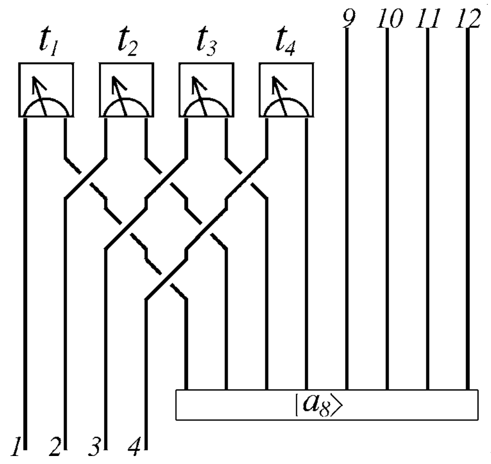

FIG. 7. Implementation of a nondestructive measurement of $\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$ that consumes one copy of $|a_8\rangle$.

$$|\Phi_{\mathbf{t}}\rangle = (\hat{c}_2^{t_1}\hat{c}_4^{t_2}\hat{c}_6^{t_3}\hat{c}_8^{t_4})(\hat{c}_9^{t_1}\hat{c}_{10}^{t_2}\hat{c}_{11}^{t_3}\hat{c}_{12}^{t_4})|\Phi_{\mathbf{0}}$$

whenever $t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$. Let us apply additional braid gates $\hat{c}_2\hat{c}_9$, $\hat{c}_4\hat{c}_{10}$, $\hat{c}_6\hat{c}_{11}$, and $\hat{c}_8\hat{c}_{12}$ controlled by classical bits t_1, t_2, t_3, and t_4, respectively (these gates are not shown on Fig. 7 to avoid clutter). They map $|\Phi_{\mathbf{t}}\rangle$ into $|\Phi_{\mathbf{0}}\rangle$, so it suffices to analyze the case $t_j=0$. Obviously, $|\Phi_{\mathbf{0}}\rangle$ has a product structure $|\Phi_{\mathbf{0}}\rangle = |0,0,0,0\rangle \otimes |\psi_{fin}\rangle$.

One can easily notice that the left-upper part of Fig. 7 with $t_j=0$ is almost identical to the preparation procedure for $\langle a_8|$; see Fig. 8. The only missing element is a projector $(1/2)(I - \hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8)$. However, one can safely add the missing projector because it stabilizes the state $|a_8\rangle$. Therefore, for the outcomes $t_j=0$ the protocol shown in Fig. 7 coincides with the one shown in Fig. 9. Taking into account that $|a_8\rangle$ is the encoded Einstein-Podolsky-Rosen (EPR) state, $|a_8\rangle = 2^{-1/2}(|\bar{0},\bar{0}\rangle + |\bar{1},\bar{1}\rangle)$, the protocol in Fig. 9 is just a projection of $|\psi_{in}\rangle$ onto the code subspace followed by teleportation of the encoded qubit from the particles 1, 2, 3, and 4 to the particles 9, 10, 11, and 12. Accordingly, $|\psi_f\rangle = (1/2)(I - \hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4)|\psi_{in}\rangle$, up to an overall normalization constant. Using similar arguments one can check that $|\psi_f\rangle = (1/2)(I + \hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4)|\psi_{in}\rangle$ whenever $t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 1$.

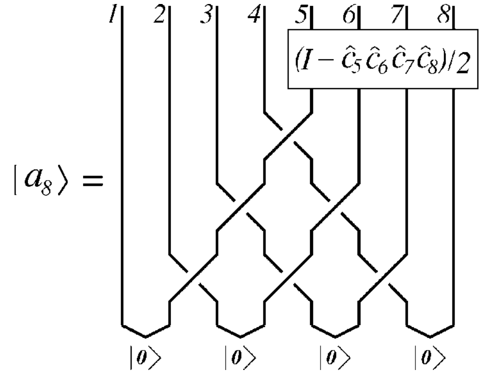

FIG. 8. Preparation of $|a_8\rangle$ via eigenvalue measurement of $\hat{c}_5\hat{c}_6\hat{c}_7\hat{c}_8$.

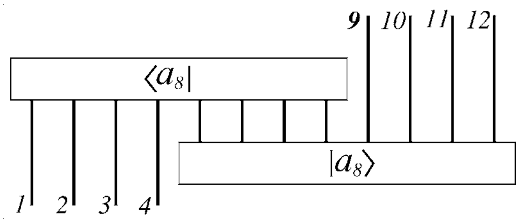

FIG. 9. Teleportation.

O2 can simulate O3. (This result has been already proved in [30].) Suppose we want to implement an operator $\exp(i\frac{\pi}{4}\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4)$. Let us prepare an ancillary pair of particles 5 and 6 in the state $|0\rangle$. Accordingly, any input state $|\psi\rangle$ of the system satisfies

$$(\hat{c}_5 + i\hat{c}_6)|\psi\rangle = 0. \tag{35}$$

Let us measure an eigenvalue of $\hat{c}_1\hat{c}_2\hat{c}_4\hat{c}_5$. Depending upon the outcome, the initial state $|\psi\rangle$ gets multiplied by a projector $\Pi_{\pm}^{(4)} = (1/2)(I \pm \hat{c}_1\hat{c}_2\hat{c}_4\hat{c}_5)$ (with a proper normalizing coefficient). Next we measure an eigenvalue of $-i\hat{c}_3\hat{c}_5$. The eigenvalues ±1 correspond to projectors $\Pi_{\pm}^{(2)} = (1/2)(1 \mp i\hat{c}_3\hat{c}_5)$. We claim that after some correction depending on the measurements outcomes, the protocol effectively executes the operator $\exp(i\frac{\pi}{4}\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4)$ while leaving the ancillary pair of particles intact. The correction step requires only braid gates. Indeed, one can use the following identities:

$$\begin{aligned}
&\exp\left(i\frac{\pi}{4}\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4\right)|\psi\rangle \\
&\quad = 2\exp\left(\frac{\pi}{4}\hat{c}_3\hat{c}_6\right)\Pi_+^{(2)}\Pi_+^{(4)}|\psi\rangle \\
&\quad = 2i\exp\left(\frac{\pi}{2}\hat{c}_1\hat{c}_2\right)\exp\left(\frac{\pi}{2}\hat{c}_3\hat{c}_4\right)\exp\left(\frac{\pi}{4}\hat{c}_3\hat{c}_6\right)\Pi_-^{(2)}\Pi_-^{(4)}|\psi \\
&\quad = 2i\exp\left(\frac{\pi}{2}\hat{c}_1\hat{c}_2\right)\exp\left(\frac{\pi}{2}\hat{c}_3\hat{c}_4\right)\exp\left(-\frac{\pi}{4}\hat{c}_3\hat{c}_6\right)\Pi_-^{(2)}\Pi_+^{(4)}|\psi\rangle \\
&\quad = 2\exp\left(-\frac{\pi}{4}\hat{c}_3\hat{c}_6\right)\Pi_-^{(2)}\Pi_-^{(4)}|\psi
\end{aligned} \tag{36}$$

[we have used Eq. (35)]. In each of the four cases one can apply a suitable correction operator U_{yz} [for example, $U_{++} = \exp(\frac{\pi}{4}\hat{c}_3\hat{c}_6)$ if the outcomes were ++, etc.] so that

$$\exp\left(i\frac{\pi}{4}\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4\right)|\psi\rangle = 2U_{yz}\Pi_y^{(2)}\Pi_z^{(4)}|\psi\rangle.$$

Each of the four outcome combinations occurs with probability 1/4. The final state is always the desired one—i.e., $\exp(i\frac{\pi}{4}\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4)|\psi\rangle$.

VI. UNIVERSAL QUANTUM COMPUTATION

The protocols described in Sec. V allow one to execute any Clifford group gates on the logical qubits. In addition to that, one can measure logical qubits in the standard basis and prepare fresh logical qubits in the state $|\bar{0}\rangle$. Let us refer to this set of operations as *Clifford operations*. As we have shown, Clifford operations can be implemented with an arbitrarily small error rate and the overhead is polylogarithmic. To simplify the discussion, we shall firstly set the error rate of Clifford operations to zero and then address the precision and overhead issues separately.

Below we will show how to execute the $\pi/8$ rotation

$$\Lambda(e^{i/\pi 4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \tag{37}$$

on the logical qubit. It is well known that the $\pi/8$ rotation and Clifford operations constitute a universal set of gates.

Although the $\pi/8$ rotation cannot be implemented by Clifford operations only, we can follow the same strategy as in Sec. IV: namely, try to use very noisy nontopological operations to prepare a state ρ that approximates some logical target state $|a\rangle$, improve the accuracy of the approximation by running a purification protocol (which now can use any Clifford operations), and then convert $|a\rangle$ into the gate $\Lambda(e^{i\pi/4})$.

It is not *a priori* clear what ancillary state $|a\rangle$ leads to the most efficient implementation of $\Lambda(e^{i\pi/4})$ We shall argue that a good choice of $|a\rangle$ is a state

$$|a_4\rangle = \frac{1}{\sqrt{2}}(|\bar{0}\rangle + e^{i\pi/4}|\bar{1}\rangle = \Lambda(e^{i\pi/4})|\mp\rangle,$$

where $|\mp\rangle = 2^{-1/2}(|\bar{0}\rangle + |\bar{1}\rangle)$. The state $|a_4\rangle$ is composed of four σ particles. A purification protocol for $|a_4\rangle$ with a high threshold error rate and polylogarithmic overhead which uses only Clifford operation has been put forward in [25] under the name "magic-states distillation." For the sake of completeness we briefly describe it below. Then we assess an efficiency of the whole simulation scheme.

In the rest of this section a word "qubit" refers to a logical qubit encoded by four σ particles as explained in Sec. III. By abuse of notation we shall abbreviate $|\bar{0}\rangle$ to $|0\rangle$ and $|\bar{1}\rangle$ to $|1\rangle$. Accordingly, $|a_4\rangle$ will be regarded as a one-qubit state.

A. Converting $|a_4\rangle$ into a non-Clifford gate

We start from explaining how to execute the gate $\Lambda(e^{i\pi/4})$ using Clifford operations and one copy of $|a_4\rangle$; see [25]. Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be an unknown state (the coefficients a and b may actually be quantum states as well). Suppose we want to apply the gate $\Lambda(e^{i\pi/4})$ to $|\psi\rangle$. Let us start from a two-qubit state $|\Psi_0\rangle = |\psi \otimes a_4\rangle$ and measure an eigenvalue of observable $T_1 = \sigma^z \otimes \sigma^z$ (recall that any multiqubit Pauli operator can be converted by Clifford gates into a one-qubit operator σ^z, which is an admissible observable in the TQC model). The outcomes ±1 of the measurement appear with the probability 1/2 each, yielding the final states

$$|\Psi_1^+\rangle = a|0,0\rangle + be^{i\pi/4}|1,1\rangle,$$

$$|\Psi_1^-\rangle = ae^{i\pi/4}|0,1\rangle + b|1,0\rangle. \tag{38}$$

Applying the controlled σ^x operator $\Lambda(\sigma^x)$ with the first qubit as a control one, we get

$$|\Psi_2^+\rangle = \Lambda(\sigma^x)|\Psi_1^+\rangle = (a|0\rangle + be^{i\pi/4}|1\rangle) \otimes |0\rangle,$$

$$|\Psi_2^-\rangle = \Lambda(\sigma^x)|\Psi_1^-\rangle = (ae^{i\pi/4}|0\rangle + b|1\rangle) \otimes |1\rangle.$$

Now let us measure the second qubit in the $\{|0\rangle, |1\rangle\}$ basis. If the outcome is $|1\rangle$, apply the additional Clifford gate $K = |0\rangle\langle 0| + i|1\rangle\langle 1|$ to the first qubit (as was mentioned in Sec. III, K is a braid gate). In both cases we end up with the final state $a|0\rangle + be^{i\pi/4}|1\rangle$. Thus the input state $|\psi\rangle$ has been acted upon by $\Lambda(e^{i\pi/4})$.

B. Purification of $|a_4\rangle$

Here we outline the magic-states distillation method; see the original paper [25] for details. A noisy $|a_4\rangle$ state will be described by a one-qubit density matrix ρ. The quality of ρ is characterized by a parameter

$$\epsilon = 1 - \langle a_4|\rho|a_4\rangle,$$

which will be referred to as the *error rate*. The purification protocol exploits some nice properties of the CSS second-order punctured Reed-Muller quantum code. It encodes one qubit into 15 qubits and has the minimal distance 3. Let Π be a projector on the code subspace of the Reed-Muller code. Consider a state

$$\rho_{out} = Z^{-1}\Pi\rho^{\otimes 15}\Pi, \quad Z \equiv \mathrm{Tr}(\Pi\rho^{\otimes 15}).$$

Although ρ_{out} is a 15-qubit state, it can be regarded as a one-qubit state encoded by the Reed-Muller code. It turns out that an error rate ϵ_{out} of the state ρ_{out} is cubically suppressed as compared to the error rate of ρ,

$$\epsilon_{out} = 35\epsilon^3 + O(\epsilon^4).$$

The properties of the Reed-Muller quantum code that are responsible for this effect are the following: (i) The minimum Hamming weight of σ^z-type errors that are not detected by the code is 3. (ii) The code has non-Clifford automorphisms: an operator $\Lambda(e^{i\pi/4})^{\otimes 15}$ commutes with Π and its action on the encoded qubit coincides with $\Lambda(e^{i\pi/4})$.

This observation provides a natural mean of purifying ρ. Namely, one takes 15 copies of ρ and measures eigenvalues of 14 stabilizer operators for the Reed-Muller code. All stabilizers are the Pauli operators, so these measurements require only Clifford gates and admissible TQC measurements. The final state is accepted iff one observes the trivial syndrome (eigenvalue of all stabilizer operators is +1). After that one applies a decoding transformation (a certain Clifford group operator) that maps ρ_{out} onto a one-qubit state. The threshold value of ϵ is determined by an equation $\epsilon_{out}(\epsilon) = \epsilon$. Denote the threshold by δ_4. Its numerical value is

$$\delta_4 \approx 0.141.$$

If $\epsilon < \delta_4$, the output state ρ_{out} is more clean than the input one—i.e., $\epsilon_{out}(\epsilon) < \epsilon$.

Let p_s be the probability for this algorithm to succeed—i.e., the probability to observe the trivial syndrome. In the limit $\epsilon \to 0$ one has $p_s \approx 2^{-10}$. Moreover, by introducing an additional "error correction" step into the algorithm one can accept a larger set of measured syndromes (syndromes for which only all σ^x-type stabilizers have eigenvalue +1). The error correction step enhances the success probability to $p_s \approx 1$ (in the limit $\epsilon \to 0$).

The initial supply of states ρ with an error rate $\epsilon_0 \equiv \epsilon$ will be called level-0 ancillas. Accordingly, level-k ancillas are obtained from the level-0 ancillas by iterating the elementary purification procedure k times. Let ϵ_k and n_k be an error rate and the total number of level-k ancillas. The numbers ϵ_{k+1}, n_{k+1}, and ϵ_k, n_k are related by recursive flow equations

$$n_{k+1} \approx \frac{n_k}{15}, \quad \epsilon_{k+1} \approx 35\epsilon_k^3 \tag{39}$$

(we are interested in the asymptotic regime $\epsilon \ll 1$). Accordingly, if one needs to prepare one copy of $|a_4\rangle$ with an error rate ϵ', one needs to have a supply of

$$n_0 \sim |\ln(\epsilon')|^\gamma, \quad \gamma = \ln_3 15 \approx 2.5, \tag{40}$$

level-0 ancillas with an error rate below the threshold, $\epsilon_0 < \delta_4$. The operational cost of the purification—i.e., the total number of Clifford gates and standard measurements needed to achieve an error rate ϵ'—has the same scaling as n_0.

C. Efficiency analysis

Suppose our goal is to simulate a quantum circuit with N one-qubit and two-qubit gates operating on n qubits. We assume that the following gate set is used:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad \Lambda(e^{i\pi/4}), \quad \Lambda(\sigma^z). \tag{41}$$

The simulation must be able to reproduce the output of the circuit with a constant error probability. Accordingly, the nontopological gates $\Lambda(e^{i\pi/4})$ and $\Lambda(\sigma^z)$ have to be simulated with an error probability $\delta \sim N^{-1}$. As we have learned in Sec. IV, preparation of $|a_8\rangle$ with an accuracy δ requires about $[\ln(\delta^{-1})]^3$ raw ancillas ρ_8 and about the same number of TQC operations. According to Sec. V one copy of $|a_8\rangle$ can be traded for a gate $\Lambda(\sigma^z)$ implemented with about the same precision. Thus each $\Lambda(\sigma^z)$ gate "costs" $O([\ln(N)]^3)$ TQC operations and raw ancilla preparations.

Simulation of the gate $\Lambda(e^{i\pi/4})$ deserves more careful analysis. Consider one round of a_4 purification at the level k. It takes as input 15 copies of level-k ancillas $|a_4\rangle$ with an error rate ϵ_k and outputs one copy of $|a_4\rangle$ with an error rate ϵ_{k+1} (sometimes it outputs nothing because we use postselection). An implementation of this a_4-purification round requires $O(1)$ gates $\Lambda(\sigma^z)$. To simulate each of these gates the a_8-purification protocol has to be invoked. Obviously, at this point it does not make sense to purify $|a_8\rangle$ ancillas all the way down to the error rate $\delta \sim N^{-1}$. Instead, the error rate $O(\epsilon_k^3)$ is sufficient, since it still gives the flow equation $\epsilon_{k+1} = C\epsilon_k^3$ for a_4 purification with some constant C. Comparing Eqs. (18) and (40) one can see that for a fixed error rate the simulation of $\Lambda(\sigma^z)$ is more demanding in terms of resources than the simulation of $\Lambda(e^{i\pi/4})$. Therefore, we can try to use the above observation to improve the efficiency of the whole simulation scheme.

Indeed, purification of one copy of $|a_8\rangle$ with the final error rate $O(\epsilon_k^3)$ requires $m_k \sim [\ln(\epsilon_k)]^3$ elementary operations. From Eq. (39) one gets $\epsilon_k \sim \exp(-c3^k)$, where $c > 0$ is a constant. Therefore, $m_k \sim 3^{3k}$. The total number of a_4-purification rounds on the level k is $g_k \approx n_{k+1} \approx n_0 15^{-k-1}$, where n_0 is the number of level-0 ancillas $|a_4\rangle$. From Eq. (40) with $\delta \sim N^{-1}$ one gets $n_0 \approx [\ln(N)]^\gamma$. Thus the total number of elementary operation needed to generate all level-$(k+1)$ ancillas $|a_4\rangle$ is $M_k = m_k g_k \sim [\ln(N)]^\gamma 15^{-k} 3^{3k}$. Clearly, M_k grows exponentially with k, so almost all resources needed to purify $|a_4\rangle$ are spent at the highest level of a_4 purification. Accordingly, the total number of elementary operations needed to purify one copy of $|a_4\rangle$ with the final error rate $\delta \sim N^{-1}$ is

$$M_{tot} = \sum_{k=1}^{d} M_k \approx M_d,$$

where d is the total number of recursion levels in the distillation that can be determined by setting $\epsilon_d = \delta$ in Eq. (39)—i.e., $3^d \sim \ln(N)$. Thus

$$M_{tot} \approx M_d \sim [\ln(N)]^\gamma 15^{-d} 3^{3d} \sim 3^{3d} \sim [\ln(N)]^3.$$

We conclude that any gate in the universal gate set Eq. (41) "costs" $O([\ln(N)]^3)$ elementary operations.

VII. IMPLEMENTATION OF NONTOPOLOGICAL OPERATIONS

This part of the paper is rather speculative, since we know almost nothing about the nontopological properties of anyons, such as the effects of a finite separation between particles, nonadiabaticity of the anyonic transport, interaction between an anyon and a control device, etc.

Recall that we need nontopological operations to prepare (may be very noisy) ancillary states $|a_4\rangle$ and $|a_8\rangle$ composed of four and eight σ particles, respectively. We shall argue below that a good strategy is to use a direct short-range interaction between anyons. One can expect that the amplitude of this interaction decays as $\exp(-l/l_H)$, where l is a separation between the particles and l_H is the magnetic length [for experiments with AlGaAs/GaAs heterostructures the magnetic field corresponding to $\nu = 5/2$ is $B \approx 5$ T, so that $l_H = (\hbar c/eB)^{1/2} \approx 10^{-6}$ cm].

Remark. Note that any state in the orbit of $|a_4\rangle$ or $|a_8\rangle$ under the action of braid gates is equally acceptable as the states $|a_4\rangle$ and $|a_8\rangle$ themselves. As the number of particles increases, the size of the orbit grows, and thus the set of acceptable states becomes larger. For example, the orbit of $|a_4\rangle$ consists of 12 states (we disregard the overall phase),

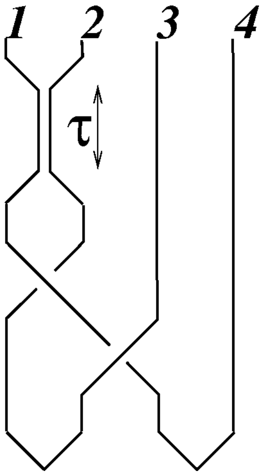

FIG. 10. A preparation of $|a_4\rangle$ based on the short-range two-particle interaction.

while the orbit of $|a_8\rangle$ consists of 240 states[2]. It suffices to prepare any of these states (we have to know which) with a fidelity above the threshold one.

A. How to prepare $|a_4\rangle$

Let us start from preparation of $|a_4\rangle$ since it is much easier. The preparation process is illustrated in Fig. 10. One starts from the vacuum state, creates two pairs of σ particles, and then brings two particles, one from each pair, sufficiently close to each other. After that one waits for a time τ and finally returns the particles to their original positions.

Taking into account that the short-range interaction is a local operator, we infer that the total charge of the four particles and the total charge of the particles 1 and 2 must be preserved. Therefore, the interaction can be described by a Hamiltonian

$$H_{int} = -i\hat{c}_1\hat{c}_2 \otimes X + I \otimes Y,$$

where X and Y are some operators acting on the environment.

A purpose of the two braid operations preceding the interaction in Fig. 10 is to create a state

$$|\phi\rangle = B_{1,2}^{\dagger}B_{2,3}|0,0\rangle = 2^{-1/2}(|0,0\rangle + |1,1\rangle) \in \mathcal{F}_4.$$

Using the qubit representation of Sec. III one gets $|\phi\rangle = 2^{-1/2}(|\bar{0}\rangle + |\bar{1}\rangle)$.

Free evolution under H_{int} for the time τ maps $|\phi\rangle$ onto a state

$$\frac{1}{\sqrt{2}}(|\bar{0}\rangle \otimes e^{i(X+Y)\tau}|\Psi_E\rangle + |\bar{1}\rangle \otimes e^{i(-X+Y)\tau}|\Psi_E\rangle).$$

Here $|\Psi_E\rangle$ is the initial state of the environment (one can always assume that it is pure). Tracing out the environment we end up with a mixed state

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & r \\ r^* & 1 \end{pmatrix}, \quad r = \langle \Psi_E | e^{i(X+Y)\tau} e^{i(X-Y)\tau} | \Psi_E \rangle.$$

The case $\rho = |a_4\rangle\langle a_4|$ corresponds to $r = e^{i\pi/4}$. By varying the interaction time τ we can try to fulfill the threshold condition $\langle a_4|\rho|a_4\rangle > 1 - \delta_4 \approx 0.86$. This may or may not be possible, depending upon particular form of X, Y, and $|\Psi_E\rangle$. For example, if X is proportional to the identity operator, $X = gI$, one gets

$$r = e^{2ig\tau}.$$

Tuning τ such that $g\tau = \pm\pi/8$ we can prepare the desired state $|a_4\rangle$ (or a state that can be converted to $|a_4\rangle$ by a braid gate).

B. How to prepare $|a_8\rangle$

The preparation of $|a_8\rangle$ based on the direct short-range interaction between anyons is more tricky because one has to cancel unwanted interactions. For example, if σ particles 1, 2, 3, and 4 are sufficiently close to each other, the interaction Hamiltonian looks as

$$H = -i\sum_{j,k} \hat{c}_j\hat{c}_k \otimes X_{jk} - \hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4 \otimes X + I \otimes Y,$$

where X_{jk}, X, and Y are some operators acting on the environment. Recall that $|a_8\rangle$ can be prepared by TQC operations and a nonlinear gate $W = \exp(i\pi/4\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4)$; see the first part of the proof of lemma 1. Free evolution under the Hamiltonian H might be used to implement W, provided that one can "turn off" the quadratic interactions $\hat{c}_j\hat{c}_k \otimes X_{jk}$. In principle, it can be done using a technique analogous to decoupling and refocusing in nuclear magnetic resonance. Indeed, denote $F = \hat{c}_1\hat{c}_2$, $G = \hat{c}_1\hat{c}_3$and consider a Hamiltonian

$$H' = \frac{1}{4}[H + FHF^{\dagger} + GHG^{\dagger} + (FG)H(FG)^{\dagger}].$$

One can easily check that

$$H' = -\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4 \otimes X + I \otimes Y.$$

Now let U_τ and U'_τ be unitary operators describing evolution under the Hamiltonians H and H', respectively, for a time τ. If τ is sufficiently small, one gets, from the Trotter expansion,

$$U'_\tau \approx U_{\tau/4} \cdot (FU_{\tau/4}F^{\dagger}) \cdot (GU_{\tau/4}G^{\dagger}) \cdot (FGU_{\tau/4}G^{\dagger}F^{\dagger}).$$

Therefore one could try to simulate U'_τ by $U_{\tau/4}$ and "control pulses" F and G. Obviously, F and G can be implemented by braid gates (for example, F corresponds to winding particle 1 around the particle 2). However, before applying any of these braid gates one has to return particles 1, 2, 3, and 4 into

[2] This counting goes along the following lines: (1) The set of four-qubit stabilizer states with a fixed parity consists of two nonoverlapping subsets: the orbit of $|a_8\rangle$ and the subset of "paired" states whose stabilizer group can be represented as in Eq. (8). (2) The number of four-qubit stabilizer states with a fixed parity (say, +1) is equal to the total number of three-qubit stabilizer states. (3) There are totally 1080 three-qubit stabilizer states. (4) There are totally $2^3 8!! = 840$ "paired" four-qubit stabilizer states with a fixed parity (say, +1). Therefore the number of states in the orbit of $|a_8\rangle$ is $1080 - 840 = 240$.

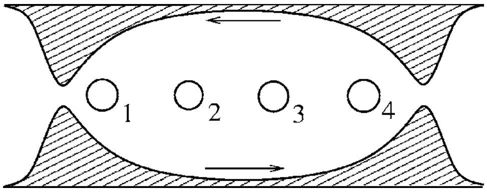

FIG. 11. A two-point contact interferometer. Four σ particles are trapped at antidots inside the interferometer loop. Electric current propagates along the top and bottom edges of the FQH electron gas (the unshaded region). Tunneling of σ particles occurs at the constrictions.

original well-separated positions. After that one can compose the evolutions U'_τ to simulate any desired interaction time.

The preparation of $|a_8\rangle$ based on the refocusing may fail to provide the necessary precision δ_8 because it involves too many noisy operations. So it is more fair to say that an additional nontopological operation is needed.

According to lemma 1, the state $|a_8\rangle$ can also be prepared by TQC operations and a nondestructive measurement of an observable $\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$. In other words, we have to measure the total topological charge (**1** or ψ) of four σ particles without destroying their pairwise correlations. It is very likely that such a measurement can be implemented using an interferometric device proposed recently by Bonderson, Kitaev, and Shtengel [16] (see also [18]) to test topological properties of σ particles.

The device is based on the Hall bar geometry (see Fig. 11), so that the transport of electric charge is governed by edge currents on the top and bottom edges of the bar. Electrical gates are used to create two constrictions in the region occupied by the FQH electron gas (the unshaded region in Fig. 11), so that σ particles can tunnel between the top and bottom edges through the electron gas at either constriction. The parameters of the device are tuned to allow quantum interference between the two tunneling paths. The total tunneling current is measured through the longitudinal resistance R_{xx}. Ideally, such a measurement projects the initial state onto an eigenvector of the tunneling current operator.

Suppose that four antidots are created inside the interferometer loop and exactly one σ particle is trapped at each antidot. Let us label the trapped σ particles by 1, 2, 3, and 4 and the tunneling σ particle by 0. The difference between the two tunneling paths corresponds to a braid b in which the tunneling particle 0 winds around the trapped particles 1, 2, 3, and 4; see Fig. 12. Using the braid group representation described in Sec. II one can easily find that the action of b is $\varphi(b) = +\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$. Thus the longitudinal resistance measurement projects the initial state of the particles 1, 2, 3, and 4 onto an eigenvector of $\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$. Combining the interferometric experiment with the standard TQC measurements one can calibrate the device to infer an eigenvalue of $\hat{c}_1\hat{c}_2\hat{c}_3\hat{c}_4$ from the measurement outcome.

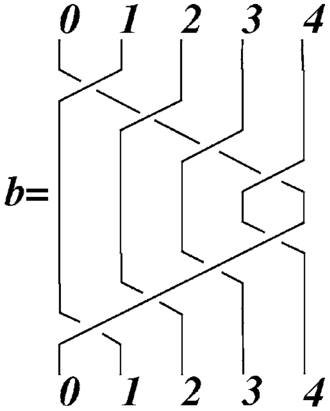

FIG. 12. A braid b describing interference of the two tunneling paths in the two-point contact interferometer.

ACKNOWLEDGMENTS

Discussions with Alexei Kitaev and Robert Raussendorf are gratefully acknowledged. The author would like to thank David DiVincenzo for a careful reading of this paper and Andrei Soklakov for useful comments concerning the magic-states distillation protocol. This research was carried out when the author was at the Institute for Quantum Information, Caltech, supported by the National Science Foundation under Grant No. EIA-0086038.

[1] P. W. Shor, in *Proceedings of the 37th Symposium on the Foundations of Computer Science*, (IEEE, Los Alamitos, CA, 1996), pp. 56–65.

[2] D. Aharonov and M. Ben-Or, e-print quant-ph/9611025.

[3] A. Y. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).

[4] P. Aliferis, D. Gottesman, and J. Preskill, e-print quant-ph/0504218.

[5] T. Szkopek, P. Boykin, H. Fan, V. Roychowdhury, E. Yablonovitch, G. Simms, M. Gyure, and B. Fong, e-print quant-ph/0411111.

[6] K. M. Svore, B. M. Terhal, and D. P. DiVincenzo, e-print quant-ph/0410047.

[7] E. Knill, Nature (London) **434**, 39 (2005).

[8] A. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (1997).

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

[10] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).

[11] R. Willett, J. P. Eisenstein, H. L. Störmer, D. C. Tsui, A. C. Gossard, and J. H. English, Phys. Rev. Lett. **59**, 1776 (1987).

[12] G. Moore and N. Read, Nucl. Phys. B **360**, 362 (1991).

[13] C. Nayak and F. Wilczek, Nucl. Phys. B **479**, 529 (1996).

[14] W. Pan, H. Stormer, D. Tsui, L. Pfeiffer, K. Baldwin, and K. West, e-print cond-mat/0103144.

[15] S. Das Sarma, M. Freedman, and C. Nayak, Phys. Rev. Lett. **94**, 166802 (2005).

[16] P. Bonderson, A. Kitaev, and K. Shtengel, e-print cond-mat/0508616.

[17] A. Stern and B. Halperin, e-print cond-mat/0508447.

[18] E. Fradkin, C. Nayak, A. Tsvelik, and F. Wilczek, Nucl. Phys. B **516**, 704 (1998).

[19] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[20] D. Gottesman, e-print quant-ph/9807006.

[21] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).

[22] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).

[23] E. Knill, e-print quant-ph/0108033.

[24] S. Bravyi, Quantum Inf. Comput. **5**(3), 216 (2005).

[25] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[26] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[27] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[28] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics (American Mathematical Society, Providence, RI, 2002).

[29] A. Kitaev, e-print cond-mat/0506438.

[30] S. Bravyi and A. Kitaev, Ann. Phys. (N.Y.) **298**, 210 (2002).

[31] S. Bravyi, e-print quant-ph/0507282.