Universal quantum computation with ideal Clifford gates and noisy ancillas

Sergey Bravyi* and Alexei Kitaev†
Institute for Quantum Information, California Institute of Technology, Pasadena, 91125 California, USA
(Received 6 May 2004; published 22 February 2005)

We consider a model of quantum computation in which the set of elementary operations is limited to Clifford unitaries, the creation of the state $|0\rangle$, and qubit measurement in the computational basis. In addition, we allow the creation of a one-qubit ancilla in a mixed state ρ, which should be regarded as a parameter of the model. Our goal is to determine for which ρ universal quantum computation (UQC) can be efficiently simulated. To answer this question, we construct purification protocols that consume several copies of ρ and produce a single output qubit with higher polarization. The protocols allow one to increase the polarization only along certain "magic" directions. If the polarization of ρ along a magic direction exceeds a threshold value (about 65%), the purification asymptotically yields a pure state, which we call a magic state. We show that the Clifford group operations combined with magic states preparation are sufficient for UQC. The connection of our results with the Gottesman-Knill theorem is discussed.

DOI: 10.1103/PhysRevA.71.022316 PACS number(s): 03.67.Lx, 03.67.Pp

I. INTRODUCTION AND SUMMARY

The theory of fault-tolerant quantum computation defines an important number called the error threshold. If the physical error rate is less than the threshold value δ, it is possible to stabilize computation by transforming the quantum circuit into a fault-tolerant form where errors can be detected and eliminated. However, if the error rate is above the threshold, then errors begin to accumulate, which results in rapid decoherence and renders the output of the computation useless. The actual value of δ depends on the error correction scheme and the error model. Unfortunately, this number seems to be rather small for all known schemes. Estimates vary from 10^{-6} (see Ref. [1]) to 10^{-4} (see Refs. [2–4]), which is hardly achievable with the present technology.

In principle, one can envision a situation in which qubits do not decohere, and a subset of the elementary gates is realized *exactly* due to special properties of the physical system. This scenario could be realized experimentally using spin, electron, or other many-body systems with topologically ordered ground states. Excitations in two-dimensional topologically ordered systems are anyons—quasiparticles with unusual statistics described by nontrivial representations of the braid group. If we have sufficient control of anyons, i.e., are able to move them around each other, fuse them, and distinguish between different particle types, then we can realize some set of unitary operators and measurements exactly. This set may or may not be computationally universal. While the universality can be achieved with sufficiently nontrivial types of anyons [5–8], more realistic systems offer only decoherence protection and an incomplete set of topological gates. (See Refs. [9,10] about non-Abelian anyons in quantum Hall systems and Refs. [11,12] about topological orders in Josephson junction arrays.) Nevertheless, universal computation is possible if we introduce some additional operations (e.g., measurements by Aharonov-Bohm interference [13] or some gates that are not related to topology at all). Of course, these nontopological operations cannot be implemented exactly and thus are prone to errors.

In this situation, the threshold error rate δ may become significantly larger than the values given above because we need to correct only errors of certain special type and we introduce a smaller amount of error in the correction stage. The main purpose of the present paper is to illustrate this statement by a particular computational model.

The model is built upon the *Clifford group*—the group of unitary operators that map the group of Pauli operators to itself under conjugation. The set of elementary operations is divided into two parts: $\mathcal{O}=\mathcal{O}_{\text{ideal}}\cup\mathcal{O}_{\text{faulty}}$. Operations from $\mathcal{O}_{\text{ideal}}$ are assumed to be perfect. We list these operations below:

(i) prepare a qubit in the state $|0\rangle$;

(ii) apply unitary operators from the Clifford group;

(iii) measure an eigenvalue of a Pauli operator (σ^x, σ^y, or σ^z) on any qubit.

Here we mean nondestructive projective measurement. We also assume that no errors occur between the operations.

It is well known that these operations are not sufficient for universal quantum computation (UQC) (unless a quantum computer can be efficiently simulated on a classical computer). More specifically, the Gottesman-Knill theorem states that by operations from $\mathcal{O}_{\text{ideal}}$ one can only obtain quantum states of a very special form called *stabilizer states*. Such a state can be specified as an intersection of eigenspaces of pairwise commuting Pauli operators, which are referred to as *stabilizers*. Using the stabilizer formalism, one can easily simulate the evolution of the state and the statistics of measurements on a classical probabilistic computer (see Ref. [14] or a textbook [15] for more details).

The set $\mathcal{O}_{\text{faulty}}$ describes faulty operations. In our model, it consists of just one operation: prepare an ancillary qubit in a mixed state ρ. The state ρ should be regarded as a parameter of the model. From the physical point of view, ρ is mixed due to imperfections of the preparation procedure (entanglement of the ancilla with the environment, thermal fluctua-

*Email address: serg@cs.caltech.edu
†Email address: kitaev@iqi.caltech.edu

tions, etc.). An essential requirement is that by preparing n qubits we obtain the state $\rho^{\otimes n}$, i.e., all ancillary qubits are independent. The independence assumption is similar to the uncorrelated errors model in the standard fault-tolerant computation theory.

Our motivation for including all Clifford group gates into $\mathcal{O}_{\text{ideal}}$ relies mostly on the recent progress in the fault-tolerant implementation of such gates. For instance, using a concatenated stabilizer code with good error correcting properties to encode each qubit and applying gates transversally (so that errors do not propagate inside code blocks) one can implement Clifford gates with an arbitrary high precision, see Ref. [16]. However, these nearly perfect gates act on *encoded* qubits. To establish a correspondence with our model, one needs to prepare an *encoded* ancilla in the state ρ. It can be done using the schemes for fault-tolerant encoding of an arbitrary *known* one-qubit state described by Knill in Ref. [17]. In the more recent paper [18] Knill constructed a scheme of fault-tolerant quantum computation which combines (i) the teleported computing and error correction technique by Gottesman and Chuang [19]; (ii) the method of purification of CSS states by Dür and Briegel [20]; and (iii) the magic states distillation algorithms described in the present paper. As was argued in Ref. [18], this scheme is likely to yield a much higher value for the threshold δ (it may be up to 1%).

Unfortunately, ideal implementation of the Clifford group cannot be currently achieved in any realistic physical system with a topological order. What universality classes of anyons allow one to implement all Clifford group gates (but do not allow one to simulate UQC) is an interesting open problem.

To fully utilize the potential of our model, we allow *adaptive* computation. It means that a description of an operation to be performed at step t may be a function of all measurement outcomes at steps $1,\ldots,t-1$. (For even greater generality, the dependence may be probabilistic. This assumption does not actually strengthen the model since tossing a fair coin can be simulated using $\mathcal{O}_{\text{ideal}}$) At this point, we need to be careful because the proper choice of operations should not only be defined mathematically—it should be computed by some *efficient algorithm*. In all protocols described below, the algorithms will actually be very simple. (Let us point out that dropping the computational complexity restriction still leaves a nontrivial problem: can we prepare an arbitrary multiqubit pure state with any given fidelity using only operations from the basis $\mathcal{O}$?)

The main question that we address in this paper is as follows: For which density matrices ρ can one efficiently simulate universal quantum computation by adaptive computation in the basis $\mathcal{O}$?

It will be convenient to use the Bloch sphere representation of one-qubit states:

$$\rho = \tfrac{1}{2}(I + \rho_x\sigma^x + \rho_y\sigma^y + \rho_z\sigma^z).$$

The vector (ρ_x,ρ_y,ρ_z) will be referred to as the *polarization vector* of ρ. Let us first consider the subset of states satisfying

$$|\rho_x| + |\rho_y| + |\rho_z| \leqslant 1.$$

This inequality says that the vector (ρ_x,ρ_y,ρ_z) lies inside the octahedron O with vertices (±1, 0, 0), (0, ±1, 0), (0, 0, ±1),

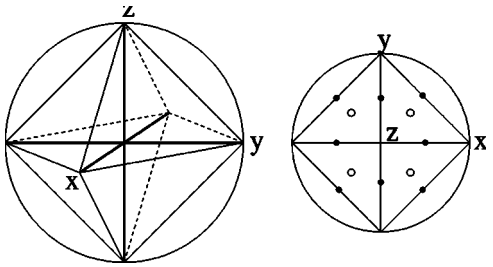

FIG. 1. Left: the Bloch sphere and the octahedron O. Right: the octahedron O projected on the $x-y$ plane. The magic states correspond to the intersections of the symmetry axes of O with the Bloch sphere. The empty and filled circles represent T-type and H-type magic states, respectively.

see Fig. 1. The six vertices of O represent the six eigenstates of the Pauli operators σ^x,σ^y, and σ^z. We can prepare these states by operations from O_{ideal} only. Since ρ is a convex linear combination (probabilistic mixture) of these states, we can prepare ρ by operations from $\mathcal{O}_{\text{ideal}}$ and by tossing a coin with suitable weights. Thus we can rephrase the Gottesman-Knill theorem in the following way.

Theorem 1. Suppose the polarization vector (ρ_x,ρ_y,ρ_z) of the state ρ belongs to the convex hull of (±1, 0, 0), (0, ±1, 0), (0, 0, ±1). Then any adaptive computation in the basis $\mathcal{O}$ can be efficiently simulated on a classical probabilistic computer.

This observation leads naturally to the following question: is it true that UQC can be efficiently simulated whenever ρ lies in the exterior of the octahedron O? In an attempt to provide at least a partial answer, we prove the universality for a large set of states. Specifically, we construct two particular schemes of UQC simulation based on a method which we call *magic states distillation*. Let us start by defining the magic states.

Definition 1. Consider pure states $|H\rangle,|T\rangle \in \mathbb{C}^2$ such that

$$|T\rangle\langle T| = \frac{1}{2}\left[I + \frac{1}{\sqrt{3}}(\sigma^x + \sigma^y + \sigma^z)\right],$$

and

$$|H\rangle\langle H| = \frac{1}{2}\left[I + \frac{1}{\sqrt{2}}(\sigma^x + \sigma^z)\right].$$

The images of $|T\rangle$ and $|H\rangle$ under the action of one-qubit Clifford operators are called magic states of T type and H type, respectively.

[This notation is chosen since $|H\rangle$ and $|T\rangle$ are eigenvectors of certain Clifford group operators: the Hadamard gate H and the operator usually denoted T, see Eq. (7).] Denote the one-qubit Clifford group by $\mathcal{C}_1$. Overall, there are 8 magic states of T type, $\{U|T\rangle, U \in \mathcal{C}_1\}$ (up to a phase) and 12 states of H type, $\{U|H\rangle, U \in \mathcal{C}_1\}$, see Fig. 1. Clearly, the polarization vectors of magic states are in one-to-one correspondence with rotational symmetry axes of the octahedron O (H-type states correspond to 180° rotations and T-type states correspond to 120° rotations). The role of magic states in our construction is twofold. First, adaptive computation in the basis $\mathcal{O}_{\text{ideal}}$ together with the preparation of magic states (of either type) allows one to simulate UQC (see Sec. III). Second, by adap-

tive computation in the basis $\mathcal{O}_{\text{ideal}}$ one can "purify" imperfect magic states. It is a rather surprising coincidence that one and the same state can comprise both of these properties, and that is the reason why we call them magic states.

More exactly, a magic state distillation procedure yields one copy of a magic state (with any desired fidelity) from several copies of the state ρ, provided that the initial fidelity between ρ and the magic state to be distilled is large enough. In the course of distillation, we use only operations from the set $\mathcal{O}_{\text{ideal}}$. By constructing two particular distillation schemes, for *T*-type and *H*-type magic states, respectively, we prove the following theorems.

Theorem 2. Let $F_T(\rho)$ be the maximum fidelity between ρ and a *T*-type magic state, i.e.,

$$F_T(\rho) = \max_{U \in \mathcal{C}_1} \sqrt{\langle T|U^\dagger \rho U|T\rangle}.$$

Adaptive computation in the basis $\mathcal{O}=\mathcal{O}_{\text{ideal}} \cup \{\rho\}$ allows one to simulate universal quantum computation whenever

$$F_T(\rho) > F_T = \left[\frac{1}{2}\left(1+\sqrt{\frac{3}{7}}\right)\right]^{1/2} \approx 0.910.$$

Theorem 3. Let $F_H(\rho)$ be the maximum fidelity between ρ and an *H*-type magic state,

$$F_H(\rho) = \max_{U \in \mathcal{C}_1} \sqrt{\langle H|U^\dagger \rho U|H\rangle}.$$

Adaptive computation in the basis $\mathcal{O}=\mathcal{O}_{\text{ideal}} \cup \{\rho\}$ allows one to simulate universal quantum computation whenever

$$F_H(\rho) > F_H \approx 0.927.$$

The quantities F_T and F_H have the meaning of threshold fidelity since our distillation schemes increase the polarization of ρ, converging to a magic state as long as the inequalities $F_T(\rho) > F_T$ or $F_H(\rho) > F_H$ are fulfilled. If they are not fulfilled, the process converges to the maximally mixed state. The conditions stated in the theorems can also be understood in terms of the polarization vector (ρ_x, ρ_y, ρ_z). Indeed, let us associate a "magic direction" with each of the magic states. Then Theorems 2 and 3 say that the distillation is possible if there is a *T* direction such that the projection of the vector (ρ_x, ρ_y, ρ_z) onto that *T* direction exceeds the threshold value of $2F_T^2-1 \approx 0.655$, or if the projection on some of the *H* directions is greater than $2F_H^2-1 \approx 0.718$.

Let us remark that, although the proposed distillation schemes are probably not optimal, the threshold fidelities F_T and F_H cannot be improved significantly. Indeed, it is easy to check that the octahedron *O* corresponding to probabilistic mixtures of stabilizer states can be defined as

$$\mathcal{O} = \{\rho : F_T(\rho) \leqslant F_T^*\},$$

where

$$F_T^* = \left[\frac{1}{2}\left(1+\sqrt{\frac{1}{3}}\right)\right]^{1/2} \approx 0.888.$$

It means that F_T^* is a lower bound on the threshold fidelity F_T for any protocol distilling *T*-type magic states. Thus any potential improvement to Theorem 2 may only decrease F_T from 0.910 down to $F_T^*=0.888$. From a practical perspective, the difference between these two numbers is not important.

On the other hand, such an improvement would be of great theoretical interest. Indeed, if Theorem 2 with F_T replaced by F_T^* is true, it would imply that the Gottesman-Knill theorem provides necessary and sufficient conditions for the classical simulation, and that a transition from classical to universal quantum behavior occurs at the boundary of the octahedron *O*. This kind of transition has been discussed in context of a general error model [21]. Our model is simpler, which gives hope for sharper results.

By the same argument, one can show that the quantity

$$F_H^* \overset{\text{def}}{=} \max_{\rho \in O} \sqrt{\langle H|\rho|H\rangle} = \left[\frac{1}{2}\left(1+\sqrt{\frac{1}{2}}\right)\right]^{1/2} \approx 0.924$$

is a lower bound on the threshold fidelity F_H for any protocol distilling *H*-type magic states.

A similar approach to UQC simulation was suggested in Ref. [22], where Clifford group operations were used to distill the entangled three-qubit state $|000\rangle+|001\rangle+|010\rangle+|100\rangle$, which is necessary for the realization of the Toffoli gate.

The rest of the paper is organized as follows. Section II contains some well-known facts about the Clifford group and stabilizer formalism, which will be used throughout the paper. In Sec. III we prove that magic states together with operations from $\mathcal{O}_{\text{ideal}}$ are sufficient for UQC. In Sec. IV ideal magic are substituted by faulty ones and the error rate that our simulation algorithm can tolerate is estimated. In Sec. V we describe a distillation protocol for *T*-type magic states. This protocol is based on the well-known five-qubit quantum code. In Sec. VI a distillation protocol for *H*-type magic states is constructed. It is based on a certain CSS stabilizer code that encodes one qubit into 15 and admits a nontrivial automorphism [23]. Specifically, the bitwise application of a certain *non-Clifford* unitary operator preserves the code subspace and effects the same operator on the encoded qubit. We conclude with a brief summary and a discussion of open problems.

II. CLIFFORD GROUP, STABILIZERS, AND SYNDROME MEASUREMENTS

Let $\mathcal{C}_n$ denote the *n*-qubit *Clifford group*. Recall that it is a finite subgroup of $\mathrm{U}(2^n)$ generated by the Hadamard gate *H* (applied to any qubit), the phase-shift gate *K* (applied to any qubit), and the controlled-not gate $\Lambda(\sigma^x)$ (which may be applied to any pair qubits),

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \Lambda(\sigma^x) = \begin{pmatrix} I & 0 \\ 0 & \sigma^x \end{pmatrix}. \tag{1}$$

The Pauli operators $\sigma^x, \sigma^y, \sigma^z$ belong to $\mathcal{C}_1$, for instance, $\sigma^z = K^2$ and $\sigma^x = HK^2H$. The *Pauli group* $P(n) \subset \mathcal{C}_n$ is generated by the Pauli operators acting on *n* qubits. It is known [24] that the Clifford group $\mathcal{C}_n$ augmented by scalar unitary operators $e^{i\varphi}I$ coincides with the normalizer of $P(n)$ in the uni-

tary group $U(2^n)$. Hermitian elements of the Pauli group are of particular importance for quantum error correction theory; they are referred to as *stabilizers*. These are operators of the form

$$\pm\sigma^{\alpha_1}\otimes\cdots\otimes\sigma^{\alpha_n},\quad \alpha_j\in\{0,x,y,z\},$$

where $\sigma^0=I$. Let us denote by $S(n)$ the set of all n-qubit stabilizers:

$$S(n)=\{S\in P(n)\ :\ S^\dagger=S\}.$$

For any two stabilizers S_1,S_2 we have $S_1S_2=\pm S_2S_1$ and $S_1^2=S_2^2=I$. It is known that for any set of pairwise commuting stabilizers $S_1,\ldots,S_k\in S(n)$ there exists a unitary operator $V\in\mathcal{C}_n$ such that

$$VS_jV^\dagger=\sigma^z[j],\quad j=1,\ldots,k,$$

where $\sigma^z[j]$ denotes the operator σ^z applied to the jth qubit, e.g., $\sigma^z[1]=\sigma^z\otimes I\otimes\cdots\otimes I$.

These properties of the Clifford group allow us to introduce a very useful computational procedure which can be realized by operations from $\mathcal{O}_{\text{ideal}}$. Specifically, we can perform a joint nondestructive eigenvalue measurement for any set of pairwise commuting stabilizers $S_1,\ldots,S_k\in S(n)$. The outcome of such a measurement is a sequence of eigenvalues $\lambda=(\lambda_1,\ldots,\lambda_k)$, $\lambda_j=\pm1$, which is usually called a *syndrome*. For any given outcome, the quantum state is acted upon by the projector

$$\Pi_\lambda=\prod_{j=1}^{k}\frac{1}{2}(I+\lambda_jS_j).$$

Now, let us consider a computation that begins with an arbitrary state and consists of operations from $\mathcal{O}_{\text{ideal}}$. It is clear that we can defer all Clifford operations until the very end if we replace the Pauli measurements by general syndrome measurements. Thus the most general transformation that can be realized by $\mathcal{O}_{\text{ideal}}$ is an *adaptive syndrome measurement*, meaning that the choice of the stabilizer S_j to be measured next depends on the previously measured values of $\lambda_1,\ldots,\lambda_{j-1}$. In general, this dependence may involve coin tossing. Without loss of generality one can assume that S_j commutes with all previously measured stabilizers $S_1,\ldots,S_{j-1}$ (for all possible values of $\lambda_1,\ldots,\lambda_{j-1}$ and coin tossing outcomes). Adaptive syndrome measurement has been used in Ref. [25] to distill entangled states of a bipartite system by local operations.

III. UNIVERSAL QUANTUM COMPUTATION WITH MAGIC STATES

In this section, we show that operations from $\mathcal{O}_{\text{ideal}}$ are sufficient for universal quantum computation if a supply of *ideal* magic states is also available. First, consider a one-qubit state

$$|A_\theta\rangle=2^{-1/2}(|0\rangle+e^{i\theta}|1\rangle) \tag{2}$$

and suppose that θ is not a multiple of $\pi/2$. We now describe a procedure that implements the phase shift gate

$$\Lambda(e^{i\theta})=\begin{pmatrix}1&0\\0&e^{i\theta}\end{pmatrix}$$

by consuming several copies of $|A_\theta\rangle$ and using only operations from $\mathcal{O}_{\text{ideal}}$.

Let $|\psi\rangle=a|0\rangle+b|1\rangle$ be the unknown initial state which should be acted on by $\Lambda(e^{i\theta})$. Prepare the state $|\Psi_0\rangle=|\psi\rangle\otimes|A_\theta\rangle$ and measure the stabilizer $S_1=\sigma^z\otimes\sigma^z$. Note that both outcomes of this measurement appear with probability $1/2$. If the outcome is "+1", we are left with the state

$$|\Psi_1^+\rangle=(a|0,0\rangle+be^{i\theta}|1,1\rangle).$$

In the case of "−1" outcome, the resulting state is

$$|\Psi_1^-\rangle=(ae^{i\theta}|0,1\rangle+b|1,0\rangle).$$

Let us apply the gate $\Lambda(\sigma^x)[1,2]$ (the first qubit is the control one). The above two states are mapped to

$$|\Psi_2^+\rangle=\Lambda(\sigma^x)[1,2]|\Psi_1^+\rangle=(a|0\rangle+be^{i\theta}|1\rangle)\otimes|0\rangle,$$

$$|\Psi_2^-\rangle=\Lambda(\sigma^x)[1,2]|\Psi_1^-\rangle=(ae^{i\theta}|0\rangle+b|1\rangle)\otimes|1\rangle.$$

Now the second qubit can be discarded, and we are left with the state $a|0\rangle+be^{\pm i\theta}|1\rangle$, depending upon the measured eigenvalue. Thus the net effect of this circuit is the application of a unitary operator that is chosen randomly between $\Lambda(e^{i\theta})$ and $\Lambda(e^{-i\theta})$ (and we know which of the two possibilities has occurred).

Applying the circuit repeatedly, we effect the transformations $\Lambda(e^{ip_1\theta})$, $\Lambda(e^{ip_2\theta})$,… for some integers $p_1,p_2,\ldots$ which obey the random-walk statistics. It is well known that such a random walk visits each integer with the probability 1. It means that sooner or later we will get $p_k=1$ and thus realize the desired operator $\Lambda(e^{i\theta})$. The probability that we will need more than N steps to succeed can be estimated as $cN^{-1/2}$ for some constant $c>0$. Note also that if θ is a rational multiple of 2π, we actually have a random walk on a cyclic group $\mathbb{Z}_q$. In this case, the probability that we will need more than N steps decreases exponentially with N.

The magic state $|H\rangle$ can be explicitly written in the standard basis as

$$|H\rangle=\cos\left(\frac{\pi}{8}\right)|0\rangle+\sin\left(\frac{\pi}{8}\right)|1\rangle. \tag{3}$$

Note that $HK|H\rangle=e^{i\pi/8}|A_{-\pi/4}\rangle$. So if we are able to prepare the state $|H\rangle$, we can realize the operator $\Lambda(e^{-i\pi/4})$. It does not belong to the Clifford group. Moreover, the subgroup of $U(2)$ generated by $\Lambda(e^{-i\pi/4})$ and $\mathcal{C}_1$ is dense in $U(2)$. [1] Thus the operators from $\mathcal{C}_1$ and $\mathcal{C}_2$ together with $\Lambda(e^{-i\pi/4})$ constitute a universal basis for quantum computation.

The magic state $|T\rangle$ can be explicitly written in the standard basis:

[1] Recall that the action of the Clifford group $\mathcal{C}_1$ on the set of operators $\pm\sigma^x$, $\pm\sigma^y$, $\pm\sigma^z$ coincides with the action of rotational symmetry group of a cube on the set of unit vectors $\pm e_x$, $\pm e_y$, $\pm e_z$, respectively.

$$|T\rangle = \cos\beta|0\rangle + e^{i(\pi/4)}\sin\beta|1\rangle, \quad \cos(2\beta) = \frac{1}{\sqrt{3}}. \qquad (4)$$

Let us prepare an initial state $|\Psi_0\rangle = |T\rangle \otimes |T\rangle$ and measure the stabilizer $S_1 = \sigma^z \otimes \sigma^z$. The outcome +1 appears with probability $p_+ = \cos^4\beta + \sin^4\beta = 2/3$. If the outcome is −1, we discard the reduced state and try again, using a fresh pair of magic states. (On average, we need three copies of the $|T\rangle$ state to get the outcome +1.) The reduced state corresponding to the outcome +1 is

$$|\Psi_1\rangle = \cos\gamma|0,0\rangle + i\sin\gamma|1,1\rangle, \quad \gamma = \frac{\pi}{12}.$$

Let us apply the gate $\Lambda(\sigma^x)[1,2]$ and discard the second qubit. We arrive at the state

$$|\Psi_2\rangle = \cos\gamma|0\rangle + i\sin\gamma|1\rangle.$$

Next apply the Hadamard gate H:

$$|\Psi_3\rangle = H|\Psi_2\rangle = 2^{-1/2}e^{i\gamma}(|0\rangle + e^{-2i\gamma}|1\rangle) = |A_{-\pi/6}\rangle.$$

We can use this state as described above to realize the operator $\Lambda(e^{-i\pi/6})$. It is easy to check that Clifford operators together with $\Lambda(e^{-i\pi/6})$ constitute a universal set of unitary gates.

Thus we have proved that the sets of operations $\mathcal{O}_{\text{ideal}} \cup \{|H\rangle\}$ and $\mathcal{O}_{\text{ideal}} \cup \{|T\rangle\}$ are sufficient for universal quantum computation.

IV. ERROR ANALYSIS

To establish a connection between the simulation algorithms described in Sec. III and the universality theorems stated in the introduction we have to substitute *ideal* magic states by *faulty* ones. Before doing that let us discuss the ideal case in more detail. Suppose that a quantum circuit to be simulated uses a gate basis in which the only non-Clifford gate is the phase shift $\Lambda(e^{-i\pi/4})$ or $\Lambda(e^{-i\pi/6})$. One can apply the algorithm of Sec. III to simulate each non-Clifford gate independently. To avoid fluctuations in the number of magic states consumed at each round, let us set a limit of K magic states per round, where K is a parameter to be chosen later. As was pointed out in Sec. III, the probability for some particular simulation round to "run out of budget" scales as $\exp(-\alpha K)$ for some constant $\alpha > 0$. If at least one simulation round runs out of budget, we declare a failure and the whole simulation must be aborted. Denote the total number of non-Clifford gates in the circuit by L. The probability p_a for the whole simulation to be aborted can be estimated as

$$p_a \sim 1 - [1 - \exp(-\alpha K)]^L \sim L\exp(-\alpha K) \ll 1,$$

provided that $L\exp(-\alpha K) \ll 1$. We will assume

$$K \gtrsim \alpha^{-1}\ln L,$$

so the abort probability can be neglected.

Each time the algorithm requests an ideal magic state, it actually receives a slightly nonideal one. Such nearly perfect magic states must be prepared using the distillation methods described in Secs. V and VI. Let us estimate an affordable error rate ϵ_{out} for *distilled* magic states. Since there are L non-Clifford gates in the circuit, one can tolerate an error rate of the order $1/L$ in implementation of these gates.[2] Each non-Clifford gate requires $K \sim \ln L$ magic states. Thus the whole simulation is reliable enough if one chooses

$$\epsilon_{\text{out}} \sim 1/(L\ln L). \qquad (5)$$

What are the resources needed to distill one copy of a magic state with the error rate ϵ_{out}? To be more specific, let us talk about H-type states. It will be shown in Sec. VI that the number n of raw (undistilled) ancillas needed to distill one copy of the $|H\rangle$ magic state with an error rate not exceeding ϵ_{out} scales as

$$n \sim [\ln(1/\epsilon_{\text{out}})]^\gamma, \quad \gamma = \log_3 15 \approx 2.5,$$

see Eq. (39). Taking ϵ_{out} from Eq. (5), one gets

$$n \sim (\ln L)^\gamma.$$

Since the whole simulation requires $KL \sim L\ln L$ copies of the distilled $|H\rangle$ state, we need

$$N \sim L(\ln L)^{\gamma+1}$$

raw ancillas overall.

Summarizing, the simulation theorems stated in the introduction follow from the following results (the last one will be proved later):

(i) the circuits described in Sec. III allow one to simulate UQC with the sets of operations $\mathcal{O}_{\text{ideal}} \cup \{|H\rangle\}$ and $\mathcal{O}_{\text{ideal}} \cup \{|T\rangle\}$;

(ii) these circuits work reliably enough if the states $|H\rangle$ and $|T\rangle$ are slightly noisy, provided that the error rate does not exceed $\epsilon_{\text{out}} \sim 1/(L\ln L)$;

(iii) a magic state having an error rate ϵ_{out} can be prepared from copies of the raw ancillary state ρ using the distillation schemes provided that $F_T(\rho) > F_T$ or $F_H(\rho) > F_H$. The distillation requires resources that are polynomial in $\ln L$.

V. DISTILLATION OF *T*-TYPE MAGIC STATES

Suppose we are given n copies of a state ρ, and our goal is to distill one copy of the magic state $|T\rangle$. The polarization vector of ρ can be brought into the positive octant of the Bloch space by a Clifford group operator, so we can assume that

$$\rho_x, \rho_y, \rho_z \geqslant 0.$$

In this case, the fidelity between ρ and $|T\rangle$ is the largest one among all T-type magic states, i.e.,

$$F_T(\rho) = \sqrt{\langle T|\rho|T\rangle}.$$

A related quantity,

[2]This fault tolerance does not require any redundancy in the implementation of the circuit (e.g., the use of concatenated codes). It is achived automatically because in the worst case the error probability accumulates linearly in the number of gates. In our model only non-Clifford gates are faulty.

$$\epsilon = 1 - \langle T|\rho|T\rangle = \frac{1}{2}\left[1 - \frac{1}{\sqrt{3}}(\rho_x + \rho_y + \rho_z)\right],$$

will be called the *initial error probability*. By definition, $0 \leqslant \epsilon \leqslant 1/2$.

The output of the distillation algorithm will be some one-qubit mixed state ρ_{out}. To quantify the proximity between ρ_{out} and $|T\rangle$, let us define a *final error probability*:

$$\epsilon_{\text{out}} = 1 - \langle T|\rho_{\text{out}}|T\rangle.$$

It will be certain function of n and ϵ. The asymptotic behavior of this function for $n \to \infty$ reveals the existence of a *threshold error probability*,

$$\epsilon_0 = \frac{1}{2}\left(1 - \sqrt{\frac{3}{7}}\right) \approx 0.173,$$

such that for $\epsilon < \epsilon_0$ the function $\epsilon_{\text{out}}(n,\epsilon)$ converges to zero. We will see that for small ϵ,

$$\epsilon_{\text{out}}(n,\epsilon) \sim (5\epsilon)^{n^\xi}, \quad \xi = 1/\log_2 30 \approx 0.2. \tag{6}$$

On the other hand, if $\epsilon > \epsilon_0$, the output state converges to the maximally mixed state, i.e., $\lim_{n\to\infty}\epsilon_{\text{out}}(n,\epsilon) = 1/2$.

Before coming to a detailed description of the distillation algorithm, let us outline the basic ideas involved in its construction. The algorithm recursively iterates an elementary distillation subroutine that transforms five copies of an imperfect magic state into one copy having a smaller error probability. This elementary subroutine involves a syndrome measurement for certain commuting stabilizers $S_1, S_2, S_3, S_4 \in S(5)$. If the measured syndrome $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ is nontrivial ($\lambda_j = -1$ for some j), the distillation attempt fails and the reduced state is discarded. If the measured syndrome is trivial ($\lambda_j = 1$ for all j), the distillation attempt is successful. Applying a decoding transformation (a certain Clifford operator) to the reduced state, we transform it to a single-qubit state. This qubit is the output of the subroutine.

Our construction is similar to concatenated codes used in many fault-tolerant quantum computation techniques, but it differs from them in two respects. First, we do not need to *correct* errors—it suffices only to *detect* them. Once an error has been detected, we simply discard the reduced state, since it does not contain any valuable information. This allows us to achieve higher threshold error probability. Second, we do not use quantum codes in the way for which they were originally designed: in our scheme, the syndrome is measured on a product state.

The state $|T\rangle$ is an eigenstate for the unitary operator

$$T = e^{i\pi/4}KH = \frac{e^{i\pi/4}}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \in \mathcal{C}_1. \tag{7}$$

Note that T acts on the Pauli operators as follows:[3]

$$T\sigma^x T^\dagger = \sigma^z, \quad T\sigma^z T^\dagger = \sigma^y, \quad T\sigma^y T^\dagger = \sigma^x. \tag{8}$$

We will denote its eigenstates by $|T_0\rangle$ and $|T_1\rangle$, so that

$$T|T_0\rangle = e^{+i\pi/3}|T_0\rangle, \quad T|T_1\rangle = e^{-i\pi/3}|T_1\rangle,$$

$$|T_{0,1}\rangle\langle T_{0,1}| = \frac{1}{2}\left[I \pm \frac{1}{\sqrt{3}}(\sigma^x + \sigma^y + \sigma^z)\right].$$

Note that $|T_0\rangle \overset{\text{def}}{=} |T\rangle$ and $|T_1\rangle = \sigma^y H|T_0\rangle$ are T-type magic states.

Let us apply a dephasing transformation,

$$D(\eta) = \frac{1}{3}(\eta + T\eta T^\dagger + T^\dagger \eta T), \tag{9}$$

to each copy of the state ρ. The transformation D can be realized by applying one of the operators I, T, T^{-1} chosen with probability $1/3$ each. Since

$$D(|T_0\rangle\langle T_1|) = D(|T_1\rangle\langle T_0|) = 0,$$

we have

$$D(\rho) = (1-\epsilon)|T_0\rangle\langle T_0| + \epsilon|T_1\rangle\langle T_1|. \tag{10}$$

We will assume that the dephasing transformation is applied at the very first step of the distillation, so ρ has the form (10). Thus the initial state for the elementary distillation subroutine is

$$\rho_{\text{in}} = \rho^{\otimes 5} = \sum_{x\in\{0,1\}^5} \epsilon^{|x|}(1-\epsilon)^{5-|x|}|T_x\rangle\langle T_x|, \tag{11}$$

where $x = (x_1, \ldots, x_5)$ is a binary string, $|x|$ is the number of 1's in x, and

$$|T_x\rangle \overset{\text{def}}{=} |T_{x_1}\rangle \otimes \cdots \otimes |T_{x_5}\rangle.$$

The stabilizers $S_1, \ldots, S_4$ to be measured on the state ρ_{in} correspond to the famous five-qubit code, see Refs. [26,27]. They are defined as follows:

$$S_1 = \sigma^x \otimes \sigma^z \otimes \sigma^z \otimes \sigma^x \otimes I,$$

$$S_2 = I \otimes \sigma^x \otimes \sigma^z \otimes \sigma^z \otimes \sigma^x,$$

$$S_3 = \sigma^x \otimes I \otimes \sigma^x \otimes \sigma^z \otimes \sigma^z,$$

$$S_4 = \sigma^z \otimes \sigma^x \otimes I \otimes \sigma^x \otimes \sigma^z. \tag{12}$$

This code has a cyclic symmetry, which becomes explicit if we introduce an auxiliary stabilizer, $S_5 = S_1S_2S_3S_4 = \sigma^z \otimes \sigma^z \otimes \sigma^x \otimes I \otimes \sigma^x$. Let $\mathcal{L}$ be the two-dimensional code subspace specified by the conditions $S_j|\Psi\rangle = |\Psi\rangle$, $j = 1, \ldots, 4$, and Π be the orthogonal projector onto $\mathcal{L}$:

$$\Pi = \frac{1}{16}\prod_{j=1}^{4}(I + S_j). \tag{13}$$

It was pointed out in Ref. [16] that the operators

$$\hat{X} = (\sigma^x)^{\otimes 5}, \quad \hat{Y} = (\sigma^y)^{\otimes 5}, \quad \hat{Z} = (\sigma^z)^{\otimes 5},$$

and

[3]The operator denoted by T in Ref. [16] does not coincide with our T. They are related by the substitution $T \to e^{-i\pi/4}T^\dagger$ though.

$$\hat{T} = (T)^{\otimes 5} \tag{14}$$

commute with Π, thus preserving the code subspace. Moreover, $\hat{X},\hat{Y},\hat{Z}$ obey the same algebraic relations as one-qubit Pauli operators, e.g., $\hat{X}\hat{Y}=i\hat{Z}$. Let us choose a basis in $\mathcal{L}$ such that $\hat{X},\hat{Y}$, and $\hat{Z}$ become logical Pauli operators σ^x,σ^y, and σ^z, respectively. How does the operator $\hat{T}$ act in this basis? From Eq. (8) we immediately get

$$\hat{T}\hat{X}\hat{T}^\dagger = \hat{Z}, \quad \hat{T}\hat{Z}\hat{T}^\dagger = \hat{Y}, \quad \hat{T}\hat{Y}\hat{T}^\dagger = \hat{X}.$$

Therefore $\hat{T}$ coincides with the logical operator T up to an overall phase factor. This factor is fixed by the condition that the logical T has eigenvalues $e^{\pm i(\pi/3)}$.

Let us find the eigenvectors of $\hat{T}$ that belong to $\mathcal{L}$. Consider two particular states from $\mathcal{L}$, namely

$$|T_1^L\rangle = \sqrt{6}\Pi|T_{00000}\rangle, \quad \text{and } |T_0^L\rangle = \sqrt{6}\Pi|T_{11111}\rangle.$$

In the Appendix we show that

$$\langle T_{00000}|\Pi|T_{00000}\rangle = \langle T_{11111}|\Pi|T_{11111}\rangle = \frac{1}{6}, \tag{15}$$

so that the states $|T_0^L\rangle$ and $|T_1^L\rangle$ are normalized. Taking into account that $[\hat{T},\Pi]=0$ and that

$$\hat{T}|T_x\rangle = e^{i(\pi/3)(5-2|x|)}|T_x\rangle \text{ for all } x \in \{0,1\}^5, \tag{16}$$

we get

$$\hat{T}|T_1^L\rangle = \sqrt{6}\hat{T}\Pi|T_{00000}\rangle = \sqrt{6}\Pi\hat{T}|T_{00000}\rangle = e^{-i\pi/3}|T_1^L\rangle.$$

Analogously, one can check that

$$\hat{T}|T_0^L\rangle = e^{+i\pi/3}|T_0^L\rangle.$$

It follows that $\hat{T}$ is exactly the logical operator T, including the overall phase, and $|T_0^L\rangle$ and $|T_1^L\rangle$ are the logical states $|T_0\rangle$ and $|T_1\rangle$ (up to some phase factors, which are not important for us). Therefore we have

$$|T_{0,1}^L\rangle\langle T_{0,1}^L| = \Pi\frac{1}{2}\left[I \pm \frac{1}{\sqrt{3}}(\hat{X}+\hat{Y}+\hat{Z})\right]. \tag{17}$$

Now we are in a position to describe the syndrome measurement performed on the state ρ_{in}. The unnormalized reduced state corresponding to the trivial syndrome is as follows:

$$\rho_s = \Pi\rho_{\text{in}}\Pi = \sum_{x\in\{0,1\}^5} \epsilon^{|x|}(1-\epsilon)^{5-|x|}\Pi|T_x\rangle\langle T_x|\Pi, \tag{18}$$

see Eq. (11). The probability for the trivial syndrome to be observed is

$$p_s = \text{Tr}\,\rho_s.$$

Note that the state $\Pi|T_x\rangle$ is an eigenvector of $\hat{T}$ for any $x \in \{0,1\}^5$. But we know that the restriction of $\hat{T}$ on $\mathcal{L}$ has eigenvalues $e^{\pm i\pi/3}$. At the same time, Eq. (16) implies that

$$\hat{T}\Pi|T_x\rangle = -\Pi|T_x\rangle$$

whenever $|x|=1$ or $|x|=4$. This eigenvalue equation is not a contradiction only if

$$\Pi|T_x\rangle = 0 \text{ for } |x| = 1,4.$$

This equality can be interpreted as an error correction property. Indeed, the initial state ρ_{in} is a mixture of the desired state $|T_{00000}\rangle$ and unwanted states $|T_x\rangle$ with $|x|>0$. We can interpret the number of "1" components in x as a number of errors. Once the trivial syndrome has been measured, we can be sure that either no errors or at least two errors have occurred. Such error correction, however, is not directly related to the minimal distance of the code.

It follows from Eq. (16) that for $|x|=2$, 3 one has $\hat{T}\Pi|T_x\rangle = e^{\pm i\pi/3}\Pi|T_x\rangle$, so that $\Pi|T_x\rangle$ must be proportional to one of the states $|T_0^L\rangle$, $|T_1^L\rangle$. Our observations can be summarized as follows:

$$\Pi|T_x\rangle = \begin{cases} 6^{-1/2}|T_1^L\rangle, & \text{if } |x|=0, \\ 0, & \text{if } |x|=1, \\ a_x|T_0^L\rangle, & \text{if } |x|=2, \\ b_x|T_1^L\rangle, & \text{if } |x|=3, \\ 0, & \text{if } |x|=4, \\ 6^{-1/2}|T_0^L\rangle, & \text{if } |x|=5. \end{cases} \tag{19}$$

Here the coefficients a_x, b_x depend upon x in some way. The output state (18) can now be written as

$$\rho_s = \left[\frac{1}{6}\epsilon^5 + \epsilon^2(1-\epsilon)^3\sum_{x:|x|=2}|a_x|^2\right]|T_0^L\rangle\langle T_0^L| + \left[\frac{1}{6}(1-\epsilon)^5 + \epsilon^3(1-\epsilon)^2\sum_{x:|x|=3}|b_x|^2\right]|T_1^L\rangle\langle T_1^L|. \tag{20}$$

To exclude the unknown coefficients a_x and b_x, we can use the identity

$$|T_0^L\rangle\langle T_0^L| + |T_1^L\rangle\langle T_1^L| = \Pi = \sum_{x\in\{0,1\}^5}\Pi|T_x\rangle\langle T_x|\Pi.$$

Substituting Eq. (19) into this identity, we get

$$\sum_{x:|x|=2}|a_x|^2 = \sum_{x:|x|=3}|b_x|^2 = \frac{5}{6}.$$

So the final expression for the output state ρ_s is as follows:

$$\rho_s = \left[\frac{\epsilon^5 + 5\epsilon^2(1-\epsilon)^3}{6}\right]|T_0^L\rangle\langle T_0^L| + \left[\frac{(1-\epsilon)^5 + 5\epsilon^3(1-\epsilon)^2}{6}\right] \times |T_1^L\rangle\langle T_1^L|. \tag{21}$$

Accordingly, the probability to observe the trivial syndrome is

$$p_s = \frac{\epsilon^5 + 5\epsilon^2(1-\epsilon)^3 + 5\epsilon^3(1-\epsilon)^2 + (1-\epsilon)^5}{6}. \tag{22}$$

A decoding transformaion for the five-qubit code is a unitary operator $V \in \mathcal{C}_5$ such that

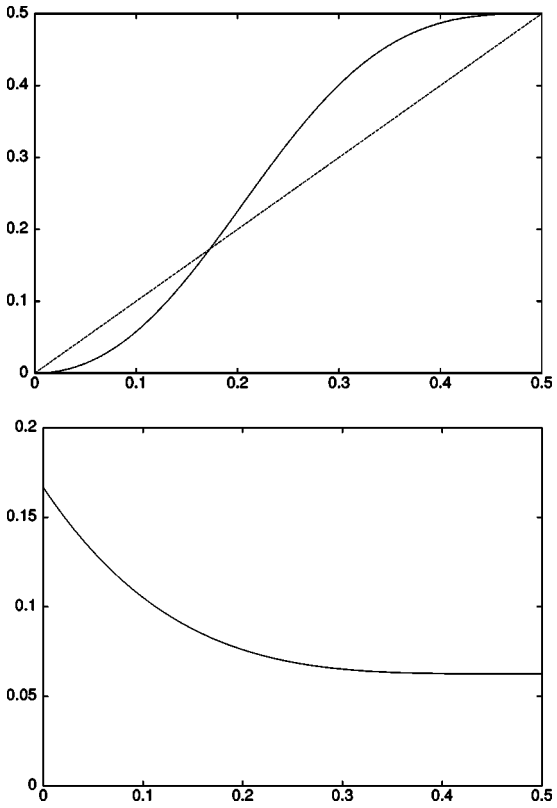

FIG. 2. The final error probability ϵ_{out} and the probability p_s to measure the trivial syndrome as functions of the initial error probability ϵ for the *T*-type states distillation.

$$V\mathcal{L} = \mathbb{C}^2 \otimes |0,0,0,0\rangle.$$

In other words, V maps the stabilizers S_j, $j=2$, 3, 4, 5 to $\sigma^z[j]$. The logical operators $\hat{X},\hat{Y},\hat{Z}$ are mapped to the Pauli operators $\sigma^x,\sigma^y,\sigma^z$ acting on the first qubit. From Eq. (17) we infer that

$$V|T_{0,1}^L\rangle = |T_{0,1}\rangle \otimes |0,0,0,0\rangle$$

(maybe up to some phase). The decoding should be followed by an additional operator $A=\sigma^y H \in \mathcal{C}_1$, which swaps the states $|T_0\rangle$ and $|T_1\rangle$ (note that for small ϵ the state ρ_s is close to $|T_1^L\rangle$, while our goal is to distill $|T_0\rangle$). After that we get a normalized output state

$$\rho_{\text{out}} = (1-\epsilon_{\text{out}})|T_0\rangle\langle T_0| + \epsilon_{\text{out}}|T_1\rangle\langle T_1|,$$

where

$$\epsilon_{\text{out}} = \frac{t^5+5t^2}{1+5t^2+5t^3+t^5}, \quad t=\frac{\epsilon}{1-\epsilon}. \tag{23}$$

The plot of the function $\epsilon_{\text{out}}(\epsilon)$ is shown on Fig. 2. It indicates that the equation $\epsilon_{\text{out}}(\epsilon)=\epsilon$ has only one nontrivial solution, $\epsilon=\epsilon_0\approx 0.173$. The exact value is

$$\epsilon_0 = \frac{1}{2}\left(1-\sqrt{\frac{3}{7}}\right).$$

If $\epsilon<\epsilon_0$, we can recursively iterate the elementary distillation subroutine to produce as good an approximation to the state $|T_0\rangle$ as we wish. On the other hand, if $\epsilon>\epsilon_0$, the distillation subroutine increases the error probability and iterations converge to the maximally mixed state. Thus ϵ_0 is a threshold error probability for our scheme. The corresponding threshold polarization is $1-2\epsilon_0=\sqrt{3/7}\approx 0.655$. For a sufficiently small ϵ, one can use the approximation $\epsilon_{\text{out}}(\epsilon)\approx 5\epsilon^2$.

The probability $p_s=p_s(\epsilon)$ to measure the trivial syndrome decreases monotonically from $1/6$ for $\epsilon=0$ to $1/16$ for $\epsilon=1/2$, see Fig. 2. In the asymptotic regime where ϵ is small, we can use the approximation $p_s\approx p_s(0)=1/6$.

Now the construction of the whole distillation scheme is straightforward. We start from $n\gg 1$ copies of the state $\rho=(1-\epsilon)|T_0\rangle\langle T_0|+\epsilon|T_1\rangle\langle T_1|$. Let us split these states into groups containing five states each and apply the elementary distillation subroutine described above to each group independently. In some of these groups the distillation attempt fails, and the outputs of such groups must be discarded. The average number of "successful" groups is obviously $p_s(\epsilon)\times(n/5)\approx n/30$ if ϵ is small. Neglecting the fluctuations of this quantity, we can say that our scheme provides a constant *yield* $r=1/30$ of output states that are characterized by the error probability $\epsilon_{\text{out}}(\epsilon)\approx 5\epsilon^2$. Therefore we can obtain $r^2 n$ states with $\epsilon_{\text{out}}\approx 5^3\epsilon^4$, $r^3 n$ states with $\epsilon_{\text{out}}\approx 5^7\epsilon^8$, and so on. We have created a hierarchy of states with n states on the first level and four or fewer states on the last level. Let k be the number of levels in this hierarchy and ϵ_{out} the error probability characterizing the states on the last level. Up to small fluctuations, the numbers $n,k,\epsilon_{\text{out}}$, and ϵ are related by the following obvious equations:

$$\epsilon_{\text{out}} \approx \tfrac{1}{5}(5\epsilon)^{2^k}, \quad r^k n \approx 1. \tag{24}$$

Their solution yields Eq. (6).

VI. DISTILLATION OF *H*-TYPE MAGIC STATES

A distillation scheme for *H*-type magic states also works by recursive iteration of a certain elementary distillation subroutine based on a syndrome measurement for a suitable stabilizer code. Let us start with introducing some relevant coding theory constructions, which reveal an unusual symmetry of this code and explain why it is particularly useful for *H*-type magic states distillation.

Let $\mathbb{F}_2^n$ be the n-dimensional binary linear space and A be a one-qubit operator such that $A^2=I$. With any binary vector $u=(u_1,\ldots,u_n)\in\mathbb{F}_2^n$ we associate the n-qubit operator

$$A(u) = A^{u_1}\otimes A^{u_2}\otimes\cdots\otimes A^{u_n}.$$

Let $(u,v)=\Sigma_{i=1}^n u_i v_i \bmod 2$ denote the standard binary inner product. If $\mathcal{L}\subseteq\mathbb{F}_2^n$ is a linear subspace, we denote by $\mathcal{L}^\perp$ the set of vectors which are orthogonal to $\mathcal{L}$. The Hamming weight of a binary vector u is denoted by $|u|$. Finally, $u\cdot v\in\mathbb{F}_2^n$ designates the bitwise product of u and v, i.e., $(u\cdot v)_i=u_i v_i$.

A systematic way of constructing stabilizer codes was suggested by Calderbank, Shor, and Steane, see Refs. [28,29]. Codes that can be described in this way will be referred to as *standard CSS codes*. In addition, we consider

their images under an arbitrary unitary transformation $V \in \mathrm{U}(2)$ applied to every qubit. Such "rotated" codes will be called *CSS codes*.

Definition 2. Consider a pair of one-qubit Hermitian operators A, B such that

$$A^2 = B^2 = I, \quad AB = -BA,$$

and a pair of binary vector spaces $\mathcal{L}_A, \mathcal{L}_B \subseteq \mathbb{F}_2^n$, such that

$$(u,v) = 0 \text{ for all } u \in \mathcal{L}_A, v \in \mathcal{L}_B.$$

A quantum code $\mathrm{CSS}(A, \mathcal{L}_A; B, \mathcal{L}_B)$ is a decomposition

$$(\mathbb{C}^2)^{\otimes n} = \bigoplus_{\mu \in \mathcal{L}_A^*} \bigoplus_{\eta \in \mathcal{L}_B^*} \mathcal{H}(\mu, \eta), \tag{25}$$

where the subspace $\mathcal{H}(\mu, \eta)$ is defined by the conditions

$$A(u)|\Psi\rangle = (-1)^{\mu(u)}|\Psi\rangle, \quad B(v)|\Psi\rangle = (-1)^{\eta(v)}|\Psi\rangle$$

for all $u \in \mathcal{L}_A$ and $v \in \mathcal{L}_B$. The linear functionals μ and η are referred to as A syndrome and B syndrome, respectively. The subspace $\mathcal{H}(0,0)$ corresponding to the trivial syndromes $\mu = \eta = 0$ is called the code subspace.

The subspaces $\mathcal{H}(\mu, \eta)$ are well defined since the operators $A(u)$ and $B(v)$ commute for any $u \in \mathcal{L}_A$ and $v \in \mathcal{L}_B$:

$$A(u)B(v) = (-1)^{(u,v)}B(v)A(u) = B(v)A(u).$$

The number of logical qubits in a CSS code is

$$k = \log_2[\dim \mathcal{H}(0,0)] = n - \dim \mathcal{L}_A - \dim \mathcal{L}_B.$$

Logical operators preserving the subspaces $\mathcal{H}(\mu, \eta)$ can be chosen as

$$\{A(u) : u \in \mathcal{L}_B^{\perp}/\mathcal{L}_A\} \text{ and } \{B(v) : v \in \mathcal{L}_A^{\perp}/\mathcal{L}_B\}.$$

(By definition, $\mathcal{L}_A \subseteq \mathcal{L}_B^{\perp}$ and $\mathcal{L}_B \subseteq \mathcal{L}_A^{\perp}$, so the factor spaces are well defined.) In the case where A and B are Pauli operators, we get a standard CSS code. Generally, $A = V\sigma^z V^{\dagger}$ and $B = V\sigma^x V^{\dagger}$ for some unitary operator $V \in \mathrm{SU}(2)$, so an arbitrary CSS code can be mapped to a standard one by a suitable bitwise rotation. By a syndrome measurement for a CSS code we mean a projective measurement associated with the decomposition (25).

Consider a CSS code such that some of the operators $A(u)$, $B(v)$ do not belong to the Pauli group $P(n)$. Let us pose this question: can one perform a syndrome measurement for this code by operations from $\mathcal{O}_{\mathrm{ideal}}$ only? It may seem that the answer is no, because by definition of $\mathcal{O}_{\mathrm{ideal}}$ one cannot measure an eigenvalue of an operator unless it belongs to the Pauli group. Surprisingly, this naive answer is wrong. Indeed, imagine that we have measured part of the operators $A(u)$, $B(v)$ (namely, those that belong to the Pauli group). Now we may restrict the remaining operators to the subspace corresponding to the obtained measurement outcomes. It may happen that the restriction of some unmeasured operator $A(u)$, which does not belong to the Pauli group, coincides with the restriction of some other operator $\widetilde{A}(\widetilde{u}) \in P(n)$. If this is the case, we can safely measure $\widetilde{A}(\widetilde{u})$ instead of $A(u)$. The 15-qubit code that we use for the distillation is actually the simplest (to our knowledge) CSS code exhibiting this strange behavior. We now come to an explicit description of this code.

Consider a function f of four Boolean variables. Denote by $[f] \in \mathbb{F}_2^{15}$ the table of all values of f except $f(0000)$. The table is considered as a binary vector, i.e.,

$$[f] = (f(0001), f(0010), f(0011), \ldots, f(1111)).$$

Let $\mathcal{L}_1$ be the set of all vectors $[f]$, where f is a linear function satisfying $f(0) = 0$. In other words, $\mathcal{L}_1$ is the linear subspace spanned by the four vectors $[x_j]$, $j = 1, 2, 3, 4$ (where x_j is an indicator function for the jth input bit):

$$\mathcal{L}_1 = \text{linear span}([x_1],[x_2],[x_3],[x_4]).$$

Let also $\mathcal{L}_2$ be the set of all vectors $[f]$, where f is a polynomial of degree at most 2 satisfying $f(0) = 0$. In other words, $\mathcal{L}_2$ is the linear subspace spanned by the four vectors $[x_j]$ and the six vectors $[x_i x_j]$:

$$\mathcal{L}_2 = \text{linear span}([x_1],[x_2],[x_3],[x_4],[x_1x_2],[x_1x_3], [x_1x_4],[x_2x_3],[x_2x_4],[x_3x_4]). \tag{26}$$

The definition of $\mathcal{L}_1$ and $\mathcal{L}_2$ resembles the definition of punctured Reed-Muller codes of order 1 and 2, respectively, see Ref. [30]. Note also that $\mathcal{L}_1$ is the dual space for the 15-bit Hamming code. The relevant properties of the subspaces $\mathcal{L}_j$ are stated in the following lemma.

Lemma 1.

(1) For any $u \in \mathcal{L}_1$ one has $|u| \equiv 0 (\mathrm{mod}\ 8)$.

(2) For any $v \in \mathcal{L}_2$ one has $|v| \equiv 0 (\mathrm{mod}\ 2)$.

(3) Let $[1]$ be the unit vector (1, 1,…, 1, 1). Then $\mathcal{L}_1^{\perp} = \mathcal{L}_2 \oplus [1]$ and $\mathcal{L}_2^{\perp} = \mathcal{L}_1 \oplus [1]$.

(4) For any vectors $u, v \in \mathcal{L}_1$ one has $|u \cdot v| \equiv 0 (\mathrm{mod}\ 4)$.

(5) For any vectors $u \in \mathcal{L}_1$ and $v \in \mathcal{L}_2^{\perp}$ one has $|u \cdot v| \equiv 0 (\mathrm{mod}\ 4)$.

Proof.

(1) Any linear function f on $\mathbb{F}_2^4$ satisfying $f(0) = 0$ takes value 1 exactly eight times (if $f \neq 0$) or zero times (if $f = 0$).

(2) All basis vectors of $\mathcal{L}_2$ have weight equal to 8 (the vectors $[x_i]$) or 4 (the vectors $[x_i x_j]$). By linearity, all elements of $\mathcal{L}_2$ have even weight.

(3) One can easily check that all basis vectors of $\mathcal{L}_1$ are orthogonal to all basis vectors of $\mathcal{L}_2$, therefore $\mathcal{L}_1 \subseteq \mathcal{L}_2^{\perp}$, $\mathcal{L}_2 \subseteq \mathcal{L}_1^{\perp}$. Besides, we have already proved that $[1] \in \mathcal{L}_1^{\perp}$ and $[1] \in \mathcal{L}_2^{\perp}$. Now the statement follows from dimension counting, since $\dim \mathcal{L}_1 = 4$ and $\dim \mathcal{L}_2 = 10$.

(4) Without loss of generality we may assume that $u \neq 0$ and $v \neq 0$. If $u = v$, the statement has been already proved, see property 1. If $u \neq v$, then $u = [f]$, $v = [g]$ for some linearly independent linear functions f and g. We can introduce new coordinates (y_1, y_2, y_3, y_4) on $\mathbb{F}_2^4$ such that $y_1 = f(x)$ and $y_2 = g(x)$. Now $|u \cdot v| = |[y_1 y_2]| = 4$.

(5) Let $u \in \mathcal{L}_1$ and $v \in \mathcal{L}_2^{\perp}$. Since $\mathcal{L}_2^{\perp} = \mathcal{L}_1 \oplus [1]$, there are two possibilities: $v \in \mathcal{L}_1$ and $v = [1] + w$ for some $w \in \mathcal{L}_1$. The first case has been already considered. In the second case we have

$$|u \cdot v| = \sum_{j=1}^{15} u_j(1 - w_j) = |u| - |u \cdot w|.$$

It follows from properties 1 and 4 that $|u \cdot v| \equiv 0 (\mathrm{mod}\, 4)$. □

Now consider the one-qubit Hermitian operator

$$A = \frac{1}{\sqrt{2}}(\sigma^x + \sigma^y) = \begin{pmatrix} 0 & e^{-i(\pi/4)} \\ e^{+i(\pi/4)} & 0 \end{pmatrix} = e^{-1(\pi/4)} K \sigma^x,$$

where K is the phase shift gate, see Eq. (1). By definition, A belongs to the Clifford group $\mathcal{C}_1$. One can easily check that $A^2 = I$ and $A\sigma^z = -\sigma^z A$, so the code $\mathrm{CSS}(\sigma^z, \mathcal{L}_2; A, \mathcal{L}_1)$ is well defined. We claim that its code subspace coincides with the code subspace of a certain stabilizer code.

Lemma 2. Consider the decomposition

$$(\mathbb{C}^2)^{\otimes 15} = \bigoplus_{\mu \in \mathcal{L}_2^*} \bigoplus_{\eta \in \mathcal{L}_1^*} \mathcal{H}(\mu, \eta),$$

associated with the code $\mathrm{CSS}(\sigma^z, \mathcal{L}_2; A, \mathcal{L}_1)$ and the decomposition

$$(\mathbb{C}^2)^{\otimes 15} = \bigoplus_{\mu \in \mathcal{L}_2^*} \bigoplus_{\eta \in \mathcal{L}_1^*} \mathcal{G}(\mu, \eta),$$

associated with the stabilizer code $\mathrm{CSS}(\sigma^z, \mathcal{L}_2; \sigma^x, \mathcal{L}_1)$. For any syndrome $\eta \in \mathcal{L}_1^*$ one has

$$\mathcal{H}(0, \eta) = \mathcal{G}(0, \eta).$$

Moreover, for any $\mu \in \mathcal{L}_2^*$ there exists some $w \in \mathbb{F}_2^{15}$ such that for any $\eta \in \mathcal{L}_1^*$

$$\mathcal{H}(\mu, \eta) = A(w)\mathcal{G}(0, \eta). \tag{27}$$

This Lemma provides a strategy to measure a syndrome of the code $\mathrm{CSS}(\sigma^z, \mathcal{L}_2; A, \mathcal{L}_1)$ by operations from $\mathcal{O}_{\mathrm{ideal}}$. Specifically, we measure μ (i.e., the σ^z part of the syndrome) first, compute $w = w(\mu)$, apply $A(w)^\dagger$, measure η using the stabilizers $\sigma^x([x_j])$, and apply $A(w)$.

Proof of the lemma. Consider an auxiliary subspace,

$$\mathcal{H} = \bigoplus_{\eta \in \mathcal{L}_1^*} \mathcal{H}(0, \eta) = \bigoplus_{\eta \in \mathcal{L}_1^*} \mathcal{G}(0, \eta),$$

corresponding to the trivial σ^z syndrome for both CSS codes. Each state $|\Psi\rangle \in \mathcal{H}(0)$ can be represented as

$$|\Psi\rangle = \sum_{v \in \mathcal{L}_2^\perp} c_v |v\rangle,$$

where c_v are some complex amplitudes and $|v\rangle = |v_1, \ldots, v_{15}\rangle$ are vectors of the standard basis. Let us show that

$$A(u)|\Psi\rangle = \sigma^x(u)|\Psi\rangle \text{ for any } |\Psi\rangle \in \mathcal{H}, \quad u \in \mathcal{L}_1.$$

To this end, we represent A as $\sigma^x e^{i\pi/4} K^\dagger$. For any $u \in \mathcal{L}_1$ and $v \in \mathcal{L}_2^\perp$ we have

$$A(u)|v\rangle = \sigma^x(u) e^{i(\pi/4)|u| - i(\pi/2)|u \cdot v|} |v\rangle = \sigma^x(u)|v\rangle,$$

because $|u| \equiv 0 (\mathrm{mod}\, 8)$ and $|u \cdot v| \equiv 0 (\mathrm{mod}\, 4)$ (see Lemma 1, parts 1 and 5).

Since for any $u \in \mathcal{L}_1$ the operators $A(u)$ and $\sigma^x(u)$ act on $\mathcal{H}$ in the same way, their eigenspaces must coincide, i.e., $\mathcal{H}(0, \eta) = \mathcal{G}(0, \eta)$ for any $\eta \in \mathcal{L}_1^*$.

Let us now consider the subspace $\mathcal{H}(\mu, \eta)$ for arbitrary $\mu \in \mathcal{L}_2^*$, $\eta \in \mathcal{L}_1^*$. By definition, μ is a linear functional on $\mathcal{L}_2 \subseteq \mathbb{F}_2^{15}$; we can extend it to a linear functional on $\mathbb{F}_2^{15}$, i.e., represent it in the form $\mu(v) = (w, v)$ for some $w \in \mathbb{F}_2^{15}$. Then for any $|\Psi\rangle \in \mathcal{H}(\mu, \eta)$, $v \in \mathcal{L}_2$, and $u \in \mathcal{L}_1$ we have

$$\sigma^z(v) A(w)^\dagger |\Psi\rangle = (-1)^{(w,v)} A(w)^\dagger \sigma^z(v)|\Psi\rangle = A(w)^\dagger |\Psi\rangle,$$

$$A(u)A(w)^\dagger |\Psi\rangle = A(w)^\dagger A(u)|\Psi\rangle = (-1)^{\eta(v)} A(w)^\dagger |\Psi\rangle$$

(as σ^z and A anticommute), hence $A(w)^\dagger |\Psi\rangle \in \mathcal{H}(0, \eta)$. Thus

$$\mathcal{H}(\mu, \eta) = A(w)\mathcal{H}(0, \eta) = A(w)\mathcal{G}(0, \eta).$$

□

Lemma 2 is closely related to an interesting property of the stabilizer code $\mathrm{CSS}(\sigma^z, \mathcal{L}_2; \sigma^x, \mathcal{L}_1)$, namely the existence of a non-Clifford automorphism [23]. Consider a one-qubit unitary operator W such that

$$W\sigma^z W^\dagger = \sigma^z \text{ and } W\sigma^x W^\dagger = A.$$

It is defined up to an overall phase and obviously does not belong to the Clifford group $\mathcal{C}_1$. However, the bitwise application of W, i.e., the operator $W^{\otimes 15}$, preserves the code subspace $\mathcal{G}(0,0)$. Indeed, $W^{\otimes 15}\mathcal{G}(0,0)$ corresponds to the trivial syndrome of the code

$$\mathrm{CSS}(W\sigma^z W^\dagger, \mathcal{L}_2; W\sigma^x W^\dagger, \mathcal{L}_1) = \mathrm{CSS}(\sigma^z, \mathcal{L}_2; A, \mathcal{L}_1).$$

Thus $W^{\otimes 15}\mathcal{G}(0,0) = \mathcal{H}(0,0)$. But $\mathcal{H}(0,0) = \mathcal{G}(0,0)$ due to the lemma.

Now we are in a position to describe the distillation scheme and to estimate its threshold and yield. Suppose we are given 15 copies of the state ρ, and our goal is to distill one copy of an H-type magic state. We will actually distill the state,

$$|A_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle) = e^{i\frac{\pi}{8}} HK^\dagger |H\rangle.$$

Note that $|A_0\rangle$ is an eigenstate of the operator A; specifically, $A|A_0\rangle = |A_0\rangle$. Let us also introduce the state

$$|A_1\rangle = \sigma^z |A_0\rangle,$$

which satisfies $A|A_1\rangle = -|A_1\rangle$. Since the Clifford group $\mathcal{C}_1$ acts transitively on the set of H-type magic states, we can assume that the fidelity between ρ and $|A_0\rangle$ is the maximum one among all H-type magic states, so that

$$F_H(\rho) = \sqrt{\langle A_0|\rho|A_0\rangle}.$$

As in Sec. V we define the initial error probability

$$\epsilon = 1 - [F_H(\rho)]^2 = \langle A_1|\rho|A_1\rangle.$$

Applying the dephasing transformation

$$D(\eta) = \frac{1}{2}(\eta + A\eta A^\dagger)$$

to each copy of ρ, we can guarantee that ρ is diagonal in the $\{A_0, A_1\}$ basis, i.e.,

$$\rho = D(\rho) = (1-\epsilon)|A_0\rangle\langle A_0| + \epsilon|A_1\rangle\langle A_1|.$$

Since $A \in \mathcal{C}_1$, the dephasing transformation can be realized by operations from $\mathcal{O}_{\text{ideal}}$. Thus our initial state is

$$\rho_{\text{in}} = \rho^{\otimes 15} = \sum_{u \in \mathbb{F}_2^{15}} \epsilon^{|u|}(1-\epsilon)^{15-|u|}|A_u\rangle\langle A_u|, \tag{28}$$

where $|A_u\rangle = |A_{u_0}\rangle \otimes \cdots \otimes |A_{u_{15}}\rangle$.

According to the remark following the formulation of Lemma 2, we can measure the syndrome (μ, η) of the code $\text{CSS}(\sigma^z, \mathcal{L}_2; A, \mathcal{L}_1)$ by operations from $\mathcal{O}_{\text{ideal}}$ only. Let us follow this scheme, omitting the very last step. So, we begin with the state ρ_{in}, measure μ, compute $w = w(\mu)$, apply $A(w)^\dagger$, and measure η. We consider the distillation attempt successful if $\eta = 0$. The measured value of μ is not important at this stage. In fact, for any $\mu \in \mathcal{L}_2^*$ the unnormalized post-measurement state is

$$\rho_s = \Pi A(w)^\dagger \rho_{\text{in}} A(w)\Pi = \Pi \rho_{\text{in}} \Pi.$$

In this equation Π is the projector onto the code subspace $\mathcal{H}(0,0) = \mathcal{G}(0,0)$, i.e., $\Pi = \Pi_z \Pi_A$ for

$$\Pi_z = \frac{1}{|\mathcal{L}_2|}\sum_{v \in \mathcal{L}_2} \sigma^z(v), \quad \Pi_A = \frac{1}{|\mathcal{L}_1|}\sum_{u \in \mathcal{L}_1} A(u). \tag{29}$$

Let us compute the state $\rho_s = \Pi \rho_{\text{in}} \Pi$. Since

$$A(u)|A_w\rangle = (-1)^{(u,w)}|A_w\rangle, \quad \sigma^z(v)|A_w\rangle = |A_{w+v}\rangle,$$

one can easily see that $\Pi_A|A_w\rangle = |A_w\rangle$ if $w \in \mathcal{L}_1^\perp$, otherwise $\Pi_A|A_w\rangle = 0$. On the other hand, $\Pi_z|A_w\rangle$ does not vanish and depends only on the coset of $\mathcal{L}_2$ that contains w. There are only two such cosets in $\mathcal{L}_1^\perp$ (because $\mathcal{L}_1^\perp = \mathcal{L}_2 \oplus [1]$, see Lemma 1), and the corresponding projected states are

$$|A_0^L\rangle = \sqrt{|\mathcal{L}_2|}\Pi_z|A_{0\ldots0}\rangle = \frac{1}{\sqrt{|\mathcal{L}_2|}}\sum_{v \in \mathcal{L}_2}|A_v\rangle,$$

$$|A_1^L\rangle = \sqrt{|\mathcal{L}_2|}\Pi_z|A_{1\ldots1}\rangle = \frac{1}{\sqrt{|\mathcal{L}_2|}}\sum_{v \in \mathcal{L}_2}|A_{v+[1]}\rangle. \tag{30}$$

The states $|A_{0,1}^L\rangle$ form an orthonormal basis of the code subspace. The projections of $|A_w\rangle$ for $w \in \mathcal{L}_1^\perp$ onto the code subspace are given by these formulas:

$$\Pi|A_w\rangle = \frac{1}{\sqrt{|\mathcal{L}_2|}}|A_0^L\rangle \text{ if } w \in \mathcal{L}_2,$$

$$\Pi|A_w\rangle = \frac{1}{\sqrt{|\mathcal{L}_2|}}|A_1^L\rangle \text{ if } w \in \mathcal{L}_2 + [1].$$

Now the unnormalized final state $\rho_s = \Pi\rho_{\text{in}}\Pi$ can be expanded as

$$\rho_s \frac{1}{|\mathcal{L}_2|}\sum_{v \in \mathcal{L}_2}(1-\epsilon)^{15-|v|}\epsilon^{|v|}|A_0^L\rangle\langle A_0^L|$$

$$\times + \frac{1}{|\mathcal{L}_2|}\sum_{v \in \mathcal{L}_2}\epsilon^{15-|v|}(1-\epsilon)^{|v|}|A_1^L\rangle\langle A_1^L|.$$

The distillation succeeds with probability

$$p_s = |\mathcal{L}_2|\text{Tr}\,\rho_s = \sum_{v \in \mathcal{L}_1^\perp}\epsilon^{15-|v|}(1-\epsilon)^{|v|}.$$

(The factor $|\mathcal{L}_2|$ reflects the number of possible values of μ, which all give rise to the same state ρ_s.)

To complete the distillation procedure, we need to apply a decoding transformation that would map the two-dimensional subspace $\mathcal{H}(0,0) \subset (\mathbb{C}^2)^{\otimes 15}$ onto the Hilbert space of one qubit. Recall that $\mathcal{H}(0,0) = \mathcal{G}(0,0)$ is the code subspace of the stabilizer code $\text{CSS}(\sigma^z, \mathcal{L}_2; \sigma^x, \mathcal{L}_1)$. Its logical Pauli operators can be chosen as

$$\hat{X} = (\sigma^x)^{\otimes 15}, \quad \hat{Y} = (\sigma^y)^{\otimes 15}, \quad \hat{Z} = -(\sigma^z)^{\otimes 15}.$$

It is easy to see that $\hat{X}, \hat{Y}, \hat{Z}$ obey the correct algebraic relations and preserve the code subspace. The decoding can be realized as a Clifford operator $V \in \mathcal{C}_{15}$ that maps $\hat{X}, \hat{Y}, \hat{Z}$ to the Pauli operators $\sigma^x, \sigma^y, \sigma^z$ acting on the first qubit. (The remaining 14 qubits become unentangled with the first one, so we can safely disregard them.) Let us show that the logical state $|A_0^L\rangle$ is transformed into $|A_0\rangle$ (up to some phase). For this, it suffices to check that $\langle A_0^L|\hat{X}|A_0^L\rangle = \langle A_0|\sigma^x|A_0\rangle$, $\langle A_0^L|\hat{Y}|A_0^L\rangle = \langle A_0|\sigma^y|A_0\rangle$, and $\langle A_0^L|\hat{Z}|A_0^L\rangle = \langle A_0|\sigma^z|A_0\rangle$. Verifying these identities becomes a straightforward task if we represent $|A_0^L\rangle$ in the standard basis:

$$|A_0^L\rangle = |\mathcal{L}_2|^{1/2}2^{-15/2}\sum_{u \in \mathcal{L}_2^\perp} e^{i(\pi/4)|u|}|u\rangle$$

$$= 2^{-5/2}\sum_{u \in \mathcal{L}_1}(|u\rangle + e^{-i(\pi/4)}|u + [1]\rangle).$$

To summarize, the distillation subroutine consists of the following steps.

(1) Measure eigenvalues of the Pauli operators $\sigma^z([x_j])$, $\sigma^z([x_j x_k])$ (for $j,k = 1,2,3,4$). The outcomes determine the σ^z syndrome, $\mu \in \mathcal{L}_2^*$.

(2) Find $w = w(\mu) \in \mathbb{F}_2^{15}$ such that $(w,v) = \mu(v)$ for any $v \in \mathcal{L}_2$.

(3) Apply the correcting operator $A(w)^\dagger$.

(4) Measure eigenvalues of the operators $\sigma^x([x_j])$. The outcomes determine the A syndrome, $\eta \in \mathcal{L}_1^*$.

(5) Declare failure if $\eta \neq 0$, otherwise proceed to the next step.

(6) Apply the decoding transformation, which takes the

code subspace to the Hilbert space of one qubit.

The subroutine succeeds with probability

$$p_s = \sum_{v \in \mathcal{L}_1^\perp} \epsilon^{15-|v|}(1-\epsilon)^{|v|}. \tag{31}$$

In the case of success, it produces the normalized output state

$$\rho_{\text{out}} = (1-\epsilon_{\text{out}})|A_0\rangle\langle A_0| + \epsilon_{\text{out}}|A_1\rangle\langle A_1| \tag{32}$$

characterized by the error probability

$$\epsilon_{\text{out}} = p_s^{-1} \sum_{v \in \mathcal{L}_2} \epsilon^{15-|v|}(1-\epsilon)^{|v|}. \tag{33}$$

The sums in Eqs. (31) and (33) are special forms of so-called weight enumerators. The *weight enumerator* of a subspace $\mathcal{L} \subseteq \mathbb{F}_2^n$ is a homogeneous polynomial of degree n in two variables, namely

$$W_{\mathcal{L}}(x,y) = \sum_{u \in \mathcal{L}} x^{n-|u|}y^{|u|}.$$

In this notation,

$$p_s = W_{\mathcal{L}_1^\perp}(\epsilon, 1-\epsilon), \quad \epsilon_{\text{out}} = \frac{W_{\mathcal{L}_2}(\epsilon,1-\epsilon)}{W_{\mathcal{L}_1^\perp}(\epsilon,1-\epsilon)}.$$

The MacWilliams identity [30] relates the weight enumerator of $\mathcal{L}$ to that of $\mathcal{L}^\perp$:

$$W_{\mathcal{L}}(x,y) = \frac{1}{|\mathcal{L}^\perp|} W_{\mathcal{L}^\perp}(x+y, x-y).$$

Applying this identity and taking into account that $\mathcal{L}_2^\perp = \mathcal{L}_1 \oplus [1]$ and that $|u| \equiv 0 (\text{mod } 2)$ for any $u \in \mathcal{L}_1$ (see Lemma 1), we get

$$p_s = \frac{1}{16} W_{\mathcal{L}_1}(1, 1-2\epsilon), \quad \epsilon_{\text{out}} = \frac{1}{2}\left(1 - \frac{W_{\mathcal{L}_1}(1-2\epsilon,1)}{W_{\mathcal{L}_1}(1,1-2\epsilon)}\right). \tag{34}$$

The weight enumerator of the subspace $\mathcal{L}_1$ is particularly simple:

$$W_{\mathcal{L}_1}(x,y) = x^{15} + 15x^7y^8.$$

Substituting this expression into Eq. (34), we arrive at the following formulas:

$$p_s = \frac{1 + 15(1-2\epsilon)^8}{16}, \tag{35}$$

$$\epsilon_{\text{out}} = \frac{1 - 15(1-2\epsilon)^7 + 15(1-2\epsilon)^8 - (1-2\epsilon)^{15}}{2[1 + 15(1-2\epsilon)^8]}. \tag{36}$$

The function $\epsilon_{\text{out}}(\epsilon)$ is plotted in Fig. 3. Solving the equation $\epsilon_{\text{out}}(\epsilon) = \epsilon$ numerically, we find the threshold error probability:

$$\epsilon_0 \approx 0.141. \tag{37}$$

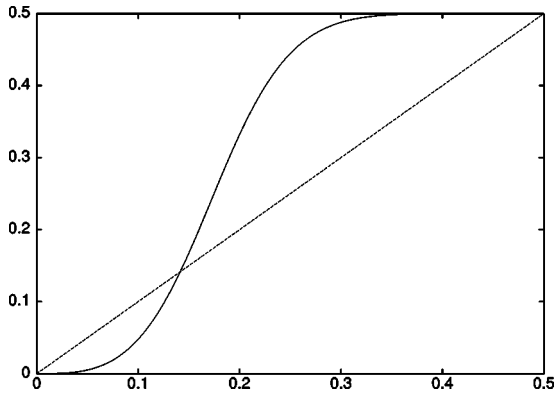

FIG. 3. The final error probability $\epsilon_{\text{out}}(\epsilon)$ for the H-type states distillation.

Let us examine the asymptotic properties of this scheme. For small ϵ the distillation subroutine succeeds with probability close to 1, therefore the yield is close to $1/15$. The output error probability is

$$\epsilon_{\text{out}} \approx 35\epsilon^3. \tag{38}$$

Now suppose that the subroutine is applied recursively. From n copies of the state ρ with a given ϵ, we distill one copy of the magic state $|A_0\rangle$ with the final error probability

$$\epsilon_{\text{out}}(n,\epsilon) \approx \frac{1}{\sqrt{35}}(\sqrt{35}\epsilon)^{3^k}, \quad 15^k \approx n,$$

where k is the number of recursion levels (here we neglect the fluctuations in the number of successful distillation attempts). Solving these equation, we obtain the relation

$$\epsilon_{\text{out}}(n,\epsilon) \sim (\sqrt{35}\epsilon)^{n^\xi}, \quad \xi = 1/\log_3 15 \approx 0.4. \tag{39}$$

It characterizes the efficiency of the distillation scheme.

VII. CONCLUSION AND SOME OPEN PROBLEMS

We have studied a simplified model of fault-tolerant quantum computation in which operations from the Clifford group are realized exactly, whereas decoherence occurs only during the preparation of nontrivial ancillary states. The model is fully characterized by a one-qubit density matrix ρ describing these states. It is shown that a good strategy for simulating universal quantum computation in this model is "magic states distillation." By constructing two particular distillation schemes we find a threshold polarization of ρ above which the simulation is possible.

The most exciting open problem is to understand the computational power of the model in the region of parameters $1 < |\rho_x| + |\rho_y| + |\rho_z| \leqslant 3/\sqrt{7}$ (which corresponds to $F_T^* < F_T(\rho) \leqslant F_T$, see Sec. I). In this region, the distillation scheme based on the five-quit code does not work, while the Gottesman-Knill theorem does not yet allow the classical simulation. One possibility is that a transition from classical to universal quantum behavior occurs on the octahedron boundary, $|\rho_x| + |\rho_y| + |\rho_z| = 1$.

To prove the existence of such a transition, one it suffices to construct a T-type states distillation scheme having the threshold fidelity F_T^*. A systematic way of constructing such schemes is to replace the five-qubit by a $GF(4)$-linear stabilizer code. A nice property of these codes is that the bitwise application of the operator T preserves the code subspace and acts on the encoded qubit as T, see Ref. [31] for more details. One can check that the error-correcting effect described in Sec. V takes place for an arbitrary GF(4)-linear stabilizer code, provided that the number of qubits is $n=6k-1$ for any integer k. Unfortunately, numerical simulations we performed for some codes with $n=11$ and $n=17$ indicate that the threshold fidelity increases as the number of qubits increases. So it may well be the case that the five-qubit code is the best GF(4)-linear code as far as the distillation is concerned.

From the experimental point of view, an exciting open problem is to design a physical system in which reliable storage of quantum information and its processing by Clifford group operations is possible. Since our simulation scheme tolerates strong decoherence on the ancilla preparation stage, such a system would be a good candidate for a practical quantum computer.

ACKNOWLEDGMENTS

We thank Mikhail Vyalyi for bringing to our attention many useful facts about the Clifford group. This work has been supported in part by the National Science Foundation under Grant No. EIA-0086038.

APPENDIX

The purpose of this section is to prove Eq. (15). Let us introduce this notation:

$$|\hat{T}_0\rangle = |T_{00000}\rangle \text{ and } |\hat{T}_1\rangle = |T_{11111}\rangle.$$

Consider the set $S_+(5)\subset S(5)$ consisting of all possible tensor products of the Pauli operators $\sigma^x,\sigma^y,\sigma^z$ on five qubits (clearly, $|S_+(5)|=4^5=|S(5)|/2$ since elements of $S(5)$ may have a plus or minus sign). For each $g\in S_+(5)$ let $|g|\in[0,5]$ be the number of qubits on which g acts nontrivially (e.g., $|\sigma^x\otimes\sigma^x\otimes\sigma^y\otimes I\otimes I|=3$). We have

$$|\hat{T}_0\rangle\langle\hat{T}_0| = \frac{1}{2^5}\sum_{g\in S_+(5)}\left(\frac{1}{\sqrt{3}}\right)^{|g|} g.$$

Now let us expand the formula (13) for the projector Π. Denote by $G\subset P(5)$ the Abelian group generated by the stabilizers S_1,S_2,S_3,S_4. It consists of 16 elements. Repeatedly conjugating the stabilizer S_1 by the operator $\hat{T}=T^{\otimes 5}$, we get three elements of G:

$$S_1 = \sigma^x\otimes\sigma^z\otimes\sigma^z\otimes\sigma^x\otimes I,$$

$$S_1S_3S_4 = \sigma^z\otimes\sigma^y\otimes\sigma^y\otimes\sigma^z\otimes I,$$

$$S_3S_4 = \sigma^y\otimes\sigma^x\otimes\sigma^x\otimes\sigma^y\otimes I.$$

Due to the cyclic symmetry mentioned in Sec. V, the 15 cyclic permutations of these elements also belong to G; together with the identity operator they exhaust the group G. Thus $G\subset S_+(5)$, and we have

$$\Pi = \frac{1}{16}\sum_{h\in G} h.$$

Taking into account that $\mathrm{Tr}(gh)=2^5\delta_{g,h}$ for any $g,h\in S_+(5)$, we get

$$\langle\hat{T}_0|\Pi|\hat{T}_0\rangle = \frac{1}{2^9}\sum_{h\in G}\sum_{g\in S_+(5)} 3^{-|g|/2}\mathrm{Tr}(gh) = \frac{1}{16}\sum_{g\in G} 3^{-|g|/2} = \frac{1}{6}.$$

Similar calculations show that $\langle\hat{T}_1|\Pi|\hat{T}_1\rangle=\frac{1}{6}$.

[1] E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).
[2] C. Zalka, e-print quant-ph/9612028.
[3] A. Steane, Phys. Rev. Lett. **78**, 2252 (1997).
[4] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[5] A. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[6] M. Freedman, M. Larsen, and Z. Wang, e-print quant-ph/0001108.
[7] M. Freedman, A. Kitaev, M. Larsen, and Z. Wang, Bull., New Ser., Am. Math. Soc. **40**, 31 (2002).
[8] C. Mochon, Phys. Rev. A **69**, 032306 (2004).
[9] G. Moore and N. Read, Nucl. Phys. B **360**, 362 (1991).
[10] C. Nayak and F. Wilczek, Nucl. Phys. B **479**, 529 (1996).
[11] B. Doucot and J. Vidal, Phys. Rev. Lett. **88**, 227005 (2001).
[12] M. Feigel'man and L. Ioffe, Phys. Rev. B **66**, 224503 (2002).
[13] J. Preskill, e-print quant-ph/9712048.
[14] D. Gottesman, Ph.D. thesis, Caltech, Pasadena, 1997, URL http://arxiv.org/abs/quant-ph/9705052.
[15] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[16] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[17] E. Knill, e-print quant-ph/0402171.
[18] E. Knill, e-print quant-ph/0404104.
[19] D. Gottesman and I. Chuang, Nature (London) **402**, 390 (1999).
[20] W. Dur and H. Briegel, Phys. Rev. Lett. **90**, 067901 (2003).
[21] D. Aharonov, e-print quant-ph/9602019.
[22] E. Dennis, Phys. Rev. A **63**, 052314 (2001).
[23] E. Knill, R. Laflamme, and W. Zurek, e-print quant-ph/9610011.

[24] A. Calderbank, E. Rains, P. Shor, and N. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[25] A. Ambainis and D. Gottesman, e-print quant-ph/0310097.
[26] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996).
[27] R. Laflamme, C. Miquel, J. Paz, and W. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[28] A. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996).
[29] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[30] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1981).
[31] A. Calderbank, E. Rains, P. Shor, and N. Sloane, e-print quant-ph/9608006.