Catalysis and activation of magic states in fault-tolerant architectures

Earl T. Campbell*

Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom,
and Institute of Physics and Astronomy, University of Potsdam, D-14476 Potsdam, Germany

(Received 20 December 2010; published 25 March 2011)

In many architectures for fault-tolerant quantum computing universality is achieved by a combination of Clifford group unitary operators and preparation of suitable nonstabilizer states, the so-called magic states. Universality is possible even for some fairly noisy nonstabilizer states, as distillation can convert many noisy copies into fewer purer magic states. Here we propose protocols that exploit multiple species of magic states in surprising ways. These protocols provide examples of previously unobserved phenomena that are analogous to catalysis and activation well known in entanglement theory.

DOI: 10.1103/PhysRevA.83.032317 PACS number(s): 03.67.Pp, 03.67.Lx

Quantum computers are capable of executing algorithms while tolerating modest rates of faults or errors. Stabilizer codes encode information in subspaces of larger Hilbert spaces and allow a proportion of errors to be actively detected and corrected [1], whereas some *anyonic* systems with topologically protected ground states provide a passive method of safely storing quantum information [2]. Research into anyonic systems has been stimulated by the recent discovery of alloys that are topological insulators [3,4], opening up a variety of readily available systems that may be suitable for anyonic quantum computing.

However, fault-tolerant quantum computing is not just about archiving quantum information, but also processing the information while stored in its protected form. However, by employing stabilizer codes and topological systems we restrict how the quantum information may be manipulated in a fault-tolerant way. Stabilizer codes only allow coherent implementation of a limited group of fault-tolerant gates, the so-called *transversal* gates. Unfortunately, recent research has shown that no stabilizer code can both protect against generic errors and offer a universal set of transversal gates [5]. Similarly, topologically protected groups of gates, implemented by braiding anyons, are not universal for many species of anyons [6–8]. Theoretically, some exotic anyons do offer universal topologically protected gates, but these are more physically speculative [9]. Consequently, an alternative route to universal and fault-tolerant quantum computing must be sought out.

This obstacle is overcome by gate injection techniques. A suitable resource state is identified, and through fault-tolerant gates and measurements, this resource is consumed in exchange for a new fault-tolerant unitary operator that promotes the group of gates to full universality. For both stabilizer codes and anyonic systems, the manifestly fault-tolerant gates are often contained within the Clifford group, the group of unitary operators that conjugate the Pauli operators. What resource states might promote the Clifford group to universality? Since the Clifford group maps stabilizer states—eigenstates of Pauli operators—to other stabilizer states, and such evolutions are efficiently classically simulable [10], we know that stabilizer states fail to provide universality. However, numerous nonstabilizer states *do* provide universality, including all single-qubit pure nonstabilizer states [11]. Bravyi and Kitaev proposed the appellation *magic* states for such resources [12]. In their seminal article, Bravyi and Kitaev showed that some mixed nonstabilizer states can enable universal quantum computing via a process of distillation into purer magic states. Since preparation of the raw resources is not fault tolerant, we expect them to be noisy, and so distillation is essential.

Some fault-tolerance schemes actually provide a proper subgroup of the Clifford group, such as when braiding Ising anyons [6–8]. Universality may still be possible via two levels of distillation if a resource state is available that first promotes the subgroup to the full Clifford group. For example, Bravyi [8] has shown that the aforementioned Ising anyon systems can be promoted to the full Clifford group by distilling certain noisy stabilizer resources.

The paradigm of magic states as a resource for promoting the Clifford group is analogous to other resource theories, such as how entanglement is a resource when only local operations are available [13] and how continuous variable Gaussian entangled states can be utilized provided with just local Gaussian operations [14]. In both these alternative examples of resource theories we have a thorough understanding of the fundamental principles behind what state transformations are possible. The role of magic states is not yet understood as comprehensively as entanglement, although lately several results have begun to illuminate the subject. Reichardt [11,15,16] provided several additional distillation protocols beyond those found by Bravyi and Kitaev. He also identified some multiqubit nonstabilizer states that cannot, even probabilistically, be reduced to a single-qubit nonstabilizer state [11]. Howard and van Dam [17,18] studied the role of noisy unitary operators as resources. They found that all depolarized single-qubit unitary operators that fall outside the Clifford group can enable universal quantum computing. Campbell and Browne [19,20] identified an analog to bound entanglement, with certain families of nonstabilizer states being undistillable for finite-sized computers. Ratanje and Virmani [21] considered resource theories that interpolate between separable states and stabilizer states and found new regimes that are efficiently classically simulable.

[*] earltcampbell@gmail.com

This article explores the fundamental principles that govern magic states, and we uncover several phenomena. Many of the phenomena have analogous, though subtly distinct, counterparts in entanglement theory, such as entanglement catalysis [22] and entanglement activation [23]. Previous work on magic states has focused on what is achievable with many copies of the same quantum state, whereas, all protocols presented here exploit two different sorts of resource in a counterintuitive manner.

Magic catalysis can be described as a scenario involving two agents: a "magic-state banker"; and an operator of a computer capable of only Clifford-group operations. The banker is willing to loan magic states to the operator, but requires that the operator returns *exactly* the same quantum state at a later time. We identify a protocol where the loaned magic state acts as a catalyst, enabling the operator to perform state transformations that would have been impossible otherwise. Our protocol counteracts the misleading but intuitive idea that resources must be consumed to serve a function.

Magic activation again involves a special resource, this time called the activator, that enables a probabilistic transformation that was impossible without this assistance. This phenomenon differs from catalysis in several key ways. The activator is not returned to a banker, and the transformation may succeed with nonunit probability. Furthermore, the probabilistic transformation also consumes a supply of bound magic states [19,20] that alone have limited computational power when in finite quantity.

Next we discuss the existence of the aforementioned computationally weak multiqubit states that were first identified by Reichardt [11], which we call *irreducible* nonstabilizer states. The defining feature of irreducible nonstabilizer states is that, on their own, no single-qubit nonstabilizer state can be extracted from one copy. We present examples of irreducible nonstabilizer states for any number of qubits above two. Next we introduce another new protocol that exploits a combination of irreducible nonstabilizer states and bound magic states. Despite both resources being of limited utility, we can, with some probability, extract a magic state of arbitrarily high fidelity. In many ways this protocol is more surprising than the previous magic-state activation protocol. However, this latter protocol relies on a large number of resources. Depending on your preferred definition of activation, this protocol may also qualify as such. However, we prefer to stress its unique aspects and so refer to it as an *asymptotic activation* protocol.

Combined, these results provide a significant step toward a complete understanding of the principles governing magic states and their manipulation. Our results also prompt several interesting open problems that we discuss in the final section.

I. TECHNICAL PREAMBLE

In this section we refine our terminology and define notation, beginning with a quick review of stabilizer states and the Clifford group. An n-qubit pure stabilizer state, $|\psi\rangle$, is a quantum state uniquely defined by n commuting, and independent, Pauli operators g_j. These operators generate by multiplication a group $\mathcal{S}$ of order 2^n, the so-called stabilizer group for $|\psi\rangle$. Every element of this group is said to stabilize the quantum state, such that $s|\psi\rangle = |\psi\rangle, \forall\, s \in \mathcal{S}$. More generally, a mixed state is a stabilizer state if and only if it is an incoherent mixture of pure stabilizer states. The Clifford group is the group of unitary operators that conjugate Pauli operators, such that for all Pauli operators p we have $CpC^\dagger = p'$. Equivalently, the Clifford group consists of the unitary operators that preserve the set of pure stabilizer states. Important single-qubit Clifford unitary operators are the H (Hadamard) and T gates, which are best described in terms of their action on Pauli operators:

$$\begin{aligned} HXH^\dagger = Z; \quad HZH^\dagger = X; \\ TXT^\dagger = Y; \quad TYT^\dagger = Z. \end{aligned} \tag{1}$$

All single-qubit Clifford unitary operators can be decomposed into some sequence of these gates; that is, they generate the single-qubit Clifford group. To generate the entire multiqubit Clifford group we have to add an entangling gate, such as the well-known control-not gate. For further information on stabilizer states and the Clifford group, we refer the reader to Refs. [1,24].

Throughout we refer to a Clifford computer as follows.

Definition 1. A *Clifford computer* is a device capable of performing ideal Clifford unitary operators, preparation of stabilizer states, classical feedforward, classical randomness, and Pauli measurements.

For transformations implemented on such a device, the following definition applies.

Definition 2. If a Clifford computer can take an input state ρ and deterministically output a state ρ', then we denote this as $\rho \rightarrow_D \rho'$, and say that ρ can be deterministically Clifford transformed to ρ'. Conversely, if there exists no such Clifford transform, we denote this as $\rho \not\rightarrow_D \rho'$.

More generally, transformations may be probabilistic, as follows.

Definition 3. If a Clifford computer can take an input state ρ and with nonzero probability output a state ρ', then we denote this as $\rho \rightarrow_P \rho'$, and say that ρ can be probabilistically Clifford transformed to ρ'. Conversely, if there exists no such probabilistic Clifford transform, we denote this as $\rho \not\rightarrow_P \rho'$.

The phenomena of catalysis and activation are essentially concerned with deterministic and probabilistic transformations, respectively.

The two most important single-qubit magic states are the eigenstates of the Clifford group unitary operators defined earlier, H and T, such that

$$\begin{aligned} H|H_0\rangle = |H_0\rangle; \quad H|H_1\rangle = -|H_1\rangle; \\ T|T_0\rangle = e^{i\pi/3}|T_0\rangle; \quad T|T_1\rangle = e^{-i\pi/3}|T_1\rangle. \end{aligned} \tag{2}$$

We also use similar notation for stabilizer states such as Y eigenstates $|Y_{0,1}\rangle$. For an n-qubit state a binary vector $\mathbf{v} = \{v_1, \ldots, v_n\}$ specifies the state

$$|H_{\mathbf{v}}\rangle = \bigotimes_{j=1}^{n} |H_{v_j}\rangle, \tag{3}$$

and similarly for $|T_{\mathbf{v}}\rangle$. Employing Greek characters for mixed density matrices, we use

$$\tau_{\mathbf{v}} = |T_{\mathbf{v}}\rangle\langle T_{\mathbf{v}}|, \tag{4}$$

with $\mathbf{v}$ again an n-bit vector.

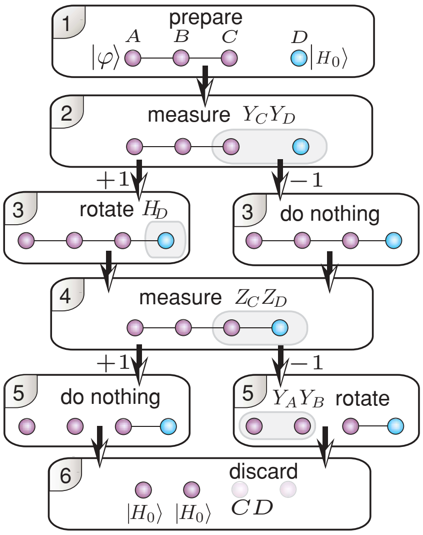

FIG. 1. (Color online) An outline of the magic catalysis protocol. Circles represent qubits, and lines between qubits denote correlations. The protocol involves two measurements with random outcomes. Although different measurement outcomes produce different projections, adaptively applied Clifford unitaries ensure the outcome is deterministic. However, the determinism of our protocol relies heavily on the symmetries of the initial states. The quantum states $|\varphi\rangle$ and $|H_0\rangle$ are defined in Theorem 1 and Eq. (2), respectively.

II. MAGIC CATALYSIS

Here we present an example of magic catalysis.

Theorem 1. Magic catalysis is possible: For the state $|\varphi\rangle \propto |H_{0,0,0}\rangle + |H_{1,1,1}\rangle$ we have $|\varphi\rangle \nrightarrow_D |H_0\rangle$ but with the addition of catalyst $|H_0\rangle$ we have $|\varphi\rangle|H_0\rangle \to_D |H_0\rangle|H_0\rangle$.

Clearly, this satisfies the constraints of the scenario described in the introduction since the process is deterministic and the catalyst is unchanged it can always be returned to the banker. First we describe a protocol, also illustrated in Fig. 1, that implements the deterministic transformation $|\varphi\rangle|H_0\rangle \to_D |H_0\rangle|H_0\rangle$:

(1) prepare the state $|\varphi\rangle$ on qubits A, B, and C and state $|H_0\rangle$ on qubit D;

(2) measure the Pauli stabilizer $Y_C Y_D$;

(3) if the measurement yields outcome $+1$, then apply the unitary operator H_D;

(4) measure the Pauli stabilizer $Z_C Z_D$;

(5) if the previous measure yields outcome -1, then apply the unitary operator $Y_A Y_B$;

(6) keep qubits A and B, and discard qubits C and D.

Although the process involves two measurements with random outcomes, each measurement is conditionally followed by a unitary operator that ensures the same output regardless of the measurement outcome. Consider step (3), after the $Y_C Y_D$ measurement with a $+1$ outcome, we have the state

$$\begin{aligned} H_D(\mathbb{1} + Y_C Y_D)|\varphi\rangle|H_0\rangle &= (\mathbb{1} - Y_C Y_D)|\varphi\rangle H_D|H_0\rangle, \\ &= (\mathbb{1} - Y_C Y_D)|\varphi\rangle|H_0\rangle, \end{aligned} \tag{5}$$

where the first line uses $H_j Y_j = -Y_j H_j$ and the second line uses $H|H_0\rangle = |H_0\rangle$. Hence, we can deterministically implement a projection onto the $-Y_C Y_D$ subspace.

Next, measurement results $-Z_C Z_D$ or $+Z_C Z_D$ give a projection of these qubits onto the state $|\Psi^-\rangle \propto |1,0\rangle - |0,1\rangle$ or $|\Phi^+\rangle \propto |0,0\rangle + |1,1\rangle$, respectively. The use of $|\Psi^-\rangle$ projections plays a pivotal role throughout this article, effectively functioning as an odd parity projector for any basis. That is, for any orthonormal basis $\{|b_0\rangle,|b_1\rangle\}$ shared between two qubits we have $|\langle\Psi^-|b_j,b_k\rangle| = (1-\delta_{j,k})/\sqrt{2}$, where $\delta_{j,k}$ is the Kronecker δ. This feature of the singlet projector follows from $(U \otimes U)|\Psi^-\rangle \propto |\Psi^-\rangle$ for any unitary operator U, and so $|\Psi^-\rangle$ is odd parity in any basis. Returning to the problem at hand, the relevant basis is the Hadamard basis, where $|\Psi^-\rangle \propto |H_{0,1}\rangle - |H_{1,0}\rangle$. Hence, the singlet projection picks out the second term of $|H_{0,0,0,0}\rangle + |H_{1,1,1,0}\rangle$, producing $|H_{1,1}\rangle|\Psi^-\rangle$. In accordance with step (5), we apply $Y_A Y_B$ (noting Y-gates flip Hadamard eigenstates) and discard the last two qubits. This yields the desired output $|H_{0,0}\rangle$.

If instead, step (4) provides a $+Z_C Z_D$ measurement outcome, we have a projection onto the state $|\Phi^+\rangle$, and so

$$\begin{aligned} \langle\Phi^+|_{C,D}|\varphi\rangle|H_0\rangle &\propto \langle\Psi^-|_{C,D}Y_D(|H_{0,0,0,0}\rangle + |H_{1,1,1,0}\rangle), \\ &\propto \langle\Psi^-|_{C,D}(|H_{0,0,0,1}\rangle + |H_{1,1,1,1}\rangle), \\ &\propto |H_{0,0}\rangle, \end{aligned}$$

where the first line uses $|\Phi^+\rangle \propto Y_D|\Psi^-\rangle$, allowing further employment of the singlet projector. Hence, we yield the desired output regardless of measurement outcomes.

To prove that we have identified a truly catalytic process, we must also show that the process was otherwise impossible, such that $|\varphi\rangle \nrightarrow_D |H_0\rangle$. We actually proceed by showing the stronger result that $|\varphi\rangle \nrightarrow_P |H_0\rangle$, which directly entails the weaker deterministic no-go result. Since we are attempting to probabilistically output a single-qubit state, we only have to consider Clifford transformations that project onto a stabilizer code space, with a single logical qubit, and then decode [19]. For a code space with logical states $|0_L\rangle$ and $|1_L\rangle$, the result of projecting and decoding performs the transformation

$$|\varphi\rangle \to |\psi_{\text{out}}\rangle \propto \langle 0_L|\varphi\rangle|0\rangle + \langle 1_L|\varphi\rangle|1\rangle. \tag{6}$$

For projections onto stabilizer subspaces, the ratio of the computational amplitudes,

$$R(|\psi_{\text{out}}\rangle) = |\langle 0_L|\varphi\rangle|^2/|\langle 1_L|\varphi\rangle|^2, \tag{7}$$

must be one of a few possible rational fractions (see Appendix A). However, for the target state, $|H_0\rangle$, this ratio is an irrational number $\tan^2(\pi/8) = 3 - 2\sqrt{2}$. Hence, the exact transformation is impossible, and our proof is complete.

The techniques in Appendix A are sufficiently general to rule out many other Clifford transformations. For example, if we ask whether n copies of $|\varphi\rangle$ can be exactly converted into a H state, our method also proves this is impossible with finite n, and so $|\varphi\rangle^{\otimes n} \nrightarrow_P |H_0\rangle$ (discussed further in Appendix B).

Describing catalysis in terms of an interaction between a magic-state banker and a computer operator gives it an operational flavor, although the scenario could be considered somewhat artificial. We feel that the true depth of catalysis is that certain transformations become possible, for *free*, assuming a reserve of magic states. Such transformations can be called *magic-assisted* Clifford group operations, and it is an interesting open problem to determine the full structure of these operations.

III. MAGIC ACTIVATION

Here we give an example of magic activation. One of the distinguishing features of activation is that it utilizes resources from a family of bound states. Rather than a general account of magic-state boundness, for brevity we describe the concept with respect to noisy T-magic states,

$$\tau(f) = f\tau_0 + (1-f)\tau_1, \tag{8}$$

where f is the fidelity and $f_{\mathrm{st}} = (1 + 1/\sqrt{3})/2$ is the threshold above which we have a nonstabilizer state. The following statement follows directly from the more general results of Ref. [20].

Theorem 2. For any finite n, there exists a positive $\epsilon_n > 0$, and a corresponding no-go region of fidelities $f \leqslant f_{\mathrm{st}} + \epsilon_n$. Inside this no-go region, it follows that for any single-qubit state, ρ, we have that $\tau(f)^{\otimes n} \rightarrow_P \rho$ if and only if $\tau(f) \rightarrow_P \rho$. We say that the family of states $\tau(f)$ is bound.

Heuristically, this result instructs us that there exist nonstabilizer states where n copies are no more useful than a single copy. Since this holds even with probabilistic postselection, we cannot distill these states to higher purity. There is clearly a parallel with bound entanglement, but there is also a subtle distinction. The threshold fidelity, $f_{\mathrm{st}} + \epsilon_n$, below which the theorem applies, depends on the number of copies, n. Hence, it is possible that the region shrinks as n is increased, maybe even such that $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$. In contrast, bound entangled states are bound regardless of how many copies we have. However, it is not known that the region actually does shrink. Rather, it is merely a limitation of the techniques of Ref. [20] that this possibility has not been ruled out. While known techniques [12] can distill noisy T states with fidelities greater than $(1 + \sqrt{3/7})/2$, there is no known method of distillation that functions below this fidelity. Hence, it is possible that even for large n the no-go region does not shrink below this level.

Subtleties aside, it is clear that $\tau(f)^{\otimes n}$, with sufficiently small fidelity and fixed n, cannot be distilled. This is in contrast with noisy H states, which are not a bound family of states. For example, consider noisy H states with *any* initial fidelity large enough that no stabilizer decomposition exists. With seven copies of such noisy H states one can implement a protocol [11,16] based on the STEANE code that, when successful, increases the fidelity.[1] The protocol must be iterated to achieve higher fidelities, and a unit fidelity is asymptotically approached with increasing n. However, the important feature is that *some* fidelity increase is always possible with finite copies, and that a similar protocol for all noisy T states is ruled out by Theorem 2. This prompts the question, *are very noisy T states ever useful resources?* We affirmatively answer this question by providing an activation protocol.

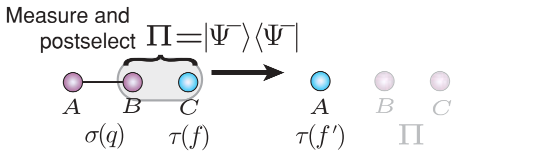

FIG. 2. (Color online) An outline of the magic-activation protocol which exploits the bound state $\tau(f)$ [see Eq. (8)] in the presence of its activator $\sigma(q)$ (defined in Theorem 2). This single-shot protocol succeeds probabilistically when qubits B and C are projected onto the singlet state.

Theorem 3. Magic activation is possible: For the activator $\sigma(q) = q\tau_{0,1} + (1-q)\tau_{1,0}$ (for some $1 > q > 1/2$) and any $\tau(f)$, with $f_{\mathrm{st}} < f$, there exists a single-qubit state ρ such that

(i) $\sigma(q) \otimes \tau(f) \rightarrow_P \rho$; even though
(ii) $\sigma(q) \not\rightarrow_P \rho$; and
(iii) $\tau(f) \not\rightarrow_P \rho$.

Alone, neither state can produce a particular output ρ, but combined it is possible. The output state is again a noisy T-magic state, so $\rho = \tau(f')$. Provided $f' > f$, condition (iii) of the theorem immediately follows.

We begin by describing the activation protocol, also illustrated in Fig. 2:

(1) Prepare state $\sigma(q)$ on qubits A and B and $\tau(f)$ on qubit C;
(2) measure the observables $Y_B Y_C$ and $Z_B Z_C$;
(3) postselect on -1 for both measurement outcomes, and discard qubits B and C.

The initial state can be expanded out as

$$\begin{aligned}\sigma(q) \otimes \tau(f) = {} & qf\tau_{0,1,0} + (1-q)f\tau_{1,0,0} \\ & + q(1-f)\tau_{0,1,1} + (1-q)(1-f)\tau_{1,0,1}.\end{aligned} \tag{9}$$

The postselected measurements project qubits B and C onto the singlet state. We use that $|\Psi^-\rangle \propto |T_{1,0}\rangle - |T_{0,1}\rangle$, and so

$$\langle\Psi^-|\sigma(q) \otimes \tau(f)|\Psi^-\rangle \propto qf\tau_0 + (1-q)(1-f)\tau_1. \tag{10}$$

We have effectively projected onto the odd parity terms of qubits B and C and then traced them out. After renormalization, the state is $\tau(f')$ with fidelity

$$f' = \frac{qf}{qf + (1-q)(1-f)}. \tag{11}$$

It is easy to see that $f' > f$ whenever $1 > q > 1/2$, and so the transformation could not be achieved with $\tau(f)$ alone, satisfying condition (iii). To complete the proof we must show condition (ii), that the transform could not be achieved with $\sigma(q)$ alone.

The simplest transformation on $\sigma(q)$ alone is to measure qubit A of $\sigma(q)$ in the computational basis. Due to the T symmetry of the state, any Pauli basis gives the same result. Hence, for a ±1 outcome of any single qubit Pauli measurement, the resulting unnormalized state is

$$\mathrm{tr}_A[(1 \pm Z_A)\sigma(q)] \propto qc_\pm\tau_1 + (1-q)(1-c_\pm)\tau_0, \tag{12}$$

where

$$c_\pm = \mathrm{tr}[(\mathbb{1} \pm Z_A)\tau_0]/2 = (1 \pm 1/\sqrt{3})/2. \tag{13}$$

[1] Note that STEANE code distillation only reduces noise polynomially rather than exponentially, and so alone the protocol is not efficient. However, overall efficiency can be achieved by using this protocol to reach a threshold fidelity and then switching to another protocol. For example, one may switch to implementing a protocol devised by Bravyi and Kitaev [12] that utilizes 15 qubits per attempt.

Clearly, the "+1" outcome gives a greater fidelity. Furthermore, we have $c_+ = f_{\mathrm{st}}$. Renormalizing gives a noisy T state with fidelity

$$f'' = \frac{q f_{\mathrm{st}}}{q f_{\mathrm{st}} + (1-q)(1-f_{\mathrm{st}})}. \tag{14}$$

This fidelity fails to match that achieved by our activation protocol. However, a single-qubit observable is clearly not the only option available, with many possible stabilizer measurements over both qubits. Checking other possible measurements (see Appendix C), one finds that the simple single-qubit measurement proves to be optimal. Therefore, a single copy of $\sigma(q)$ cannot be probabilistically Clifford transformed to $\rho(f')$, the output of the protocol, and so the activation is genuine. Of course, our argument does not rule out that many copies of $\sigma(q)$ may accomplish this transformation, as is indeed the case (see Appendix E). This feature is consistent with the analogous phenomena of activation in entanglement theory [23], as known entanglement activators are also many-copy distillable.

It is unclear whether more copies of the bound resource could be exploited to iterate or improve this particular magic-state activation protocol. However, the subsequent sections describe a more involved protocol that is stronger in two principle respects: First, it can be extended to consume arbitrarily many bound resources, with an output fidelity asymptotically approaching unity; second, the activating resources is also a computational weak state of a species that we introduce next.

IV. IRREDUCIBLE NONSTABILIZER STATES

This section introduces the notion of an irreducible nonstabilizer state, which is another form of noisy resource that is computationally weak. We also present some new examples of such states to be used in the next section.

Definition 4. A state σ is an **irreducible nonstabilizer state** (an INS state) if both

(1) σ is not a stabilizer state; and

(2) for all single-qubit nonstabilizer states, ρ, we have $\sigma \nrightarrow_P \rho$.

Reichardt identified the first examples of INS states [11]. However, Reichardt referred to them as *counterexample* states, as he presented them to disprove a conjecture that all multiqubit nonstabilizer states can be Clifford transformed to a single-qubit nonstabilizer state. Obviously, there are no single-qubit INS states, but Reichardt showed that two-qubit INS states do exist. Despite being of limited computational power, some INS states prove useful when combined with other resources. We consider states of the form

$$\sigma_{\mathrm{INS}}(q,n) = q\tau_0^{\otimes n} + (1-q)\mathbb{1}/2^n, \tag{15}$$

which satisfy the definition of an INS state whenever the weighting, q, falls in a specific interval, $q_{\mathrm{min}} < q \leqslant q_{\mathrm{max}}$, where

$$q_{\mathrm{max}} = [1 + (2f_{\mathrm{st}})^{n-1}(\sqrt{3}-1)]^{-1}, \tag{16}$$

$$q_{\mathrm{min}} = (2^n - 1)/[(1+\sqrt{3})^n - 1]. \tag{17}$$

Values of q and n satisfying these conditions are shown in Fig. 3.

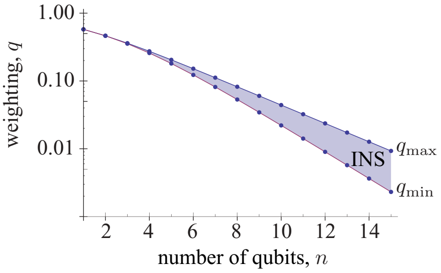

FIG. 3. (Color online) A region of INS states of the form $\sigma_{\mathrm{INS}}(q,n)$, as in Eq. (15). The weighting, q, is shown on a log-scale, against the number of qubits n. All states with the weighting satisfying $q_{\mathrm{min}} < q \leqslant q_{\mathrm{max}}$ are INS states, with the region being empty for $n = 1,2$ and appearing for $n \geqslant 3$. Some states outside the shaded region may also qualify as INS states.

First we show that for sufficiently pure states, we indeed have a nonstabilizer state, and so meet condition (1) of the definition. In general, mapping out the space of multiqubit mixed stabilizer states is an involved problem [11]. However, there exists a simple witness that can detect many nonstabilizer states. We introduce this witness in terms of a norm we call the stabilizer-norm (or just st-norm):

Lemma 1. A density matrix ρ, with decomposition in the Pauli basis $\rho = \sum_j a_j \sigma_j$, is a nonstabilizer state if

$$\|\rho\|_{\mathrm{st}} = \sum_j |a_j| > 1. \tag{18}$$

For single-qubit states the condition is not just sufficient, but also necessary. Indeed, for a single-qubit state this inequality marks out an octahderon in the Bloch sphere. However, there are many multiqubit nonstabilizer states that are not detected by this witness. To prove the lemma we first observe that the st-norm satisfies the triangle inequality and hence is convex. Furthermore, all pure stabilizer states, ρ_{st}, have unit st-norm, $\|\rho_{\mathrm{st}}\|_{\mathrm{st}} = 1$, and so no mixed stabilizer states can exceed unity.

For the states of interest here, the st-norm is

$$\|\sigma_{\mathrm{INS}}(q,n)\|_{\mathrm{st}} = q\left\|\tau_0^{\otimes n}\right\|_{\mathrm{st}} + (1-q)/2^n, \tag{19}$$

$$= q\left\|\tau_0\right\|_{\mathrm{st}}^n + (1-q)/2^n, \tag{20}$$

where the second line uses multiplicity of the st-norm with respect to the tensor product; in general, $\|\rho_a \otimes \rho_b\|_{\mathrm{st}} = \|\rho_a\|_{\mathrm{st}}\|\rho_b\|_{\mathrm{st}}$. Calculating $\|\tau_0\|_{\mathrm{st}} = (1+\sqrt{3})/2$, and requiring the st-norm exceed unity, entails $q > q_{\mathrm{min}}$.

Next we prove that for sufficiently impure states, condition (2) of our definition is satisfied. It is well known [19] that such a transformation is impossible if it cannot be achieved by projecting onto a stabilizer code space, with one logical qubit and decoding. First we note that all mixed single-qubit states with largest eigenvalue satisfying $\lambda \leqslant f_{\mathrm{st}}$ are stabilizer states. We prove that, for $q < q_{\mathrm{max}}$, all code space projections fail to achieve sufficient purity. Hence, they output stabilizer states. For a stabilizer code with projector Π, the projected state is

$$\rho_{\mathrm{out}} = \frac{q\Pi\tau_0^{\otimes n}\Pi + (1-q)\Pi/2^n}{q\,\mathrm{tr}\left(\Pi\tau_0^{\otimes n}\right) + (1-q)/2^{n-1}}. \tag{21}$$

The largest eigenvalue of the projected state is

$$\lambda = \frac{q\text{tr}\left(\Pi\tau_0^{\otimes n}\right) + (1-q)/2^n}{q\text{tr}\left(\Pi\tau_0^{\otimes n}\right) + (1-q)/2^{n-1}}. \tag{22}$$

To make further progress we must evaluate the maximum possible value of $\text{tr}(\Pi\tau_0^{\otimes n})$.

Lemma 2. For n copies of a single-qubit state, τ_0, and for all projectors, Π, onto a 2^m-dimensional stabilizer subspace, the maximum probability of projection is

$$\max_{\Pi}\left[\text{tr}\left(\Pi\tau_0^{\otimes n}\right)\right] = f_{\text{st}}^{n-m}. \tag{23}$$

This lemma asserts that the maximum probability of any stabilizer projection is achieved by a series of single-qubit stabilizer measurements. The lemma can be proven using graph codes [25] as shown in Appendix D. Applying the lemma (with $m = 1$) to Eq. (22) gives a maximum achievable value of λ, which we denote with a star:

$$\lambda^* = \frac{qf_{\text{st}}^{n-1} + (1-q)/2^n}{qf_{\text{st}}^{n-1} + (1-q)/2^{n-1}}. \tag{24}$$

If we wish to guarantee that the output is a stabilizer state, we require $\lambda^* \leqslant f_{\text{st}}$, and a little rearrangement produces the inequality $q \leqslant q_{\text{max}}$.

Hence, we have proven the existence of a whole class of INS states using a very different approach to Reichardt. Note that q_{min} and q_{max} differ only for three or more qubits, so our construction does not provide any two-qubit INS states.

V. ASYMPTOTIC MAGIC ACTIVATION

Another new protocol is described here, which demonstrates two features not exhibited by the previous activation protocol. First, it exploits a combination of an INS state and many bound magic states. Second, the output magic state can be arbitrarily pure, asymptotically approaching unit fidelity with the number of bound states used. In light of this, we distinguish this protocol by calling it *asymptotic activation*. For the purposes of this section, we consider the INS states with $q = q_{\text{max}}$, as in Eq. (19), and for brevity herein use the notation

$$\sigma_{\text{INS}}(n) = \sigma_{\text{INS}}(q_{\text{max}}, n). \tag{25}$$

Using this resource we have the following result.

Theorem 4. Asymptotic magic activation is possible: For the INS state $\sigma_{\text{INS}}(n)$ and any $\tau(f)^{\otimes n-1}$ (with $f > f_{\text{st}}$), we have that $\sigma_{\text{INS}}(n) \otimes \tau(f)^{\otimes n-1} \rightarrow_P \tau(f')$, where $f' \rightarrow 1$ as $n \rightarrow \infty$.

By definition, the INS state cannot be reduced to a single-qubit nonstabilizer state. Since the bound states also resist distillation, the protocol seems to exploit some synergy between the two resources. As with the previous activation protocol, we utilize singlet projection. The asymptotic activation protocol, also illustrated in Fig. 4, is as follows:

(1) Prepare $\sigma_{\text{INS}}(n)$ on qubits $A, B, \ldots,$ and prepare $\tau(f)^{\otimes n-1}$ on qubits $A', B', \ldots$;

(2) flip every qubit of $\tau(f)^{\otimes n-1}$ using the local Clifford HY that maps $\tau_0 \rightarrow \tau_1$;

(3) pair up $n-1$ qubits from each resource, pairing A with A' and B with B', etc.;

(4) measure the observables $X_j X_{j'}$ and $Z_j Z_{j'}$ for every pair;

(5) postselect on "-1" outcomes for every measurement outcome in every pair, and discard all measured qubits.

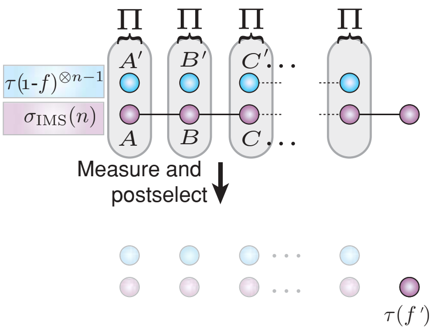

FIG. 4. (Color online) An outline of the asymptotic magic-activation protocol. The protocol uses $n-1$ copies of the noisy T states $\tau(f)$ [see Eq. (8)] and a specific n-qubit activator $\sigma_{\text{INS}}(q)$ [see Eq. (25)]. The activator is an especially weak resource, known as an irreducible nonstabilizer state (defined in Definition 4). The protocol pairs up each noisy T state with a qubit from the activator and succeeds when all $n-1$ pairs are projected onto the singlet state.

After step (2), the quantum state is

$$\begin{aligned}\rho &= q_{\text{max}}\tau_0^{\otimes n} \otimes \tau(1-f)^{\otimes n-1} \\ &\quad + (1-q_{\text{max}})\frac{\mathbb{1}}{2^n} \otimes \tau(1-f)^{\otimes n-1}.\end{aligned} \tag{26}$$

The subsequent steps project on the singlet state between paired-up qubits, giving

$$\rho \propto q_{\text{max}} a^{n-1}\tau_0 + (1-q_{\text{max}})b^{n-1}\tau_1, \tag{27}$$

where

$$\begin{aligned}a &= \langle\Psi^-|\tau_0 \otimes \tau(1-f)|\Psi^-\rangle = f/2, \\ b &= \langle\Psi^-|\mathbb{1} \otimes \tau(1-f)|\Psi^-\rangle/2 = 1/4.\end{aligned} \tag{28}$$

Combining these equations and after some manipulation, we find that the output fidelity is

$$f' = \left[1 + \left(\frac{f_{\text{st}}}{f}\right)^{n-1}(\sqrt{3}-1)\right]^{-1}. \tag{29}$$

Clearly, this approaches unity in the large n limit, provided that f exceeds the stabilizer threshold.

Unlike the previous activation protocol we are allowing for the number of copies to vary, with the phenomena becoming more pronounced in the large n limit. Since the number of copies is varying, and not fixed to some finite n, previous no-go results on the nondistillability of $\tau(f)^{\otimes n}$ do not apply. Consequently, we cannot guarantee that the transformation would be impossible without the addition of the INS state. As we have not strictly proven $\tau(f)^{\otimes n} \rightarrow_P \tau(f')$, we have exercised caution and not described this as a *vanilla* activation protocol. However, for small fidelities, $f < (1+\sqrt{3/7})/2$, there is no known protocol [12] that performs this transformation, even in the limit of many copies. The lesson this protocol teaches us is that large numbers of noisy T-states can be exploited to great effect when accompanied by another resource state. The most fundamental open problem in this research area is now whether asymptotically many nonstabilizer states can be purified when completely unassisted by activating resources.

VI. DISCUSSION AND CONCLUSIONS

We have introduced three protocols for quantum computers with Clifford-group unitary operators that are fault tolerant and, for clarity, taken to be ideal. All our protocols make use of two different species of nonstabilizer states, which is a relatively unstudied topic compared with that of distilling many identical copies of a quantum state. Each of the protocols is designed to illustrate a peculiar and counterintuitive phenomena that can occur in Clifford computers. We now review each of these protocols and discuss related open problems.

Magic catalysis demonstrates that reserves of magic states do not have to be depleted to serve a function. A magic state can act as a catalyst that enables a deterministic transformation that is impossible by Clifford transformations alone. In our catalytic protocol, the catalyst was a Hadamard eigenstate, and the protocol depended on some very specific symmetries of this state. This prompts the question of whether other nonstabilizer states can serve as catalysts. For example, can eigenstates of the T gate also act as catalysts? We conjecture that—in light of deep underlying differences between H and T states—the answer will be no. The T magic states are weaker in several regards. First, existing proposals for implementing non-Clifford gates do not directly exploit T states. Rather the T states are probabilistically converted into states on the Bloch sphere equator (see Ref. [12] or Appendix C), and only then are they used for implementing a non-Clifford gate. Second, noisy T states just outside the set of stabilizer states are undistillable, or bound, in the sense reviewed earlier. Beyond this anecdotal evidence, we have no firm proof that T states cannot function as catalysts. However, settling the conjecture either way should prove illuminating.

No protocol, prior to this article, has exploited noisy T states arbitrarily close to the set of stabilizer states. Indeed, the evidence surveyed in the previous paragraph suggests that there exist noisy T states, which despite being nonstabilizer states, cannot be utilized for any useful task. However, our magic-activation protocol shows that a noisy T state combined with an activator resource can probabilistically output a single-qubit state that could not be achieved with either resource alone. Hence, all noisy T states outside the set of stabilizer states are useful for *some* task. Since all noisy H nonstabilizer states are already known to be useful without the assistance of an activator, it is somewhat redundant to ask whether activation could be performed with H states.[2] A dissimilarity with entanglement activation is that our magic-activation protocol is not iterative, being defined for only a single round. The most interesting questions on this topic concern what kinds of iteration are possible. Our third and final protocol, asymptotic activation, gives one possible extension.

Asymptotic activation shows that $(n-1)$ copies of any noisy T state and a particular n-qubit resource can probabilistically output a magic state, which in the asymptotic limit approaches unit fidelity. Furthermore, the special n-qubit resource is an irreducible nonstabilizer state, from which no single-qubit nonstabilizer states can be probabilistically extracted. The class of irreducible nonstabilizer states is interesting in it own right, so our methods for constructing them may find applications elsewhere. Indeed, one interesting problem is whether many copies of irreducible nonstabilizer states are distillable or a new form of bound state.

Neither asymptotic activation nor standard activation are analogous to entanglement activation in every respect. For example, in the entanglement activation of Ref. [23] the protocol simultaneously exhibits the following three features:

(1) The protocol can consume a variable number, $n-1$, copies of the bound resource with the output fidelity tending toward unity with increasing n;

(2) the activating resource has a fixed size;

(3) it is proven that neither the bound resources nor the activating resource can on their own be probabilistically transformed to the output of the activation protocol.

Asymptotic activation has property (1), standard activation satisfies (2) and (3), but neither magic protocols simultaneously exhibit all three features. This prompts the following question: *Do magic protocols exist that are more sturdy analogs of entanglement activation with all three features*? The extent of symmetries between the two resource theories is far from clear, and hence so is the answer to our posited problem.

Considering all our protocols together, a key tool in all is the use of a singlet projection along with at least one state with multiqubit correlations. The singlet projector functions as a method of verifying if two qubits are nonidentical, although at the price of projecting those qubits into a stabilizer state. Since our aim is to prepare nonstabilizer states, singlet projections can only be exploited when accompanied by multiqubit correlations. Indeed, we have seen that singlet projection is an extremely useful tool in this context. So far we have not considered any scenarios with many copies of a multiqubit correlated state, but it seems plausible that the singlet projection would prove useful in such contexts. This is indeed the case, and for completeness we provide just such a strategy in Appendix E.

ACKNOWLEDGMENTS

We would like to thank Hussain Anwar for comments on the manuscript and conversations on this topic and Dan Browne, Niel de Beaudrap, and Matty Hoban for interesting discussions concerning magic states and Clifford computers. This research was supported by the Royal Commission for the Exhibition of 1851 and the EU integrated project Q-ESSENCE.

APPENDIX A

Here we show that the ratio of amplitudes in Eq. (7) can only take rational values, and hence cannot achieve the required irrational number. Furthermore, the set of possible ratios is finite, so there is a limit to how closely the target ratio can be approximated. We present a very general form of the proof, which can be used to rule out many other Clifford transformations. The techniques introduced here indicate that

[2] This is true although it is straightforward to check that a Hadamard analog of the activation protocol does work.

there may well be hope for building a general framework for understanding catalysis.

Before beginning the core proof, we make some observations. The specific initial state of interest, $|\varphi\rangle$, is Clifford equivalent to

$$|\varphi'\rangle = (|0,0,0\rangle + i|0,1,1\rangle + i|1,0,1\rangle + i|1,1,0\rangle)/2. \quad \text{(A1)}$$

The required Clifford is simply $\sqrt{X}^{\otimes 3}$, which maps the Hadamard eigenstates to the Bloch sphere equator such that

$$\sqrt{X}|H_j\rangle = |H_j'\rangle = (|0\rangle + (-1)^j e^{i\pi/4}|1\rangle)/\sqrt{2}. \quad \text{(A2)}$$

Hence, an equal superposition of $|H'_{0,0,0}\rangle$ and $|H'_{1,1,1}\rangle$ cancels out odd excitation terms, leaving only the even terms shown in Eq. (A1). Next we recall that stabilizer states must have the form [26]

$$|\psi_{\text{st}}\rangle = \sum_{\mathbf{x}\in C+\mathbf{y}} i^{l(\mathbf{x})}(-1)^{q(\mathbf{x})}|\mathbf{x}+\mathbf{y}\rangle/\sqrt{|C|}, \quad \text{(A3)}$$

where $l(\mathbf{x})$ and $q(\mathbf{x})$ are some linear and quadratic functions in $\mathbf{x}$, C is a binary linear subspace and $\mathbf{y}$ is some constant binary vector. Notice that our state $|\varphi'\rangle$ has a very similar form to stabilizer states as in the computational basis the coefficient have equal magnitude and phases are multiplies of i. Such states are interesting and deserving of their own title.

Definition 5. We say a pure quantum state, $|\psi\rangle$, is a *pseudostabilizer* state if and only if there exists a Clifford unitary U such that

$$U|\psi\rangle = \left(\sum_{\mathbf{x}\in\mathcal{P}} i^{f(\mathbf{x})}|\mathbf{x}\rangle\right)/\sqrt{|\mathcal{P}|}, \quad \text{(A4)}$$

where $\mathcal{P}$ is a set of n-qubit bit strings, and $f:\mathbf{x}\to\{0,1\}$. Furthermore, we say a pseudostabilizer state has complexity P, such that

$$P(|\psi\rangle) = \min\left\{|\mathcal{P}| \,\middle|\, U|\psi\rangle = \sum_{\mathbf{x}\in\mathcal{P}} \frac{i^{f(\mathbf{x})}|\mathbf{x}\rangle}{\sqrt{|\mathcal{P}|}}; \forall\, U\in\mathcal{C}\right\}. \quad \text{(A5)}$$

This is simply the smallest possible $|\mathcal{P}|$ over all valid decompositions.

Notice that genuine stabilizer states also satisfy this definition but have trivial complexity $P=1$, and the decomposition of Eq. (A1) entails that $P(|\varphi'\rangle)\leqslant 4$. In contrast the H states are not pseudostabilizer states as defined above.

Here we prove that the complexity of a pseudostabilizer state limits the possible single-qubit states one can produce by Clifford transformations.

Theorem 5. Consider a pseudostabilizer state $|\psi\rangle$ of complexity P. If $|\psi\rangle \to_P |\psi_{\text{out}}\rangle$, where $|\psi_{\text{out}}\rangle$ is a pure single-qubit state, then it follows that the amplitude ratio satisfies

$$R(|\psi_{\text{out}}\rangle) = \frac{|\langle 0|\psi_{\text{out}}\rangle|^2}{|\langle 1|\psi_{\text{out}}\rangle|^2} \in R_p, \quad \text{(A6)}$$

where R_P is the set of feasible ratios

$$R_P = \left\{\frac{a_0^2+b_0^2}{a_1^2+b_1^2} \,\middle|\, a_j,b_j\in\mathbb{Z}; |a_j|+|b_j|\leqslant P\right\}. \quad \text{(A7)}$$

Conversely, for any $|\psi'\rangle$ with $R(|\psi'\rangle)\notin R_P$ we can conclude $|\psi\rangle \not\to_P |\psi'\rangle$.

Notice that all of the feasible ratios from a pseudostabilizer state are rational fractions, so exactly producing a H state is impossible. The specific result $|\varphi\rangle \not\to_P |H_0\rangle$ then follows from our earlier observation that $|\varphi\rangle$ is a pseudostabilizer state of bounded complexity $P(|\varphi\rangle)\leqslant 4$.

As noted in the main text, we only have to consider probabilistic Clifford transforms that project onto a single-qubit stabilizer subspace and then decode, and so we can achieve

$$R(|\psi_{\text{out}}\rangle) = |\langle 0_L|\psi\rangle|^2/|\langle 1_L|\psi\rangle|^2, \quad \text{(A8)}$$

where $|0_L\rangle$ and $|1_L\rangle$ are logical states of the stabilizer subspace, which by Eq. (A3) can be expressed as

$$|0,1_L\rangle = \sum_{\mathbf{x}\in C_{0,1}+\mathbf{y_{0,1}}} \frac{i^{l_{0,1}(\mathbf{x})}(-1)^{q_{0,1}(\mathbf{x})}|\mathbf{x}\rangle}{\sqrt{|C_{0,1}|}}, \quad \text{(A9)}$$

with the numeric subscripts differentiating $(C,\mathbf{y},q,l)$ for the two states. It is well known that logical states of stabilizer codes can always be found such that they differ by Pauli rotations, such that $|1_L\rangle = X_L|0_L\rangle$. Pauli operators can change $\mathbf{y}$, l, and q, but not C and so $C_0 = C_1 = C$.

Using Eqs. (A4) and (A9) we find that

$$\langle 0,1_L|\psi'\rangle = \sum_{\mathbf{x}\in\mathcal{P}\cap(C+\mathbf{y_{0,1}})} \frac{i^{l_{0,1}(\mathbf{x})+f(\mathbf{x})}(-1)^{q_{0,1}(\mathbf{x})}}{\sqrt{|C\|\mathcal{P}|}}, \quad \text{(A10)}$$

each term in the summation is a multiple of i and there are no more than $P(|\psi'\rangle) = |\mathcal{P}|$ terms. Hence, we have

$$\langle 0,1_L|\psi'\rangle = (a_{0,1}+ib_{0,1})/\sqrt{|C\|\mathcal{P}|}, \quad \text{(A11)}$$

where $a_j,b_j\in\mathbb{Z}$ and the limited number of terms entails $|a_j|+|b_j|\leqslant P(|\psi'\rangle)$. Calculating the ratio of these amplitudes, the $|C\|\mathcal{P}|$ factors cancel and we have the result as stated in Theorem 5.

From an infinite set of rational numbers, one can always find an arbitrarily good approximation to any irrational. However, the set of feasible ratios is limited by the constraints $|a_j|+|b_j|\leqslant P(|\psi\rangle)$ and and so the set of possibilities is not just finite but potentially very small. We have presented an argument based on rationality for generality. However, it is quite straightforward to numerically search the limited set of possibilities and verify that for $P(|\varphi\rangle)=4$ we can never achieve $R=\tan(\pi/8)^2$. Such a search produces 1/5 as the closest possibility, which differs from the target by over 0.028. Note that Theorem 5 places a restriction on feasible ratios, but does not guarantee that all such ratios are achievable.

The theorem deduced here rules out many Clifford transforms, but is far from the generality of the majorization criteria that is used in entanglement theory [22]. In entanglement theory, the majorization criteria depend on the coefficients of the quantum state in the Schmidt basis. If we consider all possible *local* unitaries and rotate a state to have the minimal possible support in the computational basis then this also yields the all important Schmidt coefficients. Returning to the context of magic states, our approach hints that minimizing support over all possible *Clifford* unitaries also gives a decomposition with important coefficients. Our investigations into this approach are ongoing.

APPENDIX B

Here we briefly address the question of whether many copies of $|\varphi\rangle$ can be probabilistically Clifford transformed into $|H_0\rangle$. Much of the technical apparatus required was established in Appendix A. Given that $|\varphi\rangle$ is a pseudostabilizer state with complexity $P(|\varphi\rangle) \leqslant 4$, it follows that $|\varphi\rangle^{\otimes n}$ is also a pseudostabilizer state but with $P(|\varphi\rangle^{\otimes n}) \leqslant 4^n$. Hence, for finite n, Theorem 5 applies and we can conclude $|\varphi\rangle^{\otimes n} \not\to_P |H_0\rangle$. However, a supply of $|\varphi\rangle$ states is a resource for universal quantum computation. This paradox is resolved by observing that although an exact $|H_0\rangle$ is impossible to produce, we may approximate $|H_0\rangle$ with a fidelity that asymptotically approaches unity as n increases. Similarly, in entanglement theory many copies of any pure entangled state may be converted into any other state in the asymptotic limit.

APPENDIX C

We consider two qubit stabilizer measurements on the state $\sigma(q)$, defined in Theorem 3, which is an incoherent mixture of $|T_{0,1}\rangle$ and $|T_{1,0}\rangle$. We shall exploit that the state is invariant under T rotations of either qubit A or qubit B, such that

$$T_A^a T_B^b \sigma(q) \big(T_A^a T_B^b\big)^\dagger = \sigma(q) \tag{C1}$$

for any integers a and b. Furthermore, for any Pauli operator $P_A P_B$, where $P_{A,B} = \{X_{A,B}, Y_{A,B}, Z_{A,B}\}$, there exists integers a and b such that

$$T_A^a T_B^b P_A P_B \big(T_A^a T_B^b\big)^\dagger = Z_A Z_B. \tag{C2}$$

Combing these two properties of the T rotation, we have that for any two-qubit Pauli projection

$$\begin{aligned} T_A^a T_B^b (\mathbb{1} \pm P_A P_B)\sigma(q)(\mathbb{1} \pm P_A P_B)\big(T_A^a T_B^b\big)^\dagger \\ = (\mathbb{1} \pm Z_A Z_B)\sigma(q)(\mathbb{1} \pm Z_A Z_B). \end{aligned} \tag{C3}$$

This symmetry entails that we only have to consider two possible Pauli projections, $\Pi_\pm = (\mathbb{1} \pm Z_A Z_B)/2$. As an intermediate step in our proof, we see that when the state is pure, $q = 1$, two T states can be probabilistically converted into a pure state on the Bloch sphere equator. This equatorization is an important step in using these resources for implementing non-Clifford gates.

First, we note that T states in the computational basis are

$$\begin{aligned} |T_0\rangle &= \cos(\beta)|0\rangle + e^{i\pi/4}\sin(\beta)|1\rangle, \\ |T_1\rangle &= \sin(\beta)|0\rangle - e^{i\pi/4}\cos(\beta)|1\rangle, \end{aligned} \tag{C4}$$

where $\cos(2\beta) = 1/\sqrt{3}$. If we consider the Π_+ projection onto the even parity subspace, then

$$\Pi_+|T_{0,1}\rangle = \Pi_+|T_{1,0}\rangle = \cos(\beta)\sin(\beta)(|0,0\rangle - i|1,1\rangle). \tag{C5}$$

Since either pure state is projected onto the same stabilizer state, so too is the mixture $\sigma(q)$.

For the odd parity projector, Π_-, the analysis is more involved as

$$\begin{aligned} \Pi_-|T_{0,1}\rangle &= e^{i\pi/4}[\sin^2(\beta)|1,0\rangle - \cos^2(\beta)|0,1\rangle], \\ \Pi_-|T_{1,0}\rangle &= e^{i\pi/4}[\sin^2(\beta)|0,1\rangle - \cos^2(\beta)|1,0\rangle], \end{aligned}$$

which are distinct nonstabilizer states. Using the decoding $|0,1\rangle \to |-\rangle$ and $|1,0\rangle \to -i|+\rangle$, these states map to points on Bloch sphere equator,

$$\begin{aligned} \Pi_-|T_{0,1}\rangle &\to |\gamma_+\rangle = (|0\rangle + e^{i\gamma}|1\rangle)/\sqrt{2}, \\ \Pi_-|T_{1,0}\rangle &\to |\gamma_-\rangle = (|0\rangle + e^{-i\gamma}|1\rangle)/\sqrt{2}, \end{aligned}$$

where $\gamma = \pi/6$. Since $|\gamma_+\rangle$ is in the positive octant of the Bloch sphere, no other decoding gets closer to the target $|T_0\rangle$ state. Applying this analysis to the projection of the initial mixed state gives

$$\Pi_-\sigma(q)\Pi_- \to q|\gamma_+\rangle\langle\gamma_+| + (1-q)|\gamma_-\rangle\langle\gamma_-|. \tag{C6}$$

The fidelity of this output with respect to $|T_0\rangle$ is

$$f''' = q|\langle T_0|\gamma_+\rangle|^2 + (1-q)|\langle T_0|\gamma_-\rangle|^2, \tag{C7}$$

where,

$$|\langle T_0|\gamma_\pm\rangle|^2 = (9 \pm \sqrt{3})/12. \tag{C8}$$

Comparing the fidelity f''' with f'' of Eq. (14), we find that f''' is always smaller. Hence, no two qubit stabilizer projections can outperform the single-qubit projection.

APPENDIX D

This appendix provides a proof of Lemma 2, which gives the maximum probability of projection onto a 2^m-dimensional stabilizer subspace. All stabilizer subspaces are local-Clifford equivalent to a linear graph code [25], such that

$$\Pi = C_{\text{loc}} \Pi_G C_{\text{loc}}^\dagger. \tag{D1}$$

Our proof utilizes this local equivalence, so first we give a brief account of graph codes and their relevant features. A graph code is defined by a graph G and a m-dimensional linear code $\mathcal{C}$ over $\mathbb{Z}_2$. We use $|G\rangle$ to denote the graph state corresponding to graph G, which has stabilizer generators

$$k_j = X_j \bigotimes_{k \in N(j)} Z_k, \tag{D2}$$

where $N(j)$ denotes the set of vertices in the graph connected to vertex j. The subspace for the graph code is spanned by orthogonal graph states

$$|G_{\mathbf{c}}\rangle = Z_{\mathbf{c}}|G\rangle, \tag{D3}$$

where $\mathbf{c}$ represents binary vectors in the code $\mathcal{C}$, and $Z_{\mathbf{c}} = \bigotimes Z_j^{c_j}$. The projector onto the graph code subspace is then

$$\Pi_G = \sum_{\mathbf{c} \in \mathcal{C}} |G_{\mathbf{c}}\rangle\langle G_{\mathbf{c}}|. \tag{D4}$$

For our purposes we need to express this projector in terms of the graph code stabilizer $\mathcal{S}$

$$\Pi_G = \frac{1}{2^{n-m}} \sum_{s \in \mathcal{S}} s. \tag{D5}$$

The stabilizer of the graph code is

$$\mathcal{S} \equiv \left\{ s_{\mathbf{y}} = \prod_j k_j^{y_j} | \mathbf{y} \in \mathcal{C}^\perp \right\}, \tag{D6}$$

where $\mathcal{C}^{\perp}$ is the dual of $\mathcal{C}$. Allowing for local Clifford unitary operators, the stabilizer of the graph code is $\mathcal{S}' = C_{\rm loc}\mathcal{S}C_{\rm loc}^{\dagger}$, and so the actual projector is

$$\Pi = \frac{1}{2^{n-m}} \sum_{s' \in \mathcal{S}'} s'. \tag{D7}$$

In our proof we use the following fact: The stabilizers of $\mathcal{S}'$ have the same weights as the those in the locally equivalent graph code stabilizer, $\mathcal{S}$. That is, if $w(s)$ is the weight of s (the number of nonidentity Pauli operators), then $w(s') = w(C_{\rm loc} s C_{\rm loc}^{\dagger}) = w(s)$, which holds because local Cliffords conjugate Pauli operators without changing their weight. We use this fact in combination with other features of graph codes.

As for the relevant quantum state, this also has a Pauli decomposition. Using that a single T-magic state is

$$\tau_0 = \frac{1}{2}\left(1 + \frac{X+Y+Z}{\sqrt{3}}\right), \tag{D8}$$

it follows that n copies may be represented as

$$\tau_0^{\otimes n} = \frac{1}{2^n} \sum_{g \in \mathcal{G}} g \left(\frac{1}{\sqrt{3}}\right)^{w(g)}, \tag{D9}$$

where $\mathcal{G}$ is the set of Pauli operators with positive phase. Hence, the projection probability is

$$\begin{aligned}\frac{\mathrm{tr}(\Pi\tau_0^{\otimes n})}{2^{m-2n}} &= \mathrm{tr}\left[\sum_{s' \in \mathcal{S}', g \in \mathcal{G}} s' g \left(\frac{1}{\sqrt{3}}\right)^{w(g)}\right], \\ &= \sum_{s' \in \mathcal{S}', g \in \mathcal{G}} \mathrm{tr}(s' g) \left(\frac{1}{\sqrt{3}}\right)^{w(g)}. \end{aligned} \tag{D10}$$

The trace vanishes except when $gs' = \pm\mathbb{1}$, and so

$$\frac{\mathrm{tr}\big(\Pi\tau_0^{\otimes n}\big)}{2^{m-n}} = \sum_{s' \in \mathcal{S}'} \mathrm{sgn}(s') \left(\frac{1}{\sqrt{3}}\right)^{w(s')}, \tag{D11}$$

where $\mathrm{sgn}(s')$ is ± 1, matching the phase of s'. Clearly, an upper bound is established when all signs are positive, and hence,

$$\frac{\mathrm{tr}\big(\Pi\tau_0^{\otimes n}\big)}{2^{m-n}} \leqslant \sum_{s' \in \mathcal{S}'} \left(\frac{1}{\sqrt{3}}\right)^{w(s')}. \tag{D12}$$

Having arrived at an inequality purely dependent on the weights of $\mathcal{S}'$, we can use $w(s') = w(s)$ to switch to the locally equivalent graph code. To determine the graph code weights $w(s)$ we use the decomposition in terms of canonical generators expressed in Eq. (D6), where every $s_{\mathbf{y}}$ is identified with a binary vector $\mathbf{y} \in \mathcal{C}^{\perp}$,

$$w(s_{\mathbf{y}}) = w\left(\prod_j k_j^{y_j}\right). \tag{D13}$$

When multiplying generators together the X_j contributions can change into $\pm Y_j$, but never reduce in weight. Hence,

$$w(s_{\mathbf{y}}) \geqslant w(\mathbf{y}), \tag{D14}$$

where the right-hand side is the weight, number of 1 entries, in the bit string $\mathbf{y}$. Combining this result with Eq. (D12), we have

$$\frac{\mathrm{tr}\big(\Pi\tau_0^{\otimes n}\big)}{2^{m-n}} \leqslant \sum_{\mathbf{y} \in \mathcal{C}^{\perp}} \left(\frac{1}{\sqrt{3}}\right)^{w(\mathbf{y})}. \tag{D15}$$

This inequality now depends solely on the classical linear code $\mathcal{C}^{\perp}$. All such linear codes can, up to relabeling of bits, be diagonalized such that the generator matrix, M, has an identity over the first $n-m$ elements, such that $M = [\mathbb{1}_{n-m}, M']$. Dividing the bit strings into two halves $\mathbf{y} = (\mathbf{y}', \mathbf{y}'') = (y_1', \ldots, y_{n-m}', y_1'', \ldots, y_m'')$, then the elements of $\mathbf{y}'$ are fixed by diagonlization of the generator matrix. Furthermore, since $w(\mathbf{y}) = w(\mathbf{y}') + w(\mathbf{y}'')$, we can conclude

$$\mathrm{tr}\big(\Pi\tau_0^{\otimes n}\big) \leqslant 2^{m-n} \sum_{\mathbf{y} \in \{0,1\}^{n-m}} \left(\frac{1}{\sqrt{3}}\right)^{w(\mathbf{y}')+w(\mathbf{y}'')}, \tag{D16}$$

The weights of $w(\mathbf{y}')$ are fixed by diagonalization, but $w(\mathbf{y}'')$ depends on features of the code. We are interested in an upper bound, maximized over all possible projectors Π, which can be achieved when $w(\mathbf{y}'') = 0$, and so

$$\begin{aligned}\max_{\Pi}\left[\mathrm{tr}\big(\Pi\tau_0^{\otimes n}\big)\right] &\leqslant 2^{m-n} \sum_{\mathbf{y} \in \{0,1\}^{n-m}} \left(\frac{1}{\sqrt{3}}\right)^{w(\mathbf{y}')}, \\ &= 2^{m-n}\left(1 + \frac{1}{\sqrt{3}}\right)^{n-m} = f_{\rm st}^{n-m}. \end{aligned} \tag{D17}$$

This gives an upper bound, but it is easy to verify that it is saturated by measuring m qubits in the computational basis and postselecting on "+1" outcomes.

APPENDIX E

In our magic-activation protocol we saw that $\sigma(q)$ states (defined in Theorem 3) can be a powerful resource for activation of bound families of states. This suggests that they may be a powerful resource in their own right and that the ability to prepare many copies of them may enable universal quantum computation. This is the problem we address here, although for a more general class of states. We consider states of the form

$$\sigma(q,r) = q\tau_{1,0} + (1-q-2r)\tau_{0,1} + r(\tau_{0,0} + \tau_{1,1}), \tag{E1}$$

Before continuing let us reflect on some properties of these states. First, states in this class are always separable. Second, they are correlated states except for specific values $r = \sqrt{q}(1-\sqrt{q})$, which give a product state. Although this class of states is not completely general, any state can, by a suitable twirling procedure (see Appendix F), be brought into this form.

We now outline a protocol for exploiting many copies of these correlated states, where the maximum achievable fidelity approaches 1 as $r \rightarrow 0$. Since the protocol consists of a chain of projections, we refer to the protocol as the *daisy-chain* protocol:

(1) Prepare n copies of the state $\sigma(q,r)$, with the first pair as qubits A and B, pair 2 as qubits C and D, and so on;

(2) measure qubit A in the computational basis, and postselect on a "+1" outcome;

(3) for qubits B and C, measure $X_B X_C$ and $Z_B Z_C$ and postselect on "-1" outcomes for both;

(4) perform the preceding step for qubits D and E, and all subsequent pairs;

(5) leave the final qubit unmeasured and discard all measured qubits.

After step (2), qubit B is left in a product state $\tau(f_0)$ with fidelity

$$f_0 = \frac{q(1-f_{\rm st}) + r f_{\rm st}}{r + q(1-f_{\rm st}) + (1-q-2r)f_{\rm st}}, \qquad \text{(E2)}$$

which is a generalization of Eq. (14).

Step (3) results in the familiar singlet projection on the second and third qubits (B and C). After this projection, qubit D is in the state $\tau(f_1)$, where f_1 is determined by the matrix equation

$$\begin{pmatrix} f_1 \\ 1-f_1 \end{pmatrix} \propto \begin{pmatrix} q & r \\ r & (1-2r-q) \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ 1-f_0 \end{pmatrix}, \qquad \text{(E3)}$$

where we use a proportionally sign because the leftmost vector must be renormalized to obtain the fidelity. This is then repeated between every $(2j+1)$th and $(2j+2)$th qubit. After all $n-1$ singlet projections, we find that the last qubit is left in the state $\tau(f_{n-1})$, where

$$\begin{pmatrix} f_{n-1} \\ 1-f_{n-1} \end{pmatrix} \propto \begin{pmatrix} q & r \\ r & (1-2r-q) \end{pmatrix}^{n-1} \cdot \begin{pmatrix} f_0 \\ 1-f_0 \end{pmatrix}.$$

The limiting behavior, for large n, of this matrix equation is determined by the matrix eigenvalues, μ_1 and μ_2, and eigenvectors. Whenever eigenvalues have different magnitudes, the matrix (as $n \to \infty$) projects onto the eigenvector[3] with the largest eigenvalue. As one would expect, when $\sigma(q,r)$ is a product state the eigenvalues are identical, but in all other cases there is one dominant eigenvalue which determines a limiting fidelity:

$$\lim_{n\to\infty} f_n = \left\{1 + \tan\left[\frac{1}{2}\arctan\left(\frac{2r}{2(r+q)-1}\right)\right]\right\}^{-1}. \qquad \text{(E4)}$$

Convergence to this fidelity is exponentially fast in the number, n, of copies of $\sigma(q,r)$. Specifically, for large but finite n, deviations from this fidelity vanish as $(\mu_2/\mu_1)^n$, where μ_2 is the smaller eigenvalue. In Fig. 5 we chart out various parameter regimes indicating when the resource is a stabilizer state and when it provides a resource for universal quantum computing. Universality may be achieved by a combination of the daisy-chain protocol followed by the standard five-qubit distillation procedure [12].

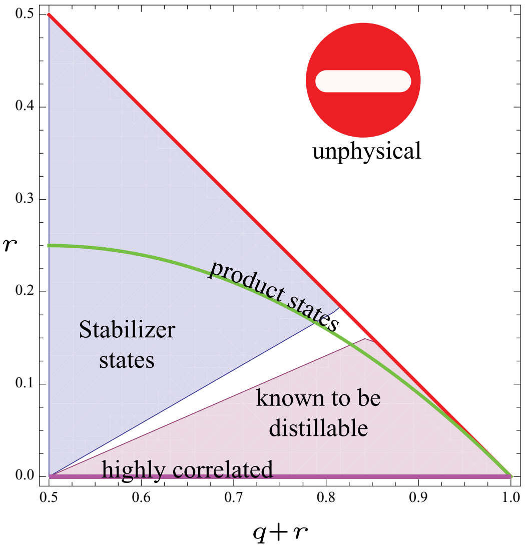

FIG. 5. (Color online) The "phase" diagram for correlated noise resource, $\sigma(q,r)$, as described by Eq. (E1). The diagram shows the region of stabilizer states, and the region of resources that are known to be universal for quantum computing. Universality is possible if the daisy-chain protocol achieves a fidelity [see Eq. (E4)] that exceeds the threshold above which the five-qubit code can be utilized as in Ref. [12].

Notice that product states are not the only nonstabilizer states where we observe a regime where no known methods enable universal quantum computing. There is a temptation to conjecture that some notion of boundness applies to any family of states that transverses the gap anywhere except via the origin. However, the daisy-chain protocol shows that all nonproduct states can be purified toward some state, even if that state is not above the threshold for the five-qubit code. As such, our current definition for boundness would not extend to these families. However, this seems like a failing of our definition more than anything else, as the extent of possible purification appears to be limited by how correlated the raw resource is.

Finally, note that a very similar protocol and analysis can be performed for two-qubit correlated states in any basis, not just the T basis.

APPENDIX F

Here we outline twirling protocols for bringing an arbitrary state into the form $\sigma(q,r)$, as defined in Eq. (E1). We perform the following:

(1) Randomly choose a unitary operator from the set $\{1, T, T^2\}$ and apply to qubit A;

(2) randomly choose a unitary operator from the set $\{1, T, T^2\}$ and apply to qubit B;

(3) randomly choose a unitary operator from the set $\{1, Y_A H_A SWAP_{A,B} H_A Y_A\}$ and apply.

The first two steps diagonalize the state in the $|T_{i,j}\rangle$ basis, and the third step mixes the symmetric terms.

[3] Note that in this context an eigenvector corresponds to a particular $(f, 1-f)$, and hence specifies a mixed state.

[1] D. Gottesman, Phys. Rev. A **57**, 127 (1998).

[2] A. Kitaev, Ann. Phys. **303**, 2 (2003).

[3] D. Hsieh, D. Qian, L. Wray, Y. Xia, Y. S. Hor, R. J. Cava, and M. Z. Hasan, Nature (London) **452**, 970 (2008).

[4] D. Hsieh *et al.*, Science **323**, 919 (2009).

[5] B. Eastin and E. Knill, Phys. Rev. Lett. **102**, 110502 (2009).

[6] M. Freedman, C. Nayak, and K. Walker, Phys. Rev. B **73**, 245307 (2006).

[7] L. S. Georgiev, Phys. Rev. B **74**, 235112 (2006).

[8] S. Bravyi, Phys. Rev. A **73**, 042313 (2006).

[9] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, Rev. Mod. Phys. **80**, 1083 (2008).

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

[11] B. W. Reichardt, Quantum Inf. Comput. **9**, 1030 (2009).

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

[13] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[14] J. Eisert and M. Plenio, Int. J. Quantum Inf. **1**, 479 (2003).

[15] B. W. Reichardt, Quantum Inf. Proc. **4**, 3 (2005); **4**, 251 (2005).

[16] B. W. Reichardt, *Algorithmica* (Springer, New York, 2007).

[17] W. van Dam and M. Howard, Phys. Rev. Lett. **103**, 170504 (2009).

[18] W. van Dam and M. Howard, Phys. Rev. A (accepted for publication) e-print arXiv:1011.2497.

[19] E. T. Campbell and D. E. Browne, Lect. Notes Comput. Sci. **5906**, 20 (2009).

[20] E. T. Campbell and D. E. Browne, Phys. Rev. Lett. **104**, 030503 (2010).

[21] N. Ratanje and S. Virmani, Phys. Rev. A (accepted for publication) e-print arXiv:1007.3455.

[22] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).

[23] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[25] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2001).

[26] J. Dehaene and B. De Moor, Phys. Rev. A **68**, 042318 (2003).