Classical simulability, entanglement breaking, and quantum computation thresholds

S. Virmani,[1] Susana F. Huelga,[1] and Martin B. Plenio[2]
[1]*School of Physics, Astronomy and Mathematics, Quantum Physics Group, STRC, University of Hertfordshire, Hatfield, Hertfordshire AL10 9AB, United Kingdom*
[2]*QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, United Kingdom*
(Received 7 September 2004; published 19 April 2005)

We investigate the amount of noise required to turn a universal quantum gate set into one that can be efficiently modeled classically. This question is useful for providing upper bounds on fault-tolerant thresholds, and for understanding the nature of the quantum-classical computational transition. We refine some previously known upper bounds using two different strategies. The first one involves the introduction of bientangling operations, a class of classically simulable machines that can generate at most bipartite entanglement. Using this class we show that it is possible to sharpen previously obtained upper bounds in certain cases. As an example, we show that under depolarizing noise on the controlled-NOT gate, the previously known upper bound of 74% can be sharpened to around 67%. Another interesting consequence is that measurement-based schemes cannot work using only two-qubit nondegenerate projections. In the second strand of the work we utilize the Gottesman-Knill theorem on the classically efficient simulation of Clifford group operations. The bounds attained using this approach for the $\pi/8$ gate can be as low as 15% for general single-gate noise, and 30% for dephasing noise.

DOI: 10.1103/PhysRevA.71.042328 PACS number(s): 03.67.Hk

I. INTRODUCTION

The recent development of quantum information has led to a great deal of interest in the classical simulation of quantum systems. An understanding of this issue is important in order to discern which resources are essential for an exponential quantum speedup. If we remove certain resources from a particular model for universal quantum computation, and find that the resulting machine can be efficiently simulated classically, then we can infer that those resources are essential to any exponential speedup that the original device may offer. For instance, this approach has been used to show that fermionic linear optics does not allow for an exponential speedup [1], and also that quantum entanglement is an essential ingredient for quantum computation [2–4].

In addition to questions of resources, an understanding of classically tractable quantum evolution is also useful for bounding the fault-tolerance thresholds of universal quantum machines. This connection becomes apparent from another important question concerning any universal quantum machine: what is the minimal amount of noise required before the device can be efficiently modeled classically? We loosely refer to this minimal noise level as the *classical tolerance* of a particular physical machine. We will also use the term *tractable* to describe any form of quantum evolution that may be modeled with polynomial classical resources. If it is true that quantum computation is not tractable classically, then upper bounds to the classical tolerance of the gates in a universal quantum gate set are also upper bounds to the fault tolerance of those gates. Aharonov and Ben-Or were among the first to obtain upper bounds on the classical tolerance thresholds of quantum gates [3]. To obtain their bounds they assumed that noise acts on every qubit at every stage of the computation, and showed that for noise above a certain amount the evolution becomes classically tractable (see also [4,5] for related work).

In addition to bounding fault tolerance, there is perhaps a more fundamental reason for investigating where the classical-quantum computational transition lies [3,6,7]. It may well be the case that noisy quantum devices cannot be simulated efficiently classically, yet cannot be used for fault-tolerant quantum computation. This would imply the existence of an "intermediate" physical device—such as a noisy quantum system controlled by a universal classical computer—which is clearly universal for computation, is better than classical as it can simulate itself efficiently, and yet is not as powerful as a full quantum computer. Hence classical tolerance thresholds also provide important (and perhaps easier) milestones for experimental efforts.

In this work, however, we will be more interested in the recent approach taken by Harrow and Nielsen [4] where they presented an algorithm for the efficient classical simulation of a quantum machine operating with *separability-preserving* (SP) quantum gate sets. The term "separability preserving" refers to any set of operations that cannot entangle product inputs. Harrow and Nielsen then derived bounds on the minimal noise levels required to turn certain universal quantum gate sets into SP machines, thereby obtaining bounds on the classical tolerance of those gates. Due to the lack of a simple characterization of the SP machines, in most cases their calculations proceeded not by considering the full set of SP machines, but instead the set of *separable machines*, which are those devices that only operate with separable quantum gates [8]. Their approach has the advantage that one can even consider weak-noise models where the noise only acts whenever multiqubit gates are applied. Depending upon the noise model, however, the upper bounds to classical tolerance derived in this way were of the order of 50% or more for interesting universal gate sets such as controlled-NOT (CNOT)+single-qubit operations. In terms of depolarizing noise only, Razborov [5] has obtained the strongest bounds that we are aware of for a general machine using gates of

 ©2005 The American Physical Society

(fan-in) $\leqslant 2$ (the *fan-in* of a gate is the number of particles that it acts upon nontrivially). He shows that for schemes based upon two qubit gates, 50% noise is an upper bound to fault tolerance. However, his approach cannot be directly compared to that of [4], as it does not consider efficient classical simulation, and assumes a different noise model (where each qubit is decohered at every time step).

In this article we will consider efficient classical simulation, and we will extend the approach taken in [4] along two different tracks. In the first track we define a class of quantum machines that can generate entanglement between product input states, but without additional resources can only generate at most two-particle entanglement. We refer to any machines that operate with our class of operations as *bientangling* (BE) machines. An extension of the algorithm presented in [4] shows that such BE machines can be efficiently simulated classically. We find that many, but not all, of the classical tolerance bounds derived in [4] are actually also optimal with respect to BE machines. One example of an improvement is the case of the CNOT gate under individual depolarizing noise on the qubits, where we show that a 67% noise rate leads to classical tractability, which is stronger than the 74% bound derived in [4]. Another interesting example comes from two-qubit measurement-based quantum computation, where we find that exponential speedup requires degeneracy in at least one of the projections—a result that cannot be directly derived from the approach in [4]. This example suggests that our approach could be more fruitful for noise models in measurement-based quantum computation. As an aside we also observe that there are separability-preserving gates that are not probabilistic mixtures of separable and separable+swap operations, thereby deciding a conjecture made in [4].

In the second track we make use of the Gottesman-Knill theorem [9]. All of the results discussed above are derived by considering machines that create a limited amount of entanglement, or are so noisy that they tend to some form of equilibrium. However, the important Gottesman-Knill theorem states that machines composed of Clifford group unitaries [10] and computational basis-state preparation and measurement can be efficiently modeled classically, despite the fact that such resources are capable of generating many-particle entanglement (although not all forms of it [11]). It is hence natural to ask whether such *Clifford machines* can lead to better bounds on classical tolerance than bientangling or SP machines. We calculate exactly the minimal noise required to take a variety of single-qubit gates into the set of Clifford operations—those operations that may be implemented by Clifford group unitaries, computational ancillae, and measurements in the computational basis. For the $\pi/8$ gate in particular [12], for generic single-operation noise, the bound obtained is approximately 14.64%, thereby showing that the $\pi/8$ gate in the standard universal set $\{\pi/8$, Clifford unitaries$\}$ cannot be made fault tolerant to more than this level of general individual gate noise. For dephasing noise on the $\pi/8$ gate the bound is twice as large, approximately 29.28%.

This paper is structured as follows. In the next section we discuss the class of bientangling machines and the classical algorithm that models them efficiently. In Sec. III we discuss the way that we will choose to represent quantum operations (via the *Jamiolkowski isomorphism* [13]), and derive our classical tolerance bound for the depolarized model of the CNOT gate that is considered in [4]. We also have performed such calculations for some other noise models; however, as they only match the bounds derived in [4], we defer those calculations to the Appendix. In Sec. IV we derive bounds for Clifford-operation-based gate sets by using the Gottesman-Knill theorem. In Sec. V we discuss some subtleties in the interpretation of results from Sec. IV. Section VI is the conclusion.

II. THE BIENTANGLING MACHINES

We define the term *bientangling machine* according to the following.

Definition. A Bientangling machine (BE machine) is one that consists of a supply of individual qubits initialized in some fixed state, augmented by the following quantum operations: (1) an arbitrary set of single-qubit quantum operations (these may be unitary, or measuring, or anything else); (2) an arbitrary set of two-qubit operations that can be expressed as convex combinations of (a) separable operations [8] that do not entangle the two qubits, (b) operations that swap the two qubits and then apply a separable operation, and (c) entanglement-breaking (EB) [14] operations that break any entanglement between the two qubits and the rest of the qubits.

The fact that any machine consisting of (1), (2a) and (2b) is efficiently classically tractable was already shown in [4], as such operations lie (strictly) within the set of separability-preserving operations. The only point added here is the inclusion of operations from (2c), and the resulting convex hull with the separable and separable with swap operations. The heuristic explanation for the algorithm is that a machine consisting of operations (1) and (2) above only has the power to generate two-particle entanglement. This allows us, with at most polynomial classical effort, to reduce the problem of tracking the evolution of a BE machine to the problem of tracking the evolution of a SP machine. One can then simply apply the results proven in [4], where it is shown that SP machines are classically tractable.

Let us now see why the evolution of BE machines may be reduced to the evolution of SP machines. As we are considering operations with (fan-in) $\leqslant 2$, we may without loss of generality assume that all operations in our BE machine are in fact two-qubit operations (by extending any single-qubit operations to trivially act on another arbitrary qubit). At the beginning of the algorithm, we may compute how each of the two-qubit gates available to us decomposes into a probabilistic mixture of the various operations listed in points (1) and (2) above. Each component of this description will in fact only be calculated to some finite precision. However, the arguments given in [4] show that the accuracy required to achieve a particular overall accuracy in the algorithm will lead to at most a polynomial increase in effort. Consequently we will proceed as if this decomposition has in fact been computed exactly.

Without loss of generality we assume that there are an even number of qubits in the quantum system. To initialize

our classical description, each qubit is paired up with a *partner* qubit. A list of the partners is stored, requiring only modest resources. Note that it is also possible to retrieve information from this list at modest cost. We will treat each such qubit partnership as a single four-level particle. Having initialized our description, we now must track the evolution of the system. By changing the way that the qubits are partnered as we advance through the algorithm, we will ensure that at each stage we end up with an easy to compute separable state. Consider the application of the first bientangling gate, and suppose that it acts upon qubits 2 and 3. If qubits 2 and 3 are already partners, then the evolution of the system essentially corresponds to single-particle evolution, as we are regarding each partnership as a single four-level system. So suppose instead that qubits 2 and 3 are not partnered, and that qubit 2 is partnered with qubit 1, and qubit 3 is partnered with qubit 4. The bientangling gate decomposes into a probabilistic application of (α) a separable gate, (β) a separable +swap gate, and (γ) an EB gate. We can sample this probability distribution efficiently, and use this to decide which component (α–γ) we will follow. The case α corresponds to a separable operation on partnerships (1,2) and (3,4). The case β results in a separable state if the partnership list is changed to (1,3) and (2,4). Finally γ results in a separable state if the partnerships are changed to (1,4) and (2,3). Hence by iterating these techniques for every gate that we apply, we ensure that we end up with a separable state over effective four-level systems. The algorithm of [4] can be applied, and hence we can see that there is a classically efficient algorithm for bientangling machines with (fan-in) $\leqslant 2$.

One might hope that the algorithm may be extended, either to gates with higher fan-in, or by incorporating all SP operations instead of only the separable and separable+swap operations. However, this cannot be done straightforwardly. We defer the discussion of why we cannot include all SP operations to the next section. To see why we cannot extend the fan-in of the gates either, it is interesting to consider the connection between the above algorithm and measurement-based quantum computation schemes [15,16,25]. This situation also provides a simple first example of where consideration of bientangling machines may yield more information than consideration of SP machines alone. In measurement-based computation schemes it is known that two-qubit measurements allow universal quantum computation [15]. However, our algorithm shows that we must allow these measurements to be degenerate, because if they are nondegenerate, then the resulting operations will be EB, and the device cannot offer an exponential speedup. This leads to a useful rule: any two-qubit measurement-based scheme for quantum computation must involve nondegenerate measurements.

Although this observation is quite simple, it applies to gates that can generate *some* entanglement (e.g., Bell measurements), and so it cannot be derived directly from the approach in [4]. However, this limit on the capacity to generate multiparticle entanglement is removed when we allow EB channels with three or more inputs, and this is one reason why universal quantum computation is possible using some forms of nondegenerate measurements on three or more particles (see, e.g., the paper by Gottesman and Chuang on teleportation based computation; they use Greenberger-Horne-Zeilinger- (GHZ-)like states and Bell measurements [16]). Therefore it is difficult to extend the bientangling class to gates acting on three or more parties.

III. REPRESENTATION OF QUANTUM OPERATIONS BY STATES

In order to utilize the above algorithm to bound the classical tolerance of quantum gates, it is important to be able to decide when a given set of quantum operations falls into the class of BE machines. In general this problem is extremely difficult. However, some important operations such as the CNOT gate possess a great deal of symmetry that makes the analysis feasible analytically. In order to perform this analysis, the Jamiolkowski isomorphism [13] provides a convenient way of representing quantum operations. To any trace-preserving quantum operation $\mathcal{E}$ on a single particle of d levels, the Jamiolkowski isomorphism associates a two-party quantum state that we will refer to as the *Jamiolkowski state* $\rho(\mathcal{E})$:

$$\rho(\mathcal{E}) := I_A \otimes \mathcal{E}_B(|+\rangle\langle+|) \tag{1}$$

where $|+\rangle := (1/\sqrt{d})\Sigma_{i=1}^{d}|ii\rangle$ is the canonical maximally entangled state for two d-level systems A and B. It is clear from the above definition that $\rho(\mathcal{E})$ has a reduced density matrix $[\rho(\mathcal{E})]_A$ that is maximally mixed. It turns out that any density matrix with this property (i.e., one with ρ_A maximally mixed) can be associated with a quantum operation $\mathcal{E}$. Moreover, a simple teleportation argument can be used to show that this association is one to one. Hence the Jamiolkowski isomorphism is a one-to-one mapping between the set of trace-preserving quantum operations $\mathcal{E}$ and two-party quantum states with maximally mixed reduced density matrix.

This isomorphism can be easily applied to multiparty quantum operations in the following way. Suppose that we have a two-particle quantum operation $\mathcal{E}_{12}$ acting upon two qubits 1 and 2. To represent this operation we must use a quantum state of four parties $A1$, $A2$, $B1$, and $B2$ [17]:

$$\rho(\mathcal{E}_{1,2}) := I_{A1} \otimes I_{A2} \otimes \mathcal{E}_{B1,B2}[(|+\rangle\langle+|)_{A1,B1} \otimes (|+\rangle\langle+|)_{A2,B2}].$$

This representation is particularly convenient because various important properties of quantum operations $\mathcal{E}$ may easily be translated into properties of the corresponding state $\rho(\mathcal{E})$. In this work we will consider three such properties (see Fig. 1). (a) An operation is separable if and only if the Jamiolkowski state is separable across the ($A1B1$)-($A2B2$) split. (b) An operation is equivalent to the swap operation, preceded by and followed by separable operations, if and only if the Jamiolkowski state is separable across the ($A1B1$)-($A2B2$) split. (c) An operation is entanglement breaking if and only if the Jamiolkowski state is separable across the ($A1A2$)-($B1B2$) split.

A set of operations is bientangling if every operation lies within the convex hull of these three classes (a), (b), and (c). An operation is hence bientangling if and only if the Jamiolkowski state that represents it can be written as

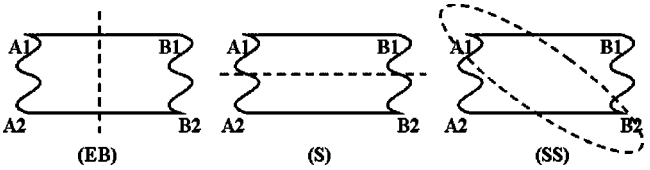

FIG. 1. Entanglement-breaking (EB), separable (S), and separable+swap (SS) operations have a simple connection to Jamiolkowski-state separability. For EB and separable operations, the dashed line indicates the corresponding separable split. For separable+swap operations the dashed ellipse indicates the splitting. In all diagrams the wavy lines indicate entanglement between pairs 1 and 2.

$$\rho = p\sum_i p_i \rho^i_{A1A2} \otimes \rho^i_{B1B2} + q\sum_j q_j \rho^j_{A1B2} \otimes \rho^j_{A2B1} + r\sum_k q_k \rho^k_{A1B1} \otimes \rho^k_{A2B2} \tag{2}$$

where (p,q,r) is a probability distribution, the sets $\{p_i\}$, $\{q_j\}$, $\{r_k\}$ are also individual probability distributions, and all ρ's on the right-hand side are valid density matrices.

This is a convenient point to discuss the relationship between BE machines and SP machines. It is clear from the above definition that BE machines contain the convex hull of the separable operations with separable+swap operations. However, they do not contain all possible separability-preserving operations. This becomes apparent from consideration of the following Jamiolkowski state:

$$\omega := \frac{1}{2}|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_{A1,A2,B1} \otimes |0\rangle\langle 0|_{B2} + \frac{1}{2}|\mathrm{GHZ}'\rangle \times \langle\mathrm{GHZ}'|_{A1,A2,B1} \otimes |1\rangle\langle 1|_{B2}$$

where

$$|\mathrm{GHZ}\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$

$$|\mathrm{GHZ}'\rangle := \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle). \tag{3}$$

As ω is a valid density matrix with the reduced state of parties $A1$ and $A2$ maximally mixed, it corresponds to the Jamiolkowski state of a valid quantum operation. When viewed as a state of four parties, ω also has the property that a GHZ-type state can be distilled from it by local operations and classical communication (LOCC) simply by measuring the particle $B2$ in the computational basis. However, as the Jamiolkowski states of bientangling operations contain only two-particle entanglement, this means that ω cannot represent a bientangling operation. However, ω manifestly represents a SP operation, because the output qubits $B1$ and $B2$ are always left in a separable state. Therefore we can also conclude that the conjecture made in [4] that SP operations $\neq$ (convex hull {separable operations, separable+swap}) is indeed true [18]. In the above definition of BE machines, we have included the ability to make separable operations, separable+swap operations, and EB operations. One might be tempted to expand this definition to include all SP operations as well. However, operations such as ω have the capacity to probabilistically generate many-particle entanglement when accompanied by EB channels such as Bell measurements, and so in our definition of BE machines we are forced to include the smaller classes of separable and separable +swap operations, and not the larger class of SP operations.

We would now like to use the class of BE machines defined above to obtain bounds on the classical tolerance of important universal gate sets. Suppose for example that we have a universal quantum computer consisting of the CNOT gate and a sufficient set of single-qubit operations. If we add some noise to the CNOT gate such that it is taken to a bientangling operation, then the whole set is taken to a BE machine, and can be efficiently classically simulated. Hence to bound the classical threshold of the CNOT gate in our device, we would like to calculate the minimal noise required to turn the CNOT gate into a bientangling operation. In general such calculations are very difficult.

It is at this point that we must discuss the form of the noise model that we consider. In the rest of this article we adopt the standard *probabilistic* noise model, where qubits are affected incoherently. In this model whenever we would like to perform an ideal quantum operation $\mathcal{E}$, instead due to noise we are forced to perform an operation $\mathcal{E}'$ that is related to $\mathcal{E}$ as follows:

$$\mathcal{E}' = (1-p)\mathcal{E} + p\mathcal{N} \tag{4}$$

where p is a probability, and $\mathcal{N}$ is some other quantum operation that represents the error. In this equation p is a measure of the error rate. Note that this is not the most general model of error, and not necessarily the most physical model either. Consider the example where our ideal operation is to simply preserve the state of a qubit, but in fact it undergoes a spontaneous emission at a sufficiently slow rate. This form of error cannot be written in the form of Eq. (4) unless the error parameter is set to $p=1$ (see, e.g., [12], p. 442). For more generic errors one would have to adopt some suitable metric $\|\cdot\|$ on the set of quantum operations and use $\|\mathcal{E}'-\mathcal{E}\|$ as a measure of error rate (see, e.g., [19] for some possible metrics). Although several authors have considered more general models of error in relation to fault tolerance [20], the only prior work on classical tolerance has been within the framework of Eq. (4), and this is the model that we will follow here. In the case of Markovian, identical, and independent noise it should be possible to extend many of the techniques presented to metric-based noise quantification, although we will not pursue that avenue further. Within the probabilistic model, one can also make further restrictions, and constrain the form of $\mathcal{N}$ to interesting forms of noise such as depolarization or dephasing. We have investigated a variety of different types of $\mathcal{N}$, and derived bounds on the classical tolerance for the CNOT gate in particular. In most of the examples that we have considered, the bounds that we have derived are equivalent to those obtained in [4], and so calculations for such examples are deferred to the Appendix. However, in the case of the depolarizing noise model considered in [4] we are able to make significant improvements, and so we will present this argument now.

In order to set up our analysis, let us initially consider $\mathcal{N}$ to be a general quantum operation. This will allow us to construct symmetry arguments that are also required for the calculations presented in the Appendix. Given that our error model is probabilistic, our task is to find the minimal value p such that there is a valid $\mathcal{N}$ taking our ideal gate into the set of bientangling operations. In general this is likely to be a difficult task. However, for the case of the CNOT gate a great deal of symmetry is present that enables the calculation to be performed exactly. In order to see how this proceeds, it will be first helpful to consider the case that the two-qubit gate is a general unitary U, and examine some of the symmetry possessed by the Jamiolkowski state that represents U.

For any two-qubit unitary U we have the trivial identity

$$[U(\sigma_i \otimes \sigma_j)U^\dagger]U(\sigma_i \otimes \sigma_j) = U \tag{5}$$

where $\{\sigma_i | i=0,x,y,z\}$ are the standard Pauli operators. This identity, together with the fact that $I \otimes A|+\rangle = A^T \otimes I|+\rangle$ for any linear operator A, can be used to show that the Jamiolkowski state representing U commutes with all operators of the form

$$W_{ij}^U := (\sigma_i^T)_{A1} \otimes (\sigma_j^T)_{A2} \otimes [U(\sigma_i \otimes \sigma_j)U^\dagger]_{B1,B2}. \tag{6}$$

It is not hard to verify that as we vary over i, j the operators in Eq. (6) form a group (up to an unimportant phase), and moreover from the commutation relationships of the Pauli operators it follows that the group is Abelian. It hence follows from Schur's lemma that any operator that commutes with all operators of the form (6) is diagonal in the eigenbasis formed by the one-dimensional irreducible representations of the group (6). We can construct these irreducible representations quite easily. In fact, the group (6) is isomorphic to the group consisting of elements

$$(\sigma_i^T)_{A1} \otimes (\sigma_j^T)_{A2} \otimes (\sigma_i)_{B1} \otimes (\sigma_j)_{B2}, \tag{7}$$

as it is related to (6) by the unitary transformation $I_{A1} \otimes I_{A2} \otimes U_{B1,B2}$. Hence we can utilize the stabilizer formalism for the Pauli group, and write the 16 common eigenstates of the operators in (6) as

$$|e,U\rangle\langle e,U| := \left(\frac{I+(-1)^{e_0}W_{0x}^U}{2}\right)\left(\frac{I+(-1)^{e_1}W_{0z}^U}{2}\right) \times \left(\frac{I+(-1)^{e_2}W_{x0}^U}{2}\right)\left(\frac{I+(-1)^{e_3}W_{z0}^U}{2}\right) \tag{8}$$

where e is a four-bit string given by its components $e_\alpha \in \{0,1\}$, $\alpha=0, 1, 2, 3$. It turns out that each of these eigenprojectors $|e\rangle\langle e|$ is a Jamiolkowski state for a valid quantum operation—the normalization and positivity are automatic, and the reduced density matrices over particles $A1$ and $A2$ are all maximally mixed (this is in turn because $\sigma_i \otimes \sigma_j$ is an irreducible representation). The Jamiolkowski state representing U is in fact given by the projector $|e=0,U\rangle\langle e=0,U|$ corresponding to $e=0$:

$$\left(\frac{I+W_{0x}^U}{2}\right)\left(\frac{I+W_{0z}^U}{2}\right)\left(\frac{I+W_{x0}^U}{2}\right)\left(\frac{I+W_{z0}^U}{2}\right). \tag{9}$$

If we denote the Jamiolkowski state that represents U by $\rho(U)=|e=0,U\rangle\langle e=0,U|$, then our task is to find the minimal probability p such that for some quantum noise $\mathcal{N}$

$$\mathcal{E} = (1-p)\rho(U) + p\rho(\mathcal{N}) \tag{10}$$

is the Jamiolkowski state of a bientangling operation. Now the properties of the CNOT gate allow us to make further simplifications. The CNOT gate is a member of the Clifford group, meaning that for any two Pauli operators σ_i, σ_j we have that

$$C_{\mathrm{CNOT}}(\sigma_i \otimes \sigma_j)C_{\mathrm{CNOT}} \sim \sigma_k \otimes \sigma_l \tag{11}$$

where σ_k, σ_l are other Pauli operators, and the symbol $\sim$ means that the two sides of the equation are equal up to an unimportant global phase. This means that the group (6) corresponding to the CNOT gate is actually a local group, where each element is a tensor product of Pauli operators acting on individual qubits of the Jamiolkowski state. We can therefore average ("twirl") over the group (6) any valid solution (10) corresponding to the CNOT gate, and as each W_{ij}^{CNOT} is local, the bientangling properties of the equation will not be changed. This means that without loss of generality, for the CNOT gate we need only consider "twirled" noise states $\rho'(\mathcal{N})$ that are also invariant under the action of the group. This means that we can set

$$\rho'(\mathcal{N}) = \sum_e \lambda_e(\mathcal{N})|e\rangle\langle e| \tag{12}$$

where $\{\lambda_e\}$ is a probability distribution of eigenvalues. If we have not constrained further the form of $\mathcal{N}$, then the form of the probability distribution $\{\lambda_e(\mathcal{N})\}$ can be left free. However, if we are restricting $\mathcal{N}$ to be of a specific form such as depolarization or dephasing, then we will have to restrict the distribution accordingly. Our task is hence to find the minimal probability p such that there exists a probability distribution $\{\lambda_e(\mathcal{N})\}$ (consistent with any further constraints upon the noise) such that the state

$$\begin{aligned}(1-p)\rho(U) + p\left(\sum_e \lambda_e(\mathcal{N})|e\rangle\langle e|\right) &\equiv [(1-p)+p\lambda_0(\mathcal{N})]|e=0\rangle \\ &\times \langle e=0| + \sum_{e\neq 0} \lambda_e(\mathcal{N})|e\rangle\langle e|\end{aligned} \tag{13}$$

is bientangling. Let us denote this optimal value of p by $p_{\min}$. We have performed this optimization for the cases that $\mathcal{N}$ is (a) an unconstrained quantum operation, (b) a separable operation, separable+swap operation, or mixture of the two, and (c) depolarizing noise. We defer the calculations for (a) and (b) to the Appendix, as they do not lead to improvements over the results in [4]. However, we present the calculation for (c) here, as it leads to an improved bound.

Depolarizing noise. In the depolarizing model of [4], each qubit undergoing a two-qubit gate is independently depolar-

ized with equal probability p. Hence a noisy two-qubit unitary U in fact acts as

$$(1-p)^2U + p(1-p)(D\otimes I)U + p(1-p)(I\otimes D)U + p^2 D\otimes D \tag{14}$$

where D represents the single-qubit depolarizing quantum operation,

$$D{:}\rho \to \frac{I}{2}, \tag{15}$$

and U represents the ideal unitary quantum operation (we often represent a unitary and the corresponding quantum operation by the same letter—the meaning should be clear from the context). In particular we will take U to be the CNOT operation. In order to derive an upper bound on the minimum value of p required to make this noisy operation bientangling, we will first show that the (unnormalized) quantum operation corresponding to the central terms of Eq. (14),

$$p(1-p)[(D\otimes I)U + (I\otimes D)U], \tag{16}$$

is in fact a separable operation (not just SP) for any value of p. Hence if the (unnormalized) operation corresponding to the outer terms

$$(1-p)^2U + p^2 D\otimes D \tag{17}$$

is entanglement breaking, then the whole operation (14) is bientangling. First we must show that the central terms (16) correspond to a separable operation. Consider the operation $(D\otimes I)U$, where U is the CNOT gate. After a little algebraic manipulation of the Jamiolkowski state corresponding to the CNOT gate, it can be shown that the Jamiolkowski state of $(D\otimes I)U$ is

$$\rho((D\otimes I)U) = \left(\frac{I + I_{A1}\otimes I_{B1}\otimes X_{A2}\otimes X_{B2}}{2}\right) \times \left(\frac{I + Z_{A1}\otimes I_{B1}\otimes Z_{A2}\otimes Z_{B2}}{2}\right).$$

Writing this out in the computational basis where $|0\rangle$ represents the $+1$ eigenstate of the Z operator and $|1\rangle$ represents the -1 eigenstate of the Z operator, we find that $\rho((D\otimes I)U)$ may be written as an equal mixture of the following four (unnormalized) pure states:

$$|0_{A1}0_{B1}\rangle\otimes(|0_{A2}0_{B2}\rangle + |1_{A2}1_{B2}\rangle),$$

$$|0_{A1}1_{B1}\rangle\otimes(|0_{A2}0_{B2}\rangle + |1_{A2}1_{B2}\rangle),$$

$$|1_{A1}0_{B1}\rangle\otimes(|0_{A2}1_{B2}\rangle + |1_{A2}0_{B2}\rangle),$$

$$|1_{A1}1_{B1}\rangle\otimes(|0_{A2}1_{B2}\rangle + |1_{A2}0_{B2}\rangle).$$

As each of these pure states is separable across the $(A1B1)$-$(A2B2)$ split, it is clear that $(D\otimes I)U$ is a separable operation. Similarly, one can show that the Jamiolkowski state representing the operation $(I\otimes D)U$ is related to the state representing $(D\otimes I)U$ in the following way:

$$\rho((I\otimes D)U) = O_{\mathrm{SWAP}_{1\leftrightarrow 2}}[H^{\otimes 4}\rho((D\otimes I)U)H^{\otimes 4}] \tag{18}$$

where the $H^{\otimes 4}$ is a Hadamard rotation on each qubit, and $O_{\mathrm{SWAP}_{1\leftrightarrow 2}}$ is the operation that interchanges $A1$ with $A2$ and $B1$ with $B2$. As $\rho((I\otimes D)U)$ is related to $\rho((D\otimes I)U)$ by local rotations followed by interchanging the labels $1\leftrightarrow 2$, it is also separable across the $(A1B1)$-$(A2B2)$ split, and hence both central terms in Eq. (14) correspond to separable operations.

It now remains for us to determine values of p for which the outer terms (17) represent an entanglement-breaking operation. The CNOT operation, as with any unitary on two qubits, is represented by a Jamiolkowski state that is maximally entangled across the $(A1B1)$-$(A2B2)$ splitting. The depolarizing operation on both qubits $D\otimes D$, on the other hand, is represented by a maximally mixed state. Hence if we are only considering the $(A1B1)$-$(A2B2)$ splitting, the state representing the operation of Eq. (17) is essentially a maximally entangled state of two four-level systems, mixed with a maximally mixed state. The conditions for such a state to correspond to an entanglement-breaking operation are that it must be separable across the $(A1B1)$-$(A2B2)$ splitting (note that this does not mean that the operation itself is separable, only that it is entanglement breaking). The conditions under which this occurs are well known, and correspond to

$$\frac{(1-p)^2 + p^2/16}{(1-p)^2 + p^2} \leqslant \frac{1}{4}, \tag{19}$$

giving that (17) is entanglement breaking whenever

$$p \geqslant 2/3 \simeq 67\%. \tag{20}$$

This means that the noisy CNOT gate is definitely bientangling whenever the depolarizing noise rate is greater than $2/3\sim 67\%$. This is an improvement over the 74% bound derived in [4] for exactly the same noise model, and hence shows that consideration of BE-machines may lead to tighter bounds than consideration of separable machines alone. Of course the calculation here is not a full optimization over all bientangling gates—we have only calculated the minimal p required to make the inner terms separable and the outer terms entanglement breaking. This hence only provides an upper bound to the minimal p required to make the CNOT gate bientangling, and hence there is a possibility that this calculation may be improved. However, as such full optimization is likely to be difficult, we leave it to another occasion.

It is also worth noting that the classical tolerance bound of $2/3$ derived here applies to any two-qubit unitary W for which the inner terms $(I\otimes D)W$ and $(D\otimes I)W$ are separable. This is because Eq. (19) guarantees that the outer terms (17) will be entanglement breaking for any two-qubit unitary, not just the CNOT gate.

IV. BOUNDS FROM THE GOTTESMAN-KNILL THEOREM

In order to apply the Gottesman-Knill theorem [9] to calculate bounds on the classical tolerance of quantum gates,

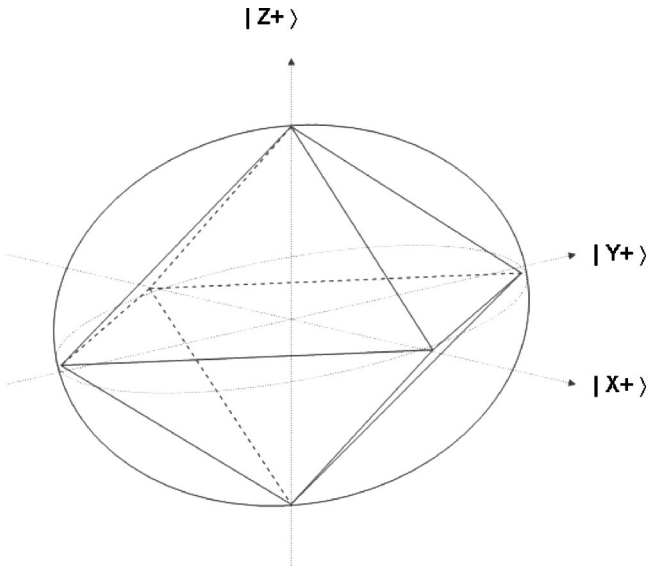

FIG. 2. The accesible states via Clifford unitaries define an octahedron in the Bloch sphere. Note that the vertices of the octahedron correspond to the Pauli eigenstates.

we need to compute the minimal amounts of noise required to take all the gates in a particular machine into the Clifford class. Unfortunately this restricts severely the possible situations in which this approach may be applied. In previous examples we have calculated the classical tolerance of certain two-qubit gates with only very loose constraints on the other gates available to the machine. In this section we will calculate the classical tolerance of single-qubit gates, assuming that the other gates in the machine are Clifford operations, where we define Clifford operations as follows.

Definition. Clifford operations are those operations that can be performed by probabilistic application of Clifford-group unitaries [10], (ancilla) state preparation in the computational basis, and measurement in the computational basis.

We will ask how much noise is required to turn non-Clifford single-qubit gates into a Clifford operation. The resulting bounds on the classical tolerance can be relatively low. For general single-qubit operations we will show that the classical tolerance to generic noise is no greater than 75%, although on a case-by-case basis this can be made much stronger. For example for the $\pi/8$ gate, we find that $(\sqrt{2}-1)/2\sqrt{2}\sim 14.64\%$ noise is the minimal amount required to turn the gate into a Clifford operation.

In order to perform these calculations, at first it seems necessary to understand which single-qubit operations can be implemented using Clifford-group unitaries and ancillas prepared in the computational basis. However, we will not characterize this set exactly here, as to obtain optimal bounds for many interesting cases it turns out that it is sufficient to consider the effect that Clifford operations have upon a particular subset of single-qubit states.

We will consider the set of states that is given by the convex hull of the Pauli operator eigenstates. This set is an octahedron O that is shown in Fig. 2. Our choice of this set is inspired by the recent work of Bravyi and Kitaev [6], who consider which single-qubit state supplies may allow the Clifford operations to become universal. We will first argue that the octahedron O can only be mapped to within itself by Clifford operations, and use this fact to simplify the optimizations that we wish to perform.

Observation. The octahedron O is closed under the action of Clifford operations.

Proof. Let us consider a system s that is prepared in one of $\{|x\pm\rangle\langle x\pm|,|y\pm\rangle\langle y\pm|,|z\pm\rangle\langle z\pm|\}$, where $|a\pm\rangle$ refer to the up and down eigenstates of the corresponding Pauli operator A. These states correspond to the vertices of the octahedron O. Suppose also that there are $n-1$ ancillae prepared in the computational basis, as can be prepared by Clifford operations. We need to calculate what final states of the system are possible given Clifford-group unitary evolution of the system +ancilla and Clifford-group measurements. As the entire input state is a stabilizer state [9,12], the final state of system +ancilla will also be a stabilizer state that is uniquely specified by its stabilizer generators

$$\{g_1,g_2,\ldots,g_n\}$$

where each g_i is a product of Pauli operators. Hence from the standard theory of stabilizers, the final state of system +ancilla will be given by

$$\left(\frac{1}{2^n}\right)\prod_{i=1..n}(I+g_i).$$

This equation may be expanded, and each element of the group that is generated by the stabilizer will contribute exactly one term in this expansion (this follows from the independence of the stabilizer generators [12]). As any nontrivial Pauli operator is traceless, tracing out the $n-1$ ancilla qubits from each term will only lead to a contribution to the final reduced state of the system if the term is of the form $(1/2^n)A_s$, where $A_s:=A_{\text{system}}\otimes I\otimes I\otimes\cdots$, in which case the term will contribute $A/2$ to the system density matrix. Our goal is hence to find every group element of the form A_s in the stabilizer group. As the identity I is an element in each stabilizer group, we will at least have a contribution of $I/2$ (which is of course a requirement in the Bloch expansion of any single-qubit state). However, we need to find all other terms of the form A_s.

This task can be constrained as follows. First, in each stabilizer group each element is its own inverse. This means that any nontrivial terms of the required form must actually be one of the six possibilities $\pm X_s$, $\pm Y_s$, or $\pm Z_s$. Moreover, at most only *one* of these six possibilities is present in each stabilizer group, as if two or more are present, then repeated multiplication we would force $-I$ to be a member of the stabilizer group [e.g., $(X_sY_s)^2=-I$], and this is not possible. This means that input system states taken from the vertices of the octahedron will be taken to either the maximally mixed state $I/2$, or one of the eigenstates of the X,Y,X operators [corresponding to $(I/2\pm X/2),(I/2\pm Y/2),\ldots$ etc.]. This means that the vertices will be taken either to the maximally mixed state, or to another vertex. Then by convexity the octahedron O can only be mapped *onto or within* itself by Clifford operations. □

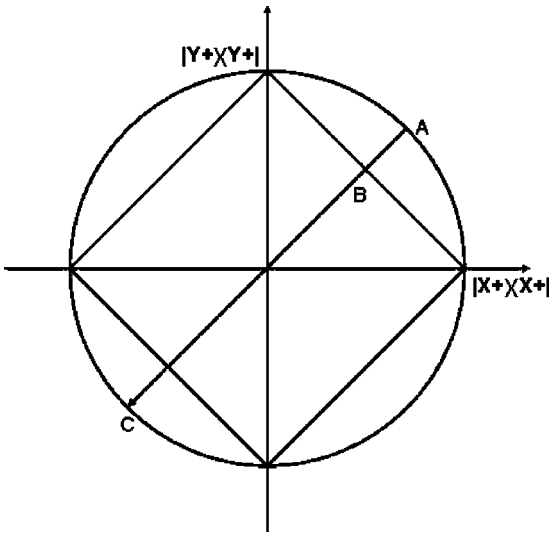

FIG. 3. Cross section of the Bloch sphere in the *x*-*y* plane. Point *A* represents the state $|\psi(\pi/4)\rangle$, and the ratio $|AB|/|AC|$ represents the exact minimal possible noise level required to take the $\pi/8$ gate into the set of Clifford operations.

This observation may be used to give *lower* bounds on the amount of noise required to take any particular unitary operation into a Clifford operation. Then by explicit construction we will be able to show that whenever the unitary is diagonal in the computational basis, these lower bounds may be achieved, and are hence tight. First let us see why the above arguments allow us to construct lower bounds on the minimal noise level required. Consider a unitary gate of the form

$$U(\theta) := |0\rangle\langle 0| + \exp(i\theta)|1\rangle\langle 1|. \tag{21}$$

This gate acts upon the $|x+\rangle$ state to give

$$|\psi(\theta)\rangle := \frac{1}{\sqrt{2}}[|0\rangle + \exp(i\theta)|1\rangle]. \tag{22}$$

We may visualize this by looking at the cross section of the Bloch sphere given by the *x*-*y* plane. This is shown in Fig. 3, with the point *A* representing $|\psi(\pi/4)\rangle$ corresponding to the action of the $\pi/8$ gate. One can see intuitively from the figure, and this can easily be shown rigorously, that the minimal noise level required to take the state $|\psi(\pi/4)\rangle$ into the octahedron is given by the ratio $|AB|/|AC|$ from the figure. In the case of the $\pi/8$ gate, the ratio $|AB|/|AC|$ corresponds to a noise level of

$$p = \frac{\sqrt{2}-1}{2\sqrt{2}} = 0.1464. \tag{23}$$

If a noise level less than this amount could be added to the gate $U(\theta)$ to turn it into a Clifford operation, then this would mean that the $|x+\rangle$ state would be mapped to outside the octahedron *O* by the noisy operation. As this is not possible, we can assert that (23) is a *lower* bound on the amount of noise required to take the operation $U(\theta)$ into the Clifford operations.

The utility of pictures such as Fig. 3 is that they may be used to show that bounds such as (23) are in fact also upper bounds, and are hence tight. The argument for this is strongly related to the construction presented [6] for the programming of unitary operations in quantum states. Every state on the circumference of the Bloch sphere in the *x*-*y* plane corresponds to a pure state of the form

$$|\psi(\theta)\rangle := \frac{1}{\sqrt{2}}[|0\rangle + \exp(i\theta)|1\rangle]. \tag{24}$$

These states are clearly isomorphic to the Jamiolkowski states representing each $U(\theta)$, simply by changing $|0\rangle \rightarrow |00\rangle$ and $|1\rangle \rightarrow |11\rangle$:

$$|J(\theta)\rangle := \frac{1}{\sqrt{2}}[|00\rangle + \exp(i\theta)|11\rangle]. \tag{25}$$

Hence by using convexity every state in the *x*-*y* cross section of the Bloch sphere represents a valid quantum operation. From this isomorphism we see hence that each of the vertices represents a Clifford unitary: $|x+\rangle$ represents the identity gate σ_0, $|x-\rangle$ represents the Pauli *Z* rotation, $|y+\rangle$ represents the so-called *phase gate* [9], denoted by the letter *S*,

$$S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{26}$$

and $|y-\rangle$ represents its inverse S^{-1}. This mapping hence shows that bounds such as (23) can indeed be attained, as the *x*-*y* plane of the Bloch sphere maps directly into a problem concerning quantum operations and a subset of the Clifford operations. Hence for gates of the form $U(\theta)$ we have the following statement.

Lemma 1. The minimal noise required to turn $U(\theta)$ into a Clifford operation is equivalent to the minimal noise required to take the state $|\psi(\theta)\rangle$ into the octahedron *O* in Fig. 3.

As shown above, in the case of the $\pi/8$ gate this lemma returns a minimal noise level of approximately 14.64%. The same procedure also yields sharp bounds for any unitary gate that may be diagonalized by Clifford-group unitaries, as well as for any quantum operation that is a convex mixture of such unitaries.

We may also apply the above arguments to some cases where the noise is constrained to be of a specific form. Suppose for example that we wish to know how much dephasing noise is required to take the $\pi/8$ gate into the set of Clifford operations. The dephasing operation takes $|x+\rangle$ to the maximally mixed state, at the center of the Bloch sphere in Fig. 3. On the other hand, when Fig. 3 is viewed as representing Jamiolkowski states of quantum operations, the center of the circle in Fig. 3 also represents the dephasing operation. Hence the above arguments also show the following lemma.

Lemma 2. The minimal dephasing noise required to take any gate $U(\theta)$ into a Clifford operation is identical to the minimal amount of the maximally mixed state required to take the corresponding state $|\psi(\theta)\rangle$ into the octahedron *O* in Fig. 3.

In the case of the $\pi/8$ gate this shows that approximately 30% dephasing noise is required to take the $\pi/8$ gate into the Clifford operations, or more precisely twice the value in Eq. (23):

$$\frac{\sqrt{2}-1}{\sqrt{2}} = 0.2928. \tag{27}$$

Although the bounds on the classical noise threshold obtained in this way are quite low compared to bounds obtained in Refs. [3–5], the above procedure has the disadvantage that it applies only to very specific gate sets, whereas previous works have applied to much wider classes of machine. At the expense of increasing the bound, we can, however, make the approach more general. For instance, we can show that the universal gate set consisting of Clifford operations augmented by *any* trace-preserving single-qubit operation has a classical noise tolerance of no greater than 75% on the additional single-qubit operation. The argument proceeds as follows. Given any single-qubit trace preserving operation $\mathcal{E}$, we can always turn it into an operation that is a convex mixture of Clifford group operations by the following method. Instead of performing $\mathcal{E}$ on an input state ρ, we perform

$$\frac{1}{4}\mathcal{E}(\rho) + \frac{3}{4}\sum_{i=x,y,z}\frac{1}{3}\sigma_i(\mathcal{E}(\sigma_i^T\rho\sigma_i^*))\sigma_i^\dagger. \tag{28}$$

In the Jamiolkowski representation this quantum operation can be represented as

$$\frac{1}{4}\{R_{\mathcal{E}} + [(\sigma_x\otimes\sigma_x)R_{\mathcal{E}}(\sigma_x\otimes\sigma_x)^\dagger] + [(\sigma_y\otimes\sigma_y)R_{\mathcal{E}}(\sigma_y\otimes\sigma_y)^\dagger] + [(\sigma_z\otimes\sigma_z)R_{\mathcal{E}}(\sigma_z\otimes\sigma_z)^\dagger]\}.$$

This corresponds to a "Bell twirling," and the resultant quantum operation is represented by a Bell diagonal state, which is a mixture of the four Pauli transformations. Hence by adding 75% noise, *any* trace-preserving single-qubit operation may be taken to a probabilistic mixture of Clifford group operations, and so any machine consisting of {CNOT+single-qubit gates} has a classical noise tolerance of at most 75% on the single-qubit gates.

V. INTERPRETATION OF THE BOUNDS

The bounds derived in the previous sections give upper bounds to the fault tolerance of specific gates. For example, in the case of the gate set {Clifford unitaries, $\pi/8$ gate}, they show that no fault-tolerant encoding can be found that protects against 14.64% *general* single-gate noise. However, this does not mean that specific forms of noise cannot be tolerated to greater than 14.64%, but one must construct protection methods that specifically target that form of noise.

Furthermore, in the case of the approach based upon the Clifford group, our results show that if the Clifford gates in a gate set are noiseless, then the noise level corresponding to Lemma 1 may not be tolerated on an additional non-Clifford gate $U(\theta)$. However, it is possible that by mixing noise in with the Clifford gates as well, and not imposing that they be noiseless, one can recover the power to do universal quantum computation. Indeed, we have been able to construct examples where mixing a certain type of noise to the gate U from a universal set {Clifford unitaries, U} leads to classically tractable evolution, but mixing the same noise [21] with the Clifford gates as well as U restores the ability to perform universal quantum computation. Although we do not include the details here, the examples that we have are all quite extreme, and work because noise that turns the non-Clifford gate U into a Clifford operation can also take the Clifford unitaries *out* of the Clifford group [22]. Nevertheless, in these examples the methods that restore universality are very specific, and cannot be used to tackle general noise of the same level.

VI. CONCLUSIONS

We have presented a class of operations—the bientangling operations—that may be efficiently simulated classically, as they are only capable of generating two-party entanglement. In some situations this class of operations may give tighter bounds than currently known on the classical noise tolerance of quantum gates. One example is the case of depolarizing noise on the CNOT gate, for which we show that 67% noise is sufficient to make the subsequent evolution efficiently tractable classically, compared to the best previous bound of 74%. Another extreme case is with measurement-based computation, where we observe that two-qubit nondegenerate measurements cannot enable exponential speedup over classical computation. It may be difficult to extend the class of bientangling operations and still generate a class that is efficiently tractable. This is because any natural generalizations to higher numbers of input particles enable perfect quantum computation, and any extensions that still involve two-particle gates are hampered by the subtle interplay between separability-preserving and separable gates.

In the second half of this work we turn to bounds on classical tolerance that may be derived from the Gottesman-Knill theorem. The subsequent bounds (e.g., 30% depolarizing noise on the $\pi/8$ gate, 14.64% for general single-gate noise) can be relatively low for this kind of approach.

In general it is quite likely that the bounds derived here may be improved. One interesting possibility is that a hybrid of the approaches used by [3,4] may be used to understand when slightly nonseparable gates may be efficiently simulated classically, albeit with a noise model more in the spirit of [3,5], where noise is applied to every qubit at every time step.

In terms of the Clifford-gate-based work, it seems quite possible that if the recent conjecture of Bravyi and Kitaev [6] is true, then gates of the form $U(\theta)=|0\rangle\langle 0|+\exp(i\theta)|1\rangle\langle 1|$ can indeed be used for quantum computation up to the noise levels derived here (and implied by their work). Their conjecture implies that a supply of single-qubit quantum states from outside the octahedron O may be "purified" to certain "magic" pure states by the use of Clifford operations only. As Clifford operations may be made fault tolerant to some degree via encoding schemes based on Clifford operations only (see, e.g., [12] and references therein), it may be pos-

sible that the noise levels that we have derived may indeed be tolerated as long as the remaining Clifford operations act within their own (potentially much tighter) fault-tolerant threshold. The Bravyi-Kitaev conjecture has recently been (partially) proven along "the Hadamard directions" [7], which include the direction relevant for the $\pi/8$ gate. Therefore it seems to be reasonable to suppose that 14.64% really is the exact probabilistic noise level that may be tolerated on the $\pi/8$ gate, as long as the remaining Clifford operations are sufficiently error-free.

These results show the potential of analyzing classical tractability with the aim of bounding from above fault-tolerance thresholds. Moreover, investigating the quantum-classical computational transition for (noisy) quantum evolution is important in its own right [3,6], particularly as there is the possibility of "intermediate" quantum computation. It may well be the case that noisy quantum devices cannot be simulated efficiently classically, yet cannot be used for fault-tolerant quantum computation. This would imply the existence of an intermediate physical device—such as a noisy quantum system controlled by a universal classical computer—which is clearly universal for computation, is better than classical as it can simulate itself efficiently, and yet is not as powerful as a full quantum computer. Such intermediate devices may be easier to construct, and hence may provide a more achievable experimental target.

ACKNOWLEDGMENTS

We thank Koenraad Audenaert and Terry Rudolph for interesting discussions, and Ben Reichardt for sending us the results of [7] prior to electronic publication. We acknowledge financial support by the U.S. Army through Grant No. DAAD 19-02-0161, The Nuffield Foundation, the Royal Society Leverhulme Trust, the Royal Commission for the Exhibition of 1851, the EPSRC QIP-IRC, and the EU Thematic Network QUPRODIS.

APPENDIX

In this appendix we calculate the minimal error rate required to take the CNOT gate into a bientangling operation, under constraints upon the form of noise other than the depolarizing model considered in Sec. III. These calculations have been placed in this appendix, as the bounds derived at best match the bounds derived in [4]. The intuitive reason for this is that two-qubit unitary operations are maximally entangled across the EB splitting (see Fig. 1), whereas they are not always maximally entangled across the other splittings. Therefore one expects that the addition of EB operations to separable and separable+swap operations might not lead to improved bounds. However, this intuition is not entirely valid, as we are also taking the convex hull after including the EB operations, and indeed for the depolarizing noise considered earlier we do obtain a large improvement. Nevertheless, for the noise forms considered in this appendix the intuition does appear to be correct.

1. No constraints

In this case we need only restrict the λ_e's to be a probability distribution, and do not need to further constrain them. Take $\lambda_0^{\mathrm{opt}}(B)$ to be the maximal possible λ_0 over all bientangling states invariant under the symmetry group (6). Then we clearly have that

$$(1-p)+p\lambda_0(\mathcal{N}) \leqslant \lambda_0^{\mathrm{opt}}(B) \tag{A1}$$

and hence as p, $\lambda_0 \geqslant 0$ we have that

$$(1-p) \leqslant \lambda_0^{\mathrm{opt}}(B) \Rightarrow p \geqslant 1-\lambda_0^{\mathrm{opt}}(B). \tag{A2}$$

This lower bound can be attained as we are free to choose the form of the noise as we wish. Hence $p_{\min}=1-\lambda_0^{\mathrm{opt}}$, and our task is now to calculate λ_0^{opt}. This is now an easier problem, as the fact that the set of bientangling states is the convex hull of separable, separable+swap, and EB states means that

$$\lambda_0^{\mathrm{opt}}(B) = \max\{\lambda_0^{\mathrm{opt}}(S), \lambda_0^{\mathrm{opt}}(SS), \lambda_0^{\mathrm{opt}}(EB)\} \tag{A3}$$

where $\lambda_0^{\mathrm{opt}}(S)$, $\lambda_0^{\mathrm{opt}}(SS)$, and $\lambda_0^{\mathrm{opt}}(EB)$ are the maximal possible λ_0's over separable states, separable+swap states, and EB states, respectively. This means that to work out the minimal generic noise required to turn the CNOT gate into a bientangling gate, we simply need to separately calculate the minimal noise required to take the CNOT gate into the different classes of separable, separable+swap, and EB states, and take the lowest value. As each of these classes separately corresponds to separability across a particular partition of the parties in the Jamiolkowski state, we can apply the techniques developed in [4]. Although we omit the details, it turns out that the Jamiolkowksi state representing the CNOT gate has only one ebit of maximal entanglement across the $(A1B1)$-$(A2B2)$ splitting or the $(A1B2)$-$(A2B1)$ splitting, but as with any two-qubit unitary has a full two ebits of maximal entanglement across the $(A1A2)$-$(B1B2)$ splitting. Hence the CNOT gate is less robust to noise across the separable–separable+swap splittings. Furthermore, the results of [4,23] show that the minimal noise that breaks the entanglement of the CNOT gate across the relevant splitting can always be chosen to be separable across that splitting. The result of all these observations is that the bounds derived in [4] for generic noise are also optimal when considering BE-machines as the classically tractable set, leading to an upper bound of 50% on the classical tolerance of a CNOT gate. It is also interesting to note that if we do not ask for the noise to take us into the bientangling set, but instead ask to be taken into the entanglement-breaking channels, then the above approach yields a weaker upper bound of 75% for *all* unitary gates, not just the CNOT [24].

2. Separable noise, separable+swap noise, and noise that is a mixture of separable and separable+swap

The previous section points out that by the arguments of [4,23], the minimal generic noise that turns the CNOT gate into a bientangling gate can always be taken to be separable, or separable+swap. Hence the bounds derived in [4] are also optimal with respect to these forms of noise, and where the classically tractable set is the set of BE-machines.

[1] L. Valiant, SIAM J. Comput. **31**, 1229 (2002); B. M. Terhal and D. P. Divincenzo, Phys. Rev. A **65**, 032325 (2002); E. Knill, e-print quant-ph/0108033; S. Bravyi, e-print quant-ph/0404180.

[2] R. Jozsa and N. Linden, e-print quant-ph/0201143; G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).

[3] D. Aharonov and M. Ben-Or, e-print quant-ph/9611029; D. Aharonov, M. Ben-Or, R. Impagliazzo, and N. Nisan, e-print quant-ph/9611028. See also D. Aharonov, Phys. Rev. A **62**, 062311 (2000) for related work.

[4] A. Harrow and M. Nielsen, Phys. Rev. A **68**, 012308 (2003).

[5] A. Razborov, e-print quant-ph/0310136.

[6] S. Bravyi and A. Kitaev, e-print quant-ph/0403025.

[7] B. W. Reichardt, e-print quant-ph/0411036.

[8] E. M. Rains, Phys. Rev. A **60**, 173 (1999); **60**, 179 (1999).

[9] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997. For recent improvements see also S. Aaronson and D. Gottesman, e-print quant-ph/0406196.

[10] The *Clifford group* is the set of unitaries U that by conjugation map tensor products of Pauli operators to tensor products of Pauli operators, i.e., we always have $U(\sigma_i \otimes \sigma_j \otimes \cdots)U^\dagger = (\sigma_m \otimes \sigma_n \otimes \cdots)$, where the σ are Pauli operators.

[11] For example, it can be shown that the W class of entangled pure states cannot be created by Clifford operations from computational basis inputs. The W class represents an important form of three-party entanglement, as defined by W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

[12] Definitions of all gates in this paper, as well as a good review of the stabilizer formalism, may be found in the textbook by M. Nielsen and I. Chuang, *Quantum Information and Quantum Computation* (Cambridge University Press, Cambridge, U.K., 2001).

[13] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).

[14] A. S. Holevo, Russ. Math. Surveys **53**, 1295 (1999).

[15] D. W. Leung, Int. J. Quantum Inf. **2**, 33 (2004).

[16] D. Gottesman and I. Chuang, Nature (London) **402**, 390 (1999).

[17] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).

[18] In fact the quantum operation conjectured by [4] as an example of a SP operation that is not in the convex hull of separable and separable+swap operations is in fact correct. The proof works by noting that LOCC on separable and separable+swap Jamiolkowski states cannot result in entanglement between particles $A1$ and $A2$. However, the SP operation presented in [4] has this property.

[19] A. Gilchrist, N. K. Langford, and M. A. Nielsen, e-print quant-ph/0408063.

[20] D. Aharanov and M. Ben-Or, e-print quant-ph/9906129; B. M. Terhal and G. Burkard, e-print quant-ph/0402104; R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **65**, 062101 (2002); M. Nielsen and C. M. Dawson, e-print quant-ph/0405134.

[21] The term "same noise" does not have a strong meaning here, as whether one form of noise on one gate is the "same" as the form of noise on another gate strongly depends upon the precise physics of real devices. For example, the same physical source of noise, such as a fluctuating magnetic field, may affect different gates in very different ways.

[22] Of course to do this the noise itself must not be a Clifford operation, so for example dephasing cannot display this phenomenon.

[23] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999); M. Steiner, Phys. Rev. A **67**, 054305 (2003).

[24] The symmetry group (6) is local across the $(A1A2)$-$(B1B2)$ split for all unitaries, and so group averaging does not change the EB properties of any EB state. Hence in looking for the minimal noise that takes a given unitary into an EB operation, the form of the noise may be restricted to being symmetric. As any state that is averaged under (6) is automatically a valid Jamiolkowski state, we may immediately utilize the results on robustness of entanglement for density matrices, and we find that all unitaries are equally robust to being taken to an EB channel by generic noise—this is unsurprising as all unitaries have Jamiolkowski states that are maximally entangled across the EB split. We find that a minimum of $3/4=75\%$ noise is required to take a two-qubit unitary into an entanglement-breaking channel.

[25] M. Nielsen, Phys. Lett. A **308**, 96 (2003); S. A. Fenner and Y. Zhang, e-print quant-ph/0111077; S. Perdrix and P. Jorrand, e-print quant-ph/0404146.