Multipartite entanglement gambling: The power of asymptotic state transformations assisted by a sublinear amount of quantum communication

Ashish V. Thapliyal*
Department of Computer Science, University of California at Berkeley, Berkeley, California 94720, USA

John A. Smolin†
IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598, USA

(Received 29 December 2002; published 31 December 2003)

Reversible state transformations under entanglement nonincreasing operations give rise to entanglement measures. It is well known that asymptotic local operations and classical communication (LOCC) are required to get a simple operational measure of bipartite pure state entanglement. For bipartite mixed states and multipartite pure states it is likely that a more powerful class of operations will be needed. To this end more powerful versions of state transformations (or reducibilities), namely, LOCCq (asymptotic LOCC with a sublinear amount of quantum communication) and CLOCC (asymptotic LOCC with catalysis) have been considered in the literature. In this paper we show that LOCCq state transformations are only as powerful as asymptotic LOCC state transformations for multipartite pure states. The basic tool we use is multipartite entanglement gambling: Any pure multipartite entangled state can be transformed to an Einstein-Podolsky-Rosen pair shared by some pair of parties and any *irreducible m*-party pure state ($m \geqslant 2$) can be used to create any other state (pure or mixed) using LOCC. We consider applications of multipartite entanglement gambling to multipartite distillability and to characterizations of multipartite minimal entanglement generating sets. We briefly consider generalizations of this result to mixed states by defining the class of *cat-distillable states*, i.e., states from which cat states ($|0^{\otimes m}\rangle + |1^{\otimes m}\rangle$) may be distilled.

DOI: 10.1103/PhysRevA.68.062324 PACS number(s): 03.67.−a

INTRODUCTION

Entanglement is a fundamental aspect of quantum mechanics. It has been found useful for various information processing tasks such as teleportation [1], superdense coding [2], entanglement assisted classical and quantum communication [3,4], quantum algorithms [5], and quantum cryptography [6]. Because of its fundamental role in quantum theory and its use as a resource in quantum information processing, it is important to quantify it.

An operational way to quantify entanglement is to study reversible state transformations induced by entanglement nonincreasing operations [7]. For bipartite pure states it is well known that asymptotic local operations and classical communication (LOCC) are required to get a simple operational measure of bipartite pure state entanglement. However, bipartite mixed state and multipartite entanglement (pure and mixed state) are not completely understood. For example, several different measures of entanglement are known for bipartite mixed states: The entanglement of formation, distillable entanglement [8,9], and relative entropy of entanglement [10]. Further, it has been proved [11,12] that under asymptotic LOCC state transformations, the amount of Einstein-Podolsky-Rosen (EPR) pairs required to create certain bound entangled [13] states cannot be recovered again, thus showing that reversible asymptotic LOCC state transformations do not give us a simple measure of entanglement in general. Thus, for bipartite mixed states and multipartite states a more powerful class of operations will be needed to quantify entanglement using the idea of reversible state transformations under entanglement nonincreasing operations. To this end Bennett *et al.* [7] have defined more powerful, yet reasonable versions of state transformations (or reducibilities), namely, LOCCq (asymptotic LOCC with a sublinear amount of quantum communication) and CLOCC (asymptotic LOCC with catalysis). In this paper we look at LOCCq state transformations and show that LOCCq state transformations are only as powerful as asymptotic LOCC state transformations for multipartite pure states.

The paper is organized as follows. In Sec. I we consider a generalization of entanglement gambling [8] from two parties to multiple parties: Any pure multipartite entangled state can be transformed to an EPR pair shared by some pair of parties and that any nontrivial *m*-party ($m \geqslant 2$) pure state can be used to create any other state (pure or mixed), using only LOCC. This is the basic tool we use to prove our main result in Sec. II. Finally, in Sec. III we look at some applications of multipartite entanglement gambling to distillability and characterizations of minimal entanglement generating sets. We also consider generalizing our main results to mixed states, by defining the class of *cat-distillable states*. Here *m*-partite cat states are states like ($|0^{\otimes m}\rangle + |1^{\otimes m}\rangle$) and cat-distillability means the possibility of obtaining cat states from a given state using asymptotic LCC state transformations.

I. MULTIPARTITE ENTANGLEMENT GAMBLING

Bennett, Bernstein, Popescu, and Schumacher introduced the idea of bipartite entanglement gambling in Ref. [8]. It involves the production of an EPR pair ($\Xi = |00\rangle + |11\rangle$) with a nonzero probability using local operations and classi-

*Also at Mathematical Sciences Research Institute, Berkeley, CA, USA; electronic address ash@msri.org, thaps@cs.berkeley.edu
†Electronic address: smolin@watson.ibm.com

cal communication (LOCC), starting from any other entangled pure state. Let us review the bipartite entanglement gambling protocol. Consider an arbitrary entangled pure state Ψ shared by A and B. It is well known that a bipartite pure state can always be written in a Schmidt decomposition

$$|\Psi\rangle=\sum_{i=1}^{k} a_i|i^A i^B\rangle, \tag{1}$$

where $k\geqslant 2$ and $a_i>0$ since the state is entangled. $|i^A\rangle$ form an orthonormal basis for A and $|i^B\rangle$ form an orthonormal basis for B. Now A and B can apply the local projectors $P^{A/B}=|0^{A/B}\rangle\langle 0^{A/B}|+|1^{A/B}\rangle\langle 1^{A/B}|$ on their halves of the state. This produces state

$$\psi_1=c|00\rangle+d|11\rangle$$

with probability $p=a_1^2+a_2^2$, where

$$c=\frac{a_1}{p} \text{ and } d=\frac{a_2}{p}.$$

Then Alice applies the local quantum operation given by the completely positive map with elements[1]

$$A_1=d|0\rangle\langle 0|+c|1\rangle\langle 1|,$$

$$A_2=\sqrt{1-d^2}|0\rangle\langle 0|+\sqrt{1-c^2}|1\rangle\langle 1|,$$

then the outcome corresponding to A_1 gives an EPR pair with probability $2c^2d^2$. Thus the total success probability for the whole process is $(2a_1^2a_2^2)/(a_1^2+a_2^2)$ which is nonzero. Thus any pure bipartite entangled state can be converted to an EPR pair with non-zero probability. Note that the success or failure of the transformation is reported to us as classical information about which outcome actually occurs.

Let us now write the above result in the notation for state transformations used by Ref. [7].[2] We first need to briefly review the notation. We start with state transformations for one copy of a state involving probabilistic outcomes, where the procedure may fail some of the time but we know when it fails. This is known as a stochastic state transformation.

We say a state Ψ is *stochastic LOCC transformable* to Φ with yield p, written as $\Psi\rightarrow_{\mathrm{LOCC}}\Phi^{\otimes p}$ (or simply as $\Psi\rightarrow\Phi^{\otimes p}$) if and only if

$$\exists\,\mathcal{L}, \quad \text{such that } \Phi=\frac{\mathcal{L}(\Psi)}{\mathrm{tr}\mathcal{L}(\Psi)}, \tag{2}$$

where $\mathcal{L}$ is a multilocally implementable quantum operation[3] such that $\mathrm{tr}\mathcal{L}(\Psi)=p$. This means that a copy of Φ may be obtained from a copy of Ψ with probability p by LOCC operations. When $p=1$ the transformation is said to be exact. Again, here the success or failure of the transformation is reported as classical information. Let $\mathcal{E}_2$ denote the set of bipartite pure entangled states, then the bipartite entanglement gambling result can be expressed as

$$\forall\,\psi\in\mathcal{E}_2, \quad \exists\ \ p>0, \quad \psi\rightarrow\Xi^{\otimes p}. \tag{3}$$

Here Ξ represents an EPR pair.

A generalized version of stochastic transformations is obtained if we allow a finite number of copies of the source and target states. We say state Ψ is multicopy stochastic LOCC transformable to state Φ with yield p, written as $\Psi\rightarrow_{\mathrm{LOCC}}\Phi^{\otimes p}$ (or simply as $\Psi\rightarrow\Phi^{\otimes p}$), if and only if

$$\exists\ \mathcal{L},m,n, \quad \text{such that } \Phi^{\otimes n}=\frac{\mathcal{L}(\Psi^{\otimes m})}{\mathrm{tr}\mathcal{L}(\Psi^{\otimes m})}, \tag{4}$$

where $\mathcal{L}$ is a multilocally implementable quantum operation such that $\mathrm{tr}\mathcal{L}(\Psi)=pm/n$. This means that n copies of Φ may be obtained from m copies of Ψ with yield p per copy by LOCC operations. Again, here the quantum operation must tell us whether the transformation succeeded or failed. Let us return to bipartite entanglement gambling again. It gives us an EPR pair with positive probability starting from any entangled pure state. Since EPR pairs can be used in a teleportation protocol to create an arbitrary bipartite state, clearly any bipartite pure entangled state may be converted to any other bipartite state with a positive probability. Notice that this protocol will in general require multiple copies of the source state since the target state may be a state with higher Schmidt number. Thus a stronger version of bipartite gambling can be written using the language of multicopy stochastic state transformations as

$$\forall\ \ \psi\in\mathcal{E}_2, \quad \exists\ \ p>0,\psi\twoheadrightarrow\phi^{\otimes p}, \tag{5}$$

where $\mathcal{E}_2$ denotes the set of bipartite pure entangled states and ϕ is any bipartite state, pure or mixed.

Now let us consider the multiparty scenario: There are m parties ($m\geqslant 2$) labeled as $\{1,2,\ldots,m\}$. Given a nontrivial subset X of the parties and its complement $\overline{X}$, we say that $\{X,\overline{X}\}$ defines a *cut* between X and $\overline{X}$. We say that pure state Ψ is *factorizable* across the cut $\{X,\overline{X}\}$ if Ψ can be written as a tensor product of two states, one with the parties in set X and the other with the parties in the complement $\overline{X}$, i.e., $\Psi=\phi^X\otimes\psi^{\overline{X}}$. We say that a pure state is *entangled* if it is not factorizable across some cut, or equivalently, a separable

[1]This map can be physically implemented by Alice teleporting half of the given state through a non–maximally entangled pure state $d|00\rangle+c|11\rangle$ in her lab.

[2]In Ref. [7] state transformations are also called as reducibilities: If ψ is transformed to ϕ we can say that the problem of creating ϕ is reducible to the problem of creating ψ. This provides the intuition behind the name reducibility. In this paper we will use the state transformations language instead of reducibilities.

[3]A multilocally implementable quantum operation is a representation of a multipartite LOCC protocol as a completely positive linear map.

pure state is factorizable across all cuts.[4] We define a pure state to be *irreducible* if it is not factorizable across any cut. Thus an irreducible m-party pure state captures the notion of a true m-party state.

It turns out that for multiple parties, gambling can be generalized in different ways. First we generalize the weaker result shown in Eq. (3). In this case we show that an entangled pure multipartite state can be transformed under LOCC to an EPR pair between some pair of parties. We write this as a lemma.[5]

Lemma 1. If state Ψ is an m-partite pure state that is entangled across the cut $\{\{i_1\},\{i_2,i_3,\ldots,i_m\}\}$ then there exists $p>0$ and two parties, say P_1 and P_2, such that

$$\Psi \rightarrow (\Xi^{P_1P_2})^{\otimes p}, \tag{6}$$

where $\Xi^{P_1P_2}$ represents an EPR pair shared by parties P_1 and P_2.

Proof. We argue by induction on the number of parties m. The first nontrivial case is when $m=2$. Here the entanglement gambling protocols we discussed in the Introduction guarantee the result. So let us assume that the result is true for $m<k$. We need to prove that it is true for $m=k>2$. For this we will use the idea of entanglement of assistance [15]. We let $A=i_1$ be the helper, $B=i_2$ be the first party, and $\{i_3,i_4,\ldots,i_m\}=C$ be the (composite) second party. Consider the entanglement of assistance of ρ^{BC}. If it is zero then the result on zero entanglement of assistance from Ref. [15] implies that either $\rho^{BC}=\rho^B\otimes|\psi^C\rangle\langle\psi^C|$ or $\rho^{BC}=|\psi^B\rangle\langle\psi^B|\otimes\rho^C$. Then either $\Psi=\psi^{AB}\otimes\psi^C$ or $\Psi=\psi^{AC}\otimes\psi^B$. In the first case, since Ψ was entangled across the partition $\{\{i_1\},\{i_2,i_3,\ldots,i_m\}\}$, ψ^{i_1,i_2} has to be entangled, thus reducing it to the bipartite case. Similarly, for the second case $\psi^{i_1,i_3,\ldots,i_m}$ must be entangled across the cut $\{\{i_1\},\{i_3,\ldots,i_m\}\}$, which by the induction hypothesis can give an EPR pair between some two parties. If the entanglement of assistance is not zero, then A can help B and C to get (with finite probability) an entangled state ψ^{BC}, i.e., state $\psi^{i_2,i_3,\ldots,i_m}$ that is entangled across the partition $\{\{i_2\},\{i_3,\ldots,i_m\}\}$. This, by the induction hypothesis, can give an EPR pair between some two parties. Thus the result is proved.

Note that the result does not require multiple copies of the starting state. For proving the above result we used the necessary and sufficient condition for a state to have zero entanglement of assistance. It is quite reasonable that the entanglement of assistance would be useful for a multipartite scenario, since the motivation for it relies on a three-party scenario.

Now we generalize the stronger version of bipartite entanglement gambling shown in Eq. (4). The generalization involves showing that any irreducible m-party state can generate any other m-party state (pure or mixed) with positive probability using the multicopy stochastic LOCC operations. We prove this by showing that we can get an EPR pair between every pair of parties from any irreducible m-partite pure state. Then using teleportation, any other state can be generated from these EPR pairs. We state this result below.

Theorem 1. If state Ψ is an irreducible m-partite state then for any two parties say P_1 and P_2 there exists $p>0$, such that

$$\Psi \twoheadrightarrow (\Xi^{P_1P_2})^{\otimes p}, \tag{7}$$

where $\Xi^{P_1P_2}$ represents an EPR pair shared by parties P_1 and P_2.

Proof. To prove this we argue by induction on the number of parties m. The first nontrivial case is when $m=2$. Since the state is irreducible, it is an entangled bipartite state and we get the result directly from Lemma 1. Assuming the result to be true for $m<k$, we show that it is true for $m=k$. Since Ψ is irreducible, by Lemma 1 we can stochastically get an EPR pair between some two parties, say, A and B. If these two are the required parties P_1 and P_2 then we are done. Otherwise by teleportation through these EPR pairs, the parties A and B can implement any operation they could if they were in the same lab. Thus we can look on them as forming a composite party, say, $\tilde{A}$. Then we have reduced the problem to the $m=k-1$ partite case, thus proving the result.

II. THE POWER OF A LITTLE QUANTUM COMMUNICATION

In this section we will define the notions of asymptotic LOCC and LOCCq state transformations and then prove the main result: For pure states asymptotic LOCCq transformations are only as powerful as asymptotic LOCC transformations.

We first consider asymptotic LOCC state transformations. State Ψ is said to be *asymptotically LOCC transformable* to state Φ, written as $\Psi \rightsquigarrow_{\mathrm{LOCC}} \Phi$, or simply as $\Psi \rightsquigarrow \Phi$, if and only if

$$\forall\ \delta>0, \quad \epsilon>0 \exists\ n,n',\mathcal{L},$$
$$|(n'/n)-1|<\delta, \quad F(\mathcal{L}(\Psi^{\otimes n}),\Phi^{\otimes n'})\geqslant 1-\epsilon. \tag{8}$$

Here $\mathcal{L}$ is a multilocally implementable superoperator that converts n copies of Ψ into a high fidelity approximation to n' copies of Φ. We will refer to the condition on n and n' as the δ-condition and the condition on the fidelity as the ϵ-condition. Note that the δ-condition says that the n and n' can differ only sublinearly with n for large n. Thus asymptotic reducibility captures the possibility of state transformations as the number of source and target copies tends to infinity, allowing a little imperfection and a little loss. Asymptotic reducibilities can have noninteger yields. This can be expressed using tensor exponents that take on any non-negative real value, so that $\Psi^{\otimes y} \rightsquigarrow \Phi^{\otimes x}$ denotes

$$\forall\ \delta>0,\ \epsilon>0, \quad \exists\ n,n',\mathcal{L},$$
$$|(n'/n)-x/y|<\delta, \quad F(\mathcal{L}(\Psi^{\otimes n}),\Phi^{\otimes n'})\geqslant 1-\epsilon. \tag{9}$$

[4] In fact, any state (pure or mixed) which is factorizable across all cuts is separable since it has to be of the form $\rho=\rho_1\otimes\rho_2\otimes\cdots\otimes\rho_m$. A (fully) separable mixed state is a correlated mixture of separable pure states $\rho=\Sigma_i p_i \rho_{i_1}\otimes\rho_{i_2}\otimes\cdots\otimes\rho_{i_m}$.

[5] This lemma was independently proved in [14].

In this case we say x/y is the asymptotic efficiency or yield with which Φ can be obtained from Ψ. Note that if $\psi \twoheadrightarrow \phi^{\otimes p}$ then $\psi \rightsquigarrow \phi^{\otimes p}$ because of the concentration results for the binomial distribution with probability p of success.[6] This justifies the notation used while writing the stochastic state transformations. In our proof of the main result, we will only consider transformations with unit yield for simplicity. The extension of the result to noninteger yields is trivially obtained by replacing the unit yield by any arbitrary yield.

A stronger version of asymptotic state transformations is obtained if we allow a sublinear amount of quantum communication during the transformation process in addition to the LOCC operations. This is called as an asymptotic LOCCq state transformation. We say state Ψ is asymptotically LOCCq transformable to state Φ, written as $\Psi \rightsquigarrow_{\mathrm{LOCCq}} \Phi$ (or simply $\Psi \rightsquigarrow_{\mathrm{q}} \Phi$), if and only if

$$\forall\ \delta>0,\ \epsilon>0\ \exists\ n,k,\mathcal{L},$$

$$(k/n)<\delta, \quad F(\mathcal{L}(\Gamma^{\otimes k}\otimes\Psi^{\otimes n}),\Phi^{\otimes n})\geqslant 1-\epsilon, \qquad (10)$$

where $\Gamma=|0^{\otimes m}\rangle+|1^{\otimes m}\rangle$ denotes the m-partite cat state. The m-partite cat states used here are a convenient way of allowing a sublinear amount, $o(n)$ of quantum communication, since they can be used as described in [7] to generate EPR pairs between any two parties, which in turn can be used to teleport quantum data between the parties. The $o(n)$ quantum communication allows the definition to be simpler in one respect: A single tensor power n can be used for the input state Ψ and output state Φ, rather than the separate powers n and n' used in the definition of ordinary asymptotic LOCC reducibility without quantum communication, because any $o(n)$ shortfall in number of copies of the output state can be made up by using the cat states to synthesize the extra output states *de novo*. This definition is more natural than that for ordinary asymptotic LOCC reducibility in that the input and output states are allowed to differ in any way that can be repaired by an $o(n)$ expenditure of quantum communication, rather than only in the specific way of being n versus n' copies of the desired state where $n-n'$ is $o(n)$. For an arbitrary yield y, we just change $\Phi^{\otimes n}$ to $\Phi^{\otimes\lfloor yn\rfloor}$ in the ϵ-condition of the above definition.

Clearly $\rightsquigarrow_{\mathrm{LOCC}}$ implies $\rightsquigarrow_{\mathrm{LOCCq}}$ because as discussed above asymptotic LOCC state transformation is a special case of LOCCq state transformations. An important question is whether LOCCq state transformations are stronger. It turns out that LOCCq state transformations are not stronger than asymptotic LOCC for pure states. This constitutes our main result.

We start by showing that under asymptotic LOCCq state transformations a state that is factorizable across some cut can only give rise to states that are factorizable across that cut. We prove this in the following lemma.

Lemma 2. Given state Ψ that is factorizable across the partition $\{X,\overline{X}\}$ and that $\Psi \rightsquigarrow_{\mathrm{LOCCq}} \Phi$, then Φ must be factorizable across the same partition.

Proof. This is essentially a two party problem, with X and $\overline{X}$ as the two compound parties. We argue by contradiction. Suppose Φ was nonfactorizable across the partition $\{X,\overline{X}\}$ with bipartite entanglement $x>0$. Then n copies of Φ would have a linear amount nx of bipartite entanglement across the partition. However, since Ψ has no entanglement across the partition and since LOCCq protocols only allow a sublinear $[o(n)]$ amount of m-partite cat states along with LOCC, they cannot increase the entanglement across the cut by a linear amount. Thus, no asymptotic LOCCq protocol can give rise to Φ starting from Ψ.

Now we prove that for irreducible pure states, asymptotic LOCCq and asymptotic LOCC are equally powerful.

Lemma 3. For an irreducible m-partite pure state Ψ and any arbitrary state Φ,

$$\Psi \rightsquigarrow_{\mathrm{LOCCq}} \Phi \Leftrightarrow \Psi \rightsquigarrow_{\mathrm{LOCC}} \Phi. \qquad (11)$$

Proof. Since Ψ is irreducible, it is cat distillable from theorem 1. Hence we can use $o(n)$ copies of Ψ to generate $o(n)$ copies of the m-partite cat state by LOCC, which we can use for the $o(n)$ quantum communication required for LOCCq. Since only $o(n)$ extra copies of Ψ are required than the LOCCq protocol, this does not change the yield asymptotically, and hence the LOCCq protocol can be simulated by an LOCC protocol. This proves the result.

Now we are ready to combine the results from the above lemmas to prove the general result as the theorem below.

Theorem 2. For m-partite pure states Ψ and Φ,

$$\Psi \rightsquigarrow_{\mathrm{LOCCq}} \Phi \Leftrightarrow \Psi \rightsquigarrow_{\mathrm{LOCC}} \Phi. \qquad (12)$$

Proof. We argue by induction on the number of parties m. Consider the first nontrivial case $m=2$. If Ψ is irreducible, then Theorem 1 along with Lemma 3 gives us the result. If Ψ is factorizable, in this case a product state, then by Lemma 2, Φ must be a product state too and thus can be created trivially by LOCC operations. Now let the theorem be true for all $m<k$, then we show that it is true for $m=k$. If Ψ is irreducible, then Theorem 1 along with Lemma 3 gives us the result. Otherwise Ψ is factorizable across some cut $\{X,\overline{X}\}$. Then Lemma 2 implies that Φ is factorizable across

[6] We outline the proof for the single copy stochastic transformations. The multicopy case is similar. We start with n copies of state Ψ and to each we apply the stochastic state transformation. We want $n'=(1-n^{-1/3})np$ copies of Φ which gives the required asymptotic yield p. Let X be the number of successful stochastic transformations. When we have $X\geqslant n'$ then we declare it a success and keep only n' of these and the output is $\rho_s=\Phi^{\otimes n'}$; otherwise we output some unentangled state, say, ρ_f. Thus the output density matrix is $\mathcal{L}(\Psi^{\otimes n})=\rho=p_s\rho_s+p_f\rho_f$, where p_s/p_f is the probability of success/failure. Now, the fidelity of the output is $F(\rho,\Phi^{\otimes n'})\geqslant p_sF(\rho_s,\Phi^{\otimes n'})\geqslant 1-\exp(n^{1/3}p/2)$, using the Chernoff bound $\mathrm{Prob}[X<(1-\Delta)\mu]<\exp(-\mu\Delta^2/2)$, μ being the expectation of X. By choosing n large enough the fidelity can be made arbitrarily good, as required for the ϵ-condition. Also note that $|n'/n-p|=p/n^{1/3}$ which can also be made arbitrarily small by choosing large n, thus satisfying the δ-condition. Since both the ϵ and δ-condition can be satisfied by making n large enough, they can be simultaneously satisfied, thus giving the result.

the same cut, i.e., $\Phi = \phi_1^X \otimes \phi_2^{\bar{X}}$. Applying this theorem for $m<k$, to the states ϕ_1^X and ϕ_2^X we have the result.

Thus we have shown that asymptotic LOCC and LOCCq state transformations are equivalent for pure states. Let us now turn our attention to an application of entanglement gambling to multipartite distillability.

III. ENTANGLEMENT GAMBLING AND MULTIPARTITE DISTILLABILITY

In this section we will briefly study some implications of the entanglement gambling result to the notion of distillability in multipartite systems. Distillation of multipartite entanglement has already been considered in Refs. [16–18], but the issues we discuss here are related to the definitions of distillability, rather than actual distillation protocols.

Since there are many different kinds of entanglement for three or more parties, one of the main problems with defining multipartite distillable entanglement is that it is not possible to maximize over the yield of all those states, since one kind of entanglement can in general be traded for another. However, we may easily generalize the notion of distillability from the bipartite scenario to get the following general definition of distillability: We say ρ is *distillable* if and only if we can asymptotically transform it to a pure entangled state with a nonzero yield. In symbols $\rho \rightsquigarrow \Psi^{\otimes x}$ for some positive x, where ψ is some entangled pure state.

However it is more useful to have EPR pairs or cat states as the target state to be produced in the distillation procedure, since they can then directly be used for other information processing tasks. Thus, one may define EPR distillability as: We say ρ is EPR-*distillable* if and only if $\rho \rightsquigarrow \Psi^{\otimes x}$ for some positive x, where Ψ is an EPR pair between some pair of parties. Similarly, one may define cat distillability except the target state Ψ is now required to be an m-partite cat state for m parties.

The relation between general distillability, EPR and cat-state distillability is an interesting issue. In the bipartite case, since any pure entangled state can be converted to an EPR pair, it turns out that EPR distillability and distillability are identical. A natural question is whether this property is true for multipartite states too.

Clearly if a state is EPR distillable then it is distillable since it can be asymtpotically converted to an entangled pure state, namely, the EPR pair. Then the question remains about whether distillability implies EPR distillability. To prove this it suffices to show that any entangled multipartite pure state can give some amount of EPR pairs. This is precisely the result of Lemma 1! Thus we can say that an m-partite state ρ is distillable if and only if it is EPR distillable.

On the other hand, if a state is cat distillable it is also distillable and EPR distillable, however the converse is not true in general. Cat-state distillable states are interesting because they can generate all other states and hence form a minimal entanglement generating set, that is, a minimal set of states that can generate any other state under asymptotic LOCC. Since the reversibility of the state transformations is not required, this is a very coarse-grained entanglement measure. Let us consider a state that is factorizable across some cut of parties $\{X,\bar{X}\}$. Then it cannot be cat-state distillable because that would imply that a separable bipartite state can be made into an entangled one with LOCC operations, which we know is impossible. Thus only irreducible states can be cat distillable. Then Lemma 1 shows that any irreducible pure state is cat distillable. Putting these together we see that a pure state is cat distillable if and only if it is irreducible. But dropping the requirement of reversibility still gives a qualitative broad picture of multipartite entanglement. This is analogous to classifying bipartite mixed states as distillable and undistillable to get a coarse-grained measure of distillable entanglement. In this light, the result is very satisfying because it says that if we allow ourselves to waste entanglement during transformation of states, then any irreducible state is equivalent to any other, and is more powerful entanglementwise than any factorizable state, thus giving a hierarchy of qualitatively different entangled states which factorize into irreducible parts of various sizes (e.g., for three parties 3-party cat state, EPR^{AB}, EPR^{BC}, EPR^{CA}).

From the discussion above, a natural question is how to define irreducibility for mixed states and whether an irreducible mixed state is also cat-state distillable. If we define irreducibility as nonfactorizability then this obviously is false, because that would imply separable but non-factorizable bipartite states could generate entanglement, which we know cannot happen. The next thing to try is replacing the idea of factorizability with that of separability. So we say that Ψ is reducible across a partition $\{X,\bar{X}\}$ of parties if it is separable across that partition. We say a state is irreducible if it is not separable across any partition of the parties. This generalization is not useful because of the existence of bound entangled states, that is, states which are inseparable but not distillable. The final idea is that we could generalize irreducibility to mixed states using distillability across cuts: We say a state is irreducible if it is distillable across all cuts. Given this generalization of the definition, it is an open question whether cat-state distillability and irreducibility are equivalent for mixed states, because Lemma 1 does not hold for mixed states in general [19,11].

DISCUSSIONS AND CONCLUSIONS

In this paper we have shown that asymptotic LOCC and LOCCq state transformations are equally powerful for pure states. An important question is whether LOCCq is more powerful than asymptotic LOCC for mixed states. Obviously, for cat (mixed) states our result showing that the two have equal power should hold since we can use $o(n)$ cat states to achieve $o(n)$ quantum communication. Thus, the open question is mainly regarding the mixed states that are not cat distillable. This is an important future direction. One possible way to get the full mixed state result, just as we did for pure states using induction, leads to the problem of how to define irreducible mixed states such that they are cat distillable and at the same time would facilitate an inductive argument.

We have shown here that any irreducible (nonfactorizable) pure state is cat distillable, however our protocols are not very efficient, and that was not the goal either. However,

in reality, we need cat-distillation protocols that are efficient. Finding such protocols is another important future direction.

ACKNOWLEDGMENTS

A.V.T. acknowledges support from the Defense Advanced Research Projects Agency (DARPA) and the Air Force Laboratory, Air Force Material Command, USAF, under Contract No. F30602-01-2-0524, from the USA Army Research Office, under Grant Nos. DAAG-55-98-C-0041, and DAAG-55-98-1-0366, and support from IBM Research. J.A.S. acknowledges support from the USA Army Research Office, under Grant No. DAAG-55-98-C-0041.

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] C.H. Bennett, P.W. Shor, J.A. Smolin, and A.V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).
[4] C.H. Bennett, P. Shor, J.A. Smolin, and A.V. Thapliyal, IEEE Trans. Inf. Theory **48**(10), 2637 (2002).
[5] P. W. Shor, in *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, New York, 1994), pp. 124–134.
[6] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India*, (IEEE, New York, 1984), pp. 175–179.
[7] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, and A.V. Thapliyal, Phys. Rev. A **63**, 012307 (2001).
[8] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[9] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[10] V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[11] P.W. Shor, J.A. Smolin, and A.V. Thapliyal, Phys. Rev. Lett. **90**, 107901 (2003).
[12] A. Acin, G. Vidal, and J.I. Cirac, Quantum Inf. Comput. **3**, 55 (2003).
[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[14] W. Dür, Phys. Rev. Lett. **87**, 230402 (2001).
[15] D. P. DiVincenzo, C. A. Fuchs, J. A. Smolin, A. Thapliyal, and A. Uhlmann, in *Proceedings of the First NASA International Conference on Quantum Computing and Quantum Communications, Palm Springs, CA, 1998*, edited by C. P. Williams (Springer-Verlag, Heidelberg, Germany, 1999), Vol. 1509.
[16] M. Murao, M.B. Plenio, S. Popescu, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, R4075 (1998).
[17] W. Dür and J.I. Cirac, Phys. Rev. A **61**, 042314 (2000).
[18] W. Dür, J.I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
[19] J.A. Smolin, Phys. Rev. A **63**, 032306 (2001).