Many Copies May Be Required for Entanglement Distillation

John Watrous*

Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4

(Received 10 December 2003; published 1 July 2004)

A mixed quantum state ρ shared between two parties is said to be *distillable* if, by means of a protocol involving only local quantum operations and classical communication, the two parties can transform some number of copies of ρ into a single shared pair of qubits having high fidelity with the maximally entangled state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. In this Letter it is proved that there exist states that are distillable, but for which an arbitrarily large number of copies is required before any distillation procedure can produce a shared pair of qubits with even a small amount of entanglement. Specifically, for every positive integer n there exists a state ρ that is distillable, but, given n or fewer copies of ρ, every distillation procedure outputting a single shared pair of qubits outputs those qubits in a separable (i.e., unentangled) state.

DOI: 10.1103/PhysRevLett.93.010502 PACS numbers: 03.67.Mn

Introduction.—Entanglement represents an important resource in quantum information theory. For example, by means of quantum teleportation [1], entanglement shared between two parties that may send only classical information to one another allows the parties to exchange quantum information. Superdense coding [2], which allows one qubit of quantum communication to transmit two classical bits of communication using prior entanglement, is another example where entanglement is used as a resource. From the point of view of such protocols, a shared pair of qubits in the state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ (or any other maximally entangled state) represents one unit of entanglement, known as an *e-bit.* For instance, at the cost of one e-bit plus two classical bits of communication, quantum teleportation allows for the transmission of one qubit of information.

Suppose that two parties, Alice and Bob, would like to perform quantum teleportation or some other protocol based on entanglement, but instead of sharing copies of the state $|\phi^+\rangle$ they share copies of some other quantum state ρ. For instance, ρ may represent a noisy copy of $|\phi^+\rangle$ that does not allow for sufficiently accurate transmission of quantum information by Alice and Bob's standards, or ρ may be a strange quantum state that is entangled but has no resemblance whatsoever to $|\phi^+\rangle$. The process of *entanglement distillation,* first considered by Bennett *et al.* [3], addresses this situation—by means of some protocol allowing Alice and Bob to perform only local quantum operations and to communicate classically (an *LOCC protocol,* for short), some number of copies of ρ may be transformed into some (possibly smaller) number of copies of $|\phi^+\rangle$ with high accuracy. When it is possible for Alice and Bob to transform one or more copies of ρ into at least one copy of $|\phi^+\rangle$ with high accuracy in this way, ρ is said to be *distillable.*

Some states ρ are distillable and some are not. In the case where ρ is a pure, entangled state, distillation is always possible [3]; even if ρ has a very small amount of entanglement, sufficiently many copies of ρ allow copies of $|\phi^+\rangle$ to be distilled with high accuracy. Similarly, if ρ is a mixed state of exactly two qubits, ρ being distillable is equivalent to ρ being entangled [4,5]. In the general case for mixed states, however, there are examples of states that are entangled but are not distillable [6]. Such states are known as *bound-entangled states.*

All currently known examples of bound entangled states have the property that the partial transpose of the density operator of the state in question is positive semidefinite. States of this sort are called PPT (positive partial transpose) states for short. While every PPT state is undistillable, the converse is not known to hold, and it is a central open question in the theory of entanglement to determine whether or not this is the case. More generally speaking, there is no effective procedure known to determine whether a given state is distillable or not. For a certain range of parameters, Werner states have been conjectured to be examples of bound entangled non-PPT states [7,8].

Some of the difficulty in understanding entanglement distillation may be attributed to the fact that, by definition, an arbitrary number of copies of the state in question may be used in the distillation process. Suppose that instead of having an unlimited number of copies of a given bipartite state ρ, Alice and Bob have some fixed number of copies that they wish to subject to distillation. One says that ρ is *n-distillable* if there exists an LOCC protocol whereby Alice and Bob can convert n copies of ρ to a shared pair of qubits that is entangled. It should be stressed that this definition places no restriction on the amount of entanglement of the shared pair of qubits output by the procedure; it requires only that this pair of qubits are in some entangled (i.e., nonseparable) state. Note, however, that a necessary and sufficient condition for a state ρ to be distillable is that ρ is n-distillable for some n. This is because a large number of copies of ρ can be collected into groups of size n, the distillation procedure used to produce entangled pairs of qubits, then these pairs of entangled qubits further distilled using the procedure of Ref. [5]. For pure states and for mixed states on a single shared pair of qubits, distillability and 1-distillability are equivalent.

The main result of this Letter establishes that for any given value of n there exist states that are distillable but not n-distillable. This was not previously observed even for the case $n = 1$. The dimension of such states does not need to depend on n; $9 \otimes 9$ dimensions are sufficient for the existence of such states for all values of n.

Theorem 1: *For any choice of integers $d \geq 3$ and $n \geq 1$, there exists a $d^2 \otimes d^2$ bipartite mixed quantum state that is distillable but not n-distillable.*

Remark: It should be noted that for the particularly simple case of $n = 1$, this theorem follows from results proved in Ref. [9]. Specifically, it is implicit in that paper that there exist states ρ and ξ that are not 1-distillable (and, in fact, ξ is not distillable at all), but such that $\rho \otimes \xi$ is 1-distillable. Assuming without loss of generality that these are states of systems of equal size, it follows that the state $\frac{1}{2}|00\rangle\langle 00| \otimes \rho + \frac{1}{2}|11\rangle\langle 11| \otimes \xi$ is 2-distillable but not 1-distillable. A similar example can be derived from the results of Ref. [10]. It is not clear, however, that this construction can be extended beyond the case $n = 1$.

Preliminaries.—Let $\mathcal{A}$ and $\mathcal{B}$ be Hilbert spaces. A vector $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ is said to have *Schmidt rank k* if

$$\mathrm{rank}(\mathrm{tr}_{\mathcal{A}} |\psi\rangle\langle\psi|) = k,$$

where $\mathrm{tr}_{\mathcal{A}}: L(\mathcal{A} \otimes \mathcal{B}) \to L(\mathcal{B})$ denotes the partial trace. Given a linear operator $X \in L(\mathcal{A} \otimes \mathcal{B})$, the partial transpose over $\mathcal{A}$ applied to X is denoted by $T_{\mathcal{A}}(X)$. Transposition must be taken with respect to a particular basis of $\mathcal{A}$, which is always assumed to be a given standard basis in this Letter.

The following fact, first proved in Ref. [6], allows entanglement distillation to be characterized without reference to LOCC transformations. A density matrix ρ acting on $\mathcal{A} \otimes \mathcal{B}$ is 1-distillable if and only if there exists some Schmidt rank 2 vector $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ for which

$$\langle\psi|T_{\mathcal{A}}(\rho)|\psi\rangle < 0,$$

and ρ is n-distillable if $\rho^{\otimes n}$ is 1-distillable. If ρ is n-distillable for some integer $n \geq 1$, then ρ is distillable, otherwise ρ is undistillable. It is convenient that this characterization holds regardless of whether the state ρ is normalized. Consequently, normalization factors for density matrices are often ignored in this Letter.

A convention that is followed throughout this Letter is that the Hilbert space $\mathcal{A}$ always refers to Alice's part of a given system and $\mathcal{B}$ refers to Bob's part. Schmidt rank and any reference to distillation is generally with respect to this partition. Different symbols, such as $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$, etc., are used to refer to Hilbert spaces of systems not necessarily shared between Alice and Bob in this way in order to avoid confusion.

Let $\mathcal{F}$ and $\mathcal{G}$ be d-dimensional Hilbert spaces, and let $\{|1\rangle, \ldots, |d\rangle\}$ be the standard basis for both of these spaces. Four projection operators on $\mathcal{F} \otimes \mathcal{G}$ play an important role in this Letter. The first two projections are

$$P = |\Phi\rangle\langle\Phi|,$$

$$Q = I - |\Phi\rangle\langle\Phi|,$$

where

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle.$$

The other two projections are

$$R = \tfrac{1}{2}(I - F),$$

$$S = \tfrac{1}{2}(I + F) = I - R,$$

where

$$F = \sum_{1 \leq i,j \leq d} |i\rangle\langle j| \otimes |j\rangle\langle i|.$$

The projection R is the projection onto the antisymmetric subspace of $\mathcal{F} \otimes \mathcal{G}$, while S is the projection onto the symmetric subspace of $\mathcal{F} \otimes \mathcal{G}$. The following relations among these projections and the partial transpose hold:

$$T_{\mathcal{F}}(P) = -\frac{1}{d}R + \frac{1}{d}S,$$

$$T_{\mathcal{F}}(Q) = \frac{d+1}{d}R + \frac{d-1}{d}S,$$

$$T_{\mathcal{F}}(R) = -\frac{d-1}{2}P + \frac{1}{2}Q,$$

$$T_{\mathcal{F}}(S) = \frac{d+1}{2}P + \frac{1}{2}Q.$$

Proof of theorem 1: Consider a system with four d-dimensional components, two in Alice's possession and two in Bob's possession. It is convenient to refer to these systems as *quantum registers* $X_1, \ldots, X_4$ with corresponding Hilbert spaces $\mathcal{H}_1, \ldots, \mathcal{H}_4$. The standard basis for these spaces is taken to be $\{|1\rangle, \ldots, |d\rangle\}$. Later it will be necessary to consider systems with more registers, which will be labeled similarly and will have corresponding Hilbert spaces labeled similarly. In all cases, it is assumed that Alice possesses the odd-numbered registers and Bob possesses the even-numbered registers. When necessary, the tensor product structure of various operators is indicated by subscripts that index these systems. For example, the projection R on $\mathcal{H}_1 \otimes \mathcal{H}_2$

tensored with the projection S on $\mathcal{H}_3 \otimes \mathcal{H}_4$ is denoted $R_{1,2} \otimes S_{3,4}$.

Define the (unnormalized) state $\rho(\varepsilon)$ as

$$\rho(\varepsilon) = \frac{d+1+\varepsilon}{d-1} R_{1,2} \otimes R_{3,4} + S_{1,2} \otimes S_{3,4}.$$

Theorem 1 follows from these two lemmas.

Lemma 2: *For any integers $d \geq 3$ and $n \geq 1$, there exists a real number $\varepsilon > 0$ such that $\rho(\varepsilon)$ is not n-distillable.*

Lemma 3: *For every $d \geq 3$ and $\varepsilon > 0$, the state $\rho(\varepsilon)$ is distillable.*

Proof of lemma 2: Let $\mathcal{A} = \mathcal{H}_1 \otimes \mathcal{H}_3$ and $\mathcal{B} = \mathcal{H}_2 \otimes \mathcal{H}_4$. The partial transpose of $\rho(\varepsilon)$ is

$$T_{\mathcal{A}}(\rho(\varepsilon)) = \tfrac{1}{4}(\mu P \otimes P - \varepsilon P \otimes Q - \varepsilon Q \otimes P + \lambda Q \otimes Q), \tag{1}$$

where $\mu = (d+1)^2 + (d+1+\varepsilon)(d-1)$ and $\lambda = 1 + \frac{d+1+\varepsilon}{d-1}$. The partial transpose of n copies of $\rho(\varepsilon)$ can be expressed as

$$[T_{\mathcal{A}}(\rho(\varepsilon))]^{\otimes n} = \frac{1}{4^n} \sum_{x \in \{0,1\}^{2n}} \alpha(x) \Pi_x,$$

where $\Pi_0 = P$, $\Pi_1 = Q$, $\Pi_x = \Pi_{x_1} \otimes \cdots \otimes \Pi_{x_{2n}}$ for $x \in \{0,1\}^{2n}$, and each coefficient $\alpha(x)$ is easily determined by Eq. (1) above. In particular, these coefficients satisfy $\alpha(1^{2n}) = \lambda^n$, $\alpha(0^{2n}) = \mu^n$, and $|\alpha(x)| \leq \varepsilon \mu^{n-1}$ for all $x \notin \{0^{2n}, 1^{2n}\}$.

Suppose that $|\psi\rangle \in \mathcal{A}^{\otimes n} \otimes \mathcal{B}^{\otimes n}$ is a unit vector having Schmidt rank equal to 2. Then

$$\langle\psi|Q^{\otimes 2n}|\psi\rangle \geq \left(1 - \frac{2}{d}\right)^{2n}.$$

This inequality is proved in Dür *et al.* [7] for the case $d = 3$, and generalizes to arbitrary d without complications. It follows that

$$\langle\psi|T_{\mathcal{A}}(\rho(\varepsilon))^{\otimes n}|\psi\rangle \geq \frac{\lambda^n}{4^n}\left(1 - \frac{2}{d}\right)^{2n} - \varepsilon\mu^{n-1}.$$

Because λ and μ can be lower bounded and upper bounded, respectively, by positive real numbers not depending on ε, it follows that the above quantity is positive for sufficiently small $\varepsilon < 0$. For such a choice of ε, it is therefore the case that $\rho(\varepsilon)$ is not n-distillable. ∎

Proof of lemma 3: It is assumed that Alice and Bob have an unbounded supply of copies of $\rho(\varepsilon)$. Alice and Bob iterate a particular process involving eight d-dimensional registers $X_1, \ldots, X_8$ with corresponding Hilbert spaces $\mathcal{H}_1, \ldots, \mathcal{H}_8$. As before, it is assumed that Alice possesses the odd-numbered registers and Bob possesses the even-numbered registers.

Suppose at some instant that the registers $X_1, \ldots, X_4$ contain the state

$$\alpha R_{1,2} \otimes R_{3,4} + S_{1,2} \otimes S_{3,4}$$

for some $\alpha \geq 0$, while registers $X_5, \ldots, X_8$ contain a copy of $\rho(\varepsilon)$, i.e.,

$$\frac{d+1+\varepsilon}{d-1} R_{5,6} \otimes R_{7,8} + S_{5,6} \otimes S_{7,8}.$$

Alice measures the pair (X_1, X_5) with respect to the measurement described by $\{P, Q\}$, and Bob does likewise with the pair (X_2, X_6). The process being iterated fails if either of the measurement outcomes does not correspond to the projection P. In case they both obtain an outcome corresponding to projection P, they discard the registers on which they performed the measurements, which leaves the four registers (X_3, X_4, X_7, X_8) in the state

$$\begin{aligned}
&\alpha \frac{d+1+\varepsilon}{d-1} \mathrm{tr}[(P_{1,5} \otimes P_{2,6})(R_{1,2} \otimes R_{5,6})] R_{3,4} \otimes R_{7,8} + \\
&\quad \alpha\, \mathrm{tr}[(P_{1,5} \otimes P_{2,6})(R_{1,2} \otimes S_{5,6})] R_{3,4} \otimes S_{7,8} + \\
&\frac{d+1+\varepsilon}{d-1} \mathrm{tr}[(P_{1,5} \otimes P_{2,6})(S_{1,2} \otimes R_{5,6})] S_{3,4} \otimes R_{7,8} + \\
&\quad \mathrm{tr}[(P_{1,5} \otimes P_{2,6})(S_{1,2} \otimes S_{5,6})] S_{3,4} \otimes S_{7,8}.
\end{aligned}$$

One may calculate that

$$\mathrm{tr}[(P_{1,5} \otimes P_{2,6})(R_{1,2} \otimes R_{5,6})] = \frac{d-1}{2d},$$

$$\mathrm{tr}[(P_{1,5} \otimes P_{2,6})(R_{1,2} \otimes S_{5,6})] = 0,$$

$$\mathrm{tr}[(P_{1,5} \otimes P_{2,6})(S_{1,2} \otimes R_{5,6})] = 0,$$

$$\mathrm{tr}[(P_{1,5} \otimes P_{2,6})(S_{1,2} \otimes S_{5,6})] = \frac{d+1}{2d},$$

and therefore the state of the registers (X_3, X_4, X_7, X_8) above is

$$\frac{d+1}{2d}\left[\alpha\left(1 + \frac{\varepsilon}{d+1}\right) R_{3,4} \otimes R_{7,8} + S_{3,4} \otimes S_{7,8}\right].$$

Now, based on this process, Alice and Bob distill their copies of $\rho(\varepsilon)$ as follows. They begin with $(X_1, \ldots, X_4)$ and $(X_5, \ldots, X_8)$, each containing a copy of $\rho(\varepsilon)$, and the above iteration is performed. If it is successful, they relabel registers (X_3, X_4, X_7, X_8) as (X_1, X_2, X_3, X_4) and initialize $(X_5, \ldots, X_8)$ with a new copy of $\rho(\varepsilon)$. Otherwise, if it is not successful, they start the entire process over with both $(X_1, \ldots, X_4)$ and $(X_5, \ldots, X_8)$ initialized to $\rho(\varepsilon)$. This process is repeated until a number k of consecutive successes has been achieved that satisfies

$$\frac{d+1+\varepsilon}{d-1}\left(1 + \frac{\varepsilon}{d+1}\right)^k > 3.$$

This eventually happens with probability 1. At a point when it has happened, the registers (X_1, X_2, X_3, X_4) contain a state of the form $\alpha R_{1,2} \otimes R_{3,4} + S_{1,2} \otimes S_{3,4}$ for $\alpha > 3$.

It remains to prove that for $\alpha > 3$ the state

$$\alpha R_{1,2} \otimes R_{3,4} + S_{1,2} \otimes S_{3,4}$$

is 1-distillable. To see this, consider the Schmidt rank 2 vector

$$|\phi\rangle = |1\rangle_1 |2\rangle_2 (|1\rangle_3 |1\rangle_4 + |2\rangle_3 |2\rangle_4).$$

Because

$$T_{\mathcal{A}}(\alpha R_{1,2} \otimes R_{3,4} + S_{1,2} \otimes S_{3,4}) = \frac{\alpha+1}{4} I_{1,2} \otimes I_{3,4} - \frac{(\alpha-1)d}{4} I_{1,2} \otimes P_{3,4} - \frac{(\alpha-1)d}{4} P_{1,2} \otimes I_{3,4} + \frac{(\alpha+1)d^2}{4} P_{1,2} \otimes P_{3,4},$$

it follows that

$$\langle\phi| T_{\mathcal{A}}(\alpha R_{1,2} \otimes R_{3,4} + S_{1,2} \otimes S_{3,4}) |\phi\rangle = \frac{3-\alpha}{2} < 0.$$

This completes the proof. ■

Discussion.—Theorem 1 establishes a counterintuitive property of entanglement distillation, which is that entanglement distillation is nonlinear with respect to the number of copies used in the distillation process. It is curious that there exist, for instance, examples of quantum states ρ such that 10^6 copies of ρ are not sufficient for a single shared pair of nonseparable qubits to be distilled, but with many more copies of ρ near-perfect e-bits can be distilled.

As discussed in the introduction, no effective procedure is known that determines whether or not a given bipartite state is distillable. This Letter rules out the possibility that distillability is equivalent to n-distillability for some finite value of n, and therefore implies the characterization for n-distillability introduced in Ref. [6] and discussed above does not extend to an effective test for distillability in any obvious way.

Finally, the result proved here has implications to the conjecture of Refs. [7,8] concerning the distillability of Werner states for certain ranges of parameters. More specifically, the (unnormalized) family of Werner states $\sigma_W(\alpha) = S + \alpha R$ in $d \otimes d$ dimensions are readily seen to be non-PPT states for $(d+1)/(d-1) < \alpha$, and 1-distillable if and only if $\alpha > 3$. The conjecture of Refs. [7,8] is that $\sigma_W(\alpha)$ is undistillable for $\alpha \leq 3$, which would imply that the PPT states are a proper subset of the undistillable states. One of the pieces of evidence presented in support of this conjecture was that for every positive integer n, there exists some value of $\alpha > (d+1)/(d-1)$ for which $\sigma_W(\alpha)$ is not n-distillable. (Indeed, the proof of lemma 2 above proceeds along similar lines to the proof of this fact from Ref. [7].) This Letter certainly does not refute this conjecture, but does call into question the evidence just discussed. In particular, the states $\rho(\varepsilon)$ defined in the proof of theorem 1 possess essentially the same property of being neither PPT nor n-distillable for some choice of ε, but nevertheless are distillable. Perhaps this fact may shed some light on the question of whether or not non-PPT states can always be distilled.

Thanks to John Smolin, Ashish Thapliyal, and others for very helpful comments and corrections. This research was supported by Canada's NSERC and the Canada Research Chairs program.

*Electronic address: jwatrous@cpsc.ucalgary.ca

[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, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[6] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[7] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A **61**, 062313 (2000).
[8] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
[9] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
[10] K. H. Vollbrecht and M. M. Wolf, Phys. Rev. Lett. **88**, 247901 (2002).