Random Bipartite Entanglement from W and W-Like States

Ben Fortescue and Hoi-Kwong Lo

Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada

(Received 3 August 2006; published 28 June 2007)

We describe a protocol for distilling maximally entangled bipartite states between random pairs of parties from those sharing a tripartite W state $|W\rangle = (1/\sqrt{3})(|100\rangle + |010\rangle + |001\rangle)_{ABC}$, and show that the total distillation rate E_t^∞ [the total number of Einstein-Podolsky-Rosen (EPR) pairs distilled per W, irrespective of who shares them] may be done at a higher rate than EPR distillation between specified pairs of parties. Specifically, the optimal rate for distillation to specified parties has been previously shown to be 0.92 EPR pairs per W, while our protocol can asymptotically distill 1 EPR pair per W between random pairs of parties, which we conjecture to be optimal. We thus demonstrate a tradeoff between overall distillation rate and final distribution of EPR pairs. We further show that there exist states with fixed lower-bounded E_t^∞, but arbitrarily small distillable entanglement for specified parties.

DOI: 10.1103/PhysRevLett.98.260501 PACS numbers: 03.67.Mn, 03.65.Ud

For pure entangled states ρ_{AB} shared between two parties, Alice and Bob, the standard measure of entanglement is the von Neumann entropy S,

$$S(\rho_A) = -\mathrm{tr}(\rho_A \log_2 \rho_A), \tag{1}$$

where $\rho_A = \mathrm{tr}_B(\rho_{AB})$. This has been shown to be a fungible measure [1] such that if Alice and Bob occupy distant laboratories they may, through only local operations in their own laboratories and classical communication between their laboratories (LOCC), reversibly convert N copies of ρ_{AB} to $NS(\rho_A)$ Einstein-Podolsky-Rosen (EPR) pairs

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \tag{2}$$

in the large N limit.

For states shared between >2 parties there is no single "maximally entangled state" fulfilling the role of the EPR pair in the two-party case. One can, however, consider distillation of multiparty states to EPR pairs shared between two of the parties. Previous studies on EPR distillation protocols have focused mainly on the distillation of EPR pairs between two *a priori* specified parties. In contrast, in this Letter we consider a different problem—the distillation of EPR pairs between any (*a priori* unspecified) pairs of parties.

We find the surprising result that, by not *a priori* specifying which pairs of parties share EPR pairs, one can achieve a higher distillation rate of EPR pairs than is otherwise possible. Moreover, we will show that such a surprising result does not occur for Greenberger-Horne-Zeilinger (GHZ) states $(1/\sqrt{2})(|000\rangle + |111\rangle)_{ABC}$ or certain "GHZ-like" states, but does for the W state and certain W-like states. Furthermore, we will also show that, for any M-partite pure state, the regularized relative entropy of entanglement provides an upper bound on the rate of our random distillation protocol. We hope that our new line of investigation presented in this Letter will shed some light on the subtleties of multipartite entanglement. Previous results on tripartite and W state distillation include [2–4].

We consider distillation of an M-party pure state ψ through LOCC

$$|\psi\rangle^{\otimes N}_{A_1,\ldots,A_M} \rightarrow \bigotimes_{ij} |\mathrm{EPR}\rangle^{\otimes N_{A_iA_j}}_{A_iA_j}. \tag{3}$$

For specified parties A_I, A_J, the asymptotic entanglement of assistance (that is, the optimal rate of EPR distillation) $E^\infty_{A_IA_J}(\psi) \equiv \sup_{N\rightarrow\infty}(N_{A_IA_J}/N)$ was shown in [5] (with the three-party case earlier shown by [6]) to be

$$E^\infty_{A_IA_J}(\rho) = \min_T\{S(\rho_{A_IT}), S(\rho_{A_J\bar{T}})\}, \tag{4}$$

where $\rho = |\psi\rangle\langle\psi|$ and the minimum is over all partitions of the parties into two groups T and $\bar{T}$. We further define the specified entanglement E_s^∞ as the maximum of $E^\infty_{A_IA_J}$ over all pairs of parties I, J.

We also define the total EPR distillation rate (the maximum overall rate of distilling EPR pairs, irrespective of which parties share them) $E_t^\infty(\psi)$ as

$$E_t^\infty(\psi) = \sup \frac{\sum_{ij} N_{A_iA_j}}{N} \tag{5}$$

in the limit $N \rightarrow \infty$ (thus $E_t^\infty \geq E_s^\infty$ in general). We further define E_t and E_s as the single-copy analogs (the expected rates for obtaining EPRs from a single copy of the state) of E_t^∞ and E_s^∞.

We first discuss the case of distilling the W state. Consider many copies of the W state shared between three parties Alice, Bob and Charlie. If, say, Bob and Charlie wish to distill EPRs from the W's with the help of Alice, then from (4) we have that the maximum rate (i.e., the maximum number of EPRs per W) which they can obtain is

$$E_s^\infty(W) = H_2(1/3) \approx 0.92, \tag{6}$$

where H_2 is the binary entropy function

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x). \quad (7)$$

By symmetry this is likewise the optimum rate for Alice and Bob distilling EPRs with Charlie's help, etc. In the case of a single copy of the W state we find from the general bound of [7] that the maximum probability of obtaining an EPR between Alice and Bob is $E_s(W) = G_{AB}(W) = 2/3$, where G_{AB} is the concurrence of assistance, originally defined in [8]. (This is in contrast to the GHZ state, for which $E_s = 1$—one can always obtain an EPR between specified parties from a GHZ through LOCC.)

However, suppose the three parties merely wish to distill as many EPRs as possible without regard for which of the parties share them. In this case we find they can achieve a single-copy rate $E_t(W)$, where

Theorem 1:

$$E_t(W) \geq 1 \quad (8)$$

Proof: If Alice, Bob and Charlie each apply the rotation

$$|1\rangle \rightarrow |1\rangle, \qquad |0\rangle \rightarrow \sqrt{1-\epsilon^2}|0\rangle + \epsilon|2\rangle, \quad (9)$$

then

$$|W\rangle_{ABC} \rightarrow (1-\epsilon^2)|W\rangle + \frac{\epsilon}{\sqrt{3}}(|021\rangle + |201\rangle + |012\rangle + |210\rangle + |102\rangle + |120\rangle) + O(\epsilon^2). \quad (10)$$

If all 3 parties then make a measurement on their qubit using the projectors

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad B = |2\rangle\langle 2| \quad (11)$$

then either

(1) All 3 parties get outcome "A," with probability $(1-\epsilon^2)^2$, and hence share a W again, the rotations and projective measurements are then repeated.

(2) One of the three parties gets outcome "B" (i.e., their qubit is in state $|2\rangle$), with probability $(2/3)\epsilon^2(1-\epsilon^2)$ each. Say this is Alice, then following the measurement the state is $|2\rangle_A \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{BC}$; i.e., Bob and Charlie share an EPR pair. By symmetry, if the party with a $|2\rangle$ is Bob, then Alice and Charlie will share an EPR pair and so on, for a total success probability of $2\epsilon^2(1-\epsilon^2)$

(3) Two or more parties get outcome "B," resulting in a product state, with total probability ϵ^4. Thus if the parties are performing up to D rounds of the protocol (only performing fewer if an EPR or product state results in fewer than D rounds) their final expected entanglement is

$$\langle E_D\rangle = 2\epsilon_D^2(1-\epsilon_D^2) + (1-\epsilon_D^2)^2\langle E_{D-1}\rangle, \quad (12)$$

where ϵ_D is the chosen ϵ for the round of the protocol when up to D rounds remain (thus ϵ is different in each round). It follows by differentiation and induction that the optimal ϵ_D is $\epsilon_D^{\rm opt} = 1/\sqrt{D+1}$, which gives

$$\langle E_D^{\rm opt}\rangle = \frac{D}{D+1}. \quad (13)$$

Thus for finite D the single-copy limit of $E_s = 2/3$ is surpassed for $D \geq 3$ and the asymptotic limit of $E_s^\infty = H_2(1/3)$ is surpassed for $D \geq 12$. In the limit as $D \rightarrow \infty$ two of the three parties end up sharing an EPR pair with probability $\rightarrow 1$. That is, $E_t^\infty \geq E_t \geq 1$. □

This protocol was developed in collaboration with Gottesman [9].

By symmetry, in the limit of many copies N of the W state each pair of parties (AB, BC, AC) will end up sharing on average $N/3$ EPR pairs under this protocol. We note that the parties could then use the EPRs to share through quantum teleportation [10] $N/2$ copies of the GHZ or any other three-qubit state, for an overall distillation rate of 0.5. However for GHZ states at least this is not optimal—a rate of 0.64 is demonstrated (and also shown to be optimal under a specified class of protocols) in [6].

We also find that similar distillation can be advantageous for asymmetric W-like states.

Theorem 2: Defining a W-like state

$$|W'\rangle = a|100\rangle + b|010\rangle + c|001\rangle. \quad (14)$$

For a W' where (without loss of generality) $0 \leq a \leq b \leq c$ with a, b, c real:

$$E_t^\infty(W') \geq 1 - [1-(a/c)^2](b^2+c^2) \times \left[1 - H_2\left(\frac{b^2}{b^2+c^2}\right)\right]. \quad (15)$$

It follows, for example, that $E_t^\infty(W') \geq 1$ for $b = c$.

Proof: The above rate can be achieved by the combination of a filtering protocol and the random W distillation protocol.

If Alice applies the unitary

$$|0\rangle \rightarrow \frac{a}{c}|0\rangle + \sqrt{1-(a/c)^2}|2\rangle, \qquad |1\rangle \rightarrow |1\rangle \quad (16)$$

then

$$|W'\rangle \rightarrow (a|100\rangle + ab/c|010\rangle + a|001\rangle)_{ABC} + \sqrt{1-(a/c)^2}|2\rangle(b|10\rangle + c|01\rangle)_{ABC}. \quad (17)$$

Alice then measures her qubit using the projection (11), obtaining either a tripartite state [first term in (17), after normalization] or an entangled pair of von Neumann entropy $H_2[b^2/(b^2+c^2)]$ shared between Bob and Charlie. This latter outcome occurs with probability $[1-(a/c)^2]\times(b^2+c^2)$.

We will now show that, in all other circumstances, an EPR pair is obtained, thus proving the theorem. If Alice announces that a tripartite state has been obtained, Bob applies the unitary

$$|0\rangle \rightarrow \frac{b}{c}|0\rangle + \sqrt{1-(b/c)^2}|2\rangle, \qquad |1\rangle \rightarrow |1\rangle, \quad (18)$$

thus leaving the three parties with the state

$$|\psi\rangle = \frac{1}{\sqrt{2+(b/c)^2}}\left(\frac{\sqrt{3}b}{c}|W\rangle_{ABC} + \sqrt{2}|2\rangle_B\sqrt{1-(b/c)^2}|{\rm EPR}\rangle_{AC}\right). \quad (19)$$

Bob performs the projection (11) to obtain either a shared W or a shared EPR between Alice and Charlie. Bob announces his result—if a W is obtained then the random W distillation is performed to obtain a randomly shared EPR pair. □

For the W', $E_s^\infty(W') = H_2(b^2)$ which is less than or equal to the lower bound on E_t^∞ of Theorem 2.

Conjecture: $E_t^\infty(W) = 1$

That is, we conjecture that distillation using the protocol described in Theorem 1 is optimal for the W state. However we have no proof of this—our tightest upper bound is as follows.

Theorem 3: For a pure tripartite state σ_{ABC}

$$E_t^\infty(\sigma_{ABC}) \leq \min\{S(\sigma_{BC}) + E_r^\infty(\sigma_{BC}), S(\sigma_{AC}) + E_r^\infty(\sigma_{AC}), S(\sigma_{AB}) + E_r^\infty(\sigma_{AB})\}, \quad (20)$$

where the asymptotic relative entropy of entanglement $E_r^\infty(\rho) = \lim_{N\to\infty} E_r(\rho^{\otimes N})/N$ and for an M-party state

$$E_r(\rho_{A_i,\ldots,A_M}) = \min_{\sigma^{\rm sep}_{A_i,\ldots,A_M}} S(\rho_{A_i,\ldots,A_M} \| \sigma_{A_i,\ldots,A_M}), \quad (21)$$

where $\sigma^{\rm sep}_{A_i,\ldots,A_M}$ are separable states.

Proof: (Our proof is a simple application of the result in [11]). It was shown in [11] that for any three-party LOCC protocol starting from a pure initial state ρ_{ABC}

$$\langle E_r(\rho_{BC})\rangle_{\rm final} - E_r(\rho_{BC})_{\rm initial} \leq S(\rho_A)_{\rm initial} - \langle S(\rho_A)\rangle_{\rm final}. \quad (22)$$

For a distillation (3) of a pure state σ_{ABC} we have, assuming asymptotic continuity [12],

$$S(\rho_A)_{\rm initial} = S(\sigma_A^{\otimes N}) = NS(\sigma_A), \quad (23)$$

$$\langle S(\rho_A)\rangle_{\rm final} = N_{AB} + N_{AC}, \quad (24)$$

$$\langle E_r(\rho_{BC})\rangle_{\rm final} = N_{BC}, \quad (25)$$

$$E_r(\rho_{BC})_{\rm initial} = E_r(\sigma_{BC}^{\otimes N}), \quad (26)$$

thus

$$N_{AB} + N_{BC} + N_{AC} \leq NS(\sigma_A) + E_r(\sigma_{BC}^{\otimes N}) = NS(\sigma_{BC}) + E_r(\sigma_{BC}^{\otimes N}). \quad (27)$$

Since we are free to permute $\{A, B, C\}$, dividing through by N and taking $\lim_{N\to\infty}$ leads to (20). □

Theorem 3 leads to an explicit bound on E_t^∞ for states defined as $|W_{ab}\rangle \equiv a|100\rangle + b|010\rangle + b|001\rangle$ (a, b real). From [13] [Eqs. (54)–(56)] we have that for W_{ab}

$$E_r(\sigma_{BC})_{\rm initial} = -(1+a^2)\log_2\left(\frac{1+a^2}{2}\right) + a^2\log_2 a^2. \quad (28)$$

Since $E_r(\sigma_{BC}) \leq E_r^\infty(\sigma_{BC})$ and $S(\sigma_A) = H_2(a^2)$, we have

$$E_t^\infty(W_{ab}) \leq -(1-a^2)\log_2(1-a^2) - (1 + a^2)\log_2\left(\frac{1+a^2}{2}\right). \quad (29)$$

This is illustrated in Fig. 1. This bound is a maximum for the W state with $a^2 = 1/3$, for which $E_t^\infty(W) \leq \log_2(9/4) \approx 1.17$.

We also find a more general bound for any number of parties.

Theorem 4: For an M-party pure state $\sigma_{A_1,\ldots,A_M}$,

$$E_t^\infty(\sigma) \leq E_r^\infty(\sigma), \quad (30)$$

This was noted for the 3-party case by Plenio [14], which follows from Theorem 3 above and Theorem 1 of [15].

Proof: Reference [15] derives a bound on the relative entropy of tripartite systems from [16], noting that this readily generalizes to the multiparty case. The general multiparty bound is

$$E_r^\infty(\sigma_{A_1,\ldots,A_M}) \geq \max\{S(\sigma_{A_1,\ldots,A_{M-1}}) + E_r^\infty(\sigma_{A_1,\ldots,A_{M-1}}), \ldots\}, \quad (31)$$

where the maximum is over all permutations of the parties A_1 to A_M. Considering the final state in (3) $\rho^f_{A_1,\ldots,A_M} = \bigotimes_{ij}|{\rm EPR}\rangle^{\otimes N_{A_iA_j}}_{A_iA_j}$, we have

$$S(\rho^f_{A_1,\ldots,A_{M-1}}) = \sum_i N_{A_iA_M} \quad (32)$$

and, by induction from the three-party bound,

$$E_r^\infty(\rho^f_{A_1,\ldots,A_{M-1}}) \geq \sum_{\{i,j\}\neq M} N_{A_iA_j}. \quad (33)$$

Thus (since E_r^∞ is an entanglement monotone), for the

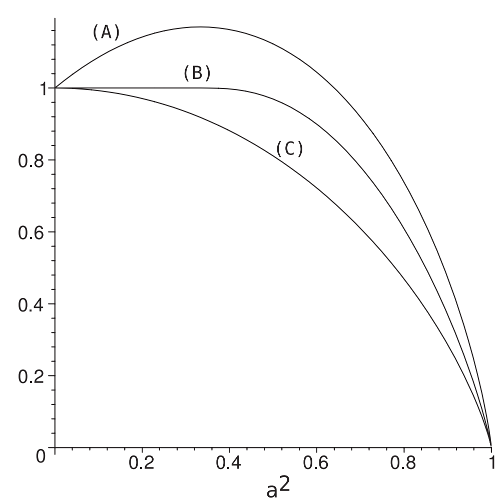

FIG. 1. For W_{ab}, a plot as a function of a^2 of (A) upper bound on E_t^∞ [as specified in Eq. (29)], (B) lower bound on E_t^∞ [as specified in Eq. (15)], (C) E_s (“specified entanglement”), equal to $H_2(b^2)$. The gap between (B) and (C) shows that distillation to random parties can be more efficient by certain measures than distillation to specified parties.

distillation (3), $NE_r^\infty(\psi) \geq E_r^\infty(\psi^{\otimes N}) \geq E_r^\infty(\rho_f) \geq \sum_{ij} N_{A_iA_j}$, leading to (30). □

Various conclusions follow from this bound—since $E_r^\infty(\rho_{ABC}) \leq E_r(\rho_{ABC})$ generally, we find, for example, that since for GHZ-like states $|\mathrm{GHZ}'\rangle = \alpha|000\rangle + \beta|111\rangle$ we have $E_r^\infty(\mathrm{GHZ}') = E_s(\mathrm{GHZ}') = H_2(|\alpha|^2)$ [15], then random distillation gives no advantage over specified distillation for such states. See also Ref. [17].

Our protocol for W states (in which a randomly determined party announces their measurement result to leave the remaining two parties with an EPR pair) can be straightforwardly generalized to a multiparty protocol in which multiple announcements are made, which leads to the following result.

Theorem 5: One can construct states with arbitrarily small E_s^∞ for which $E_t^\infty \geq 1$.

Proof: Consider the class of states which we denote as $|W_M\rangle$:

$$|W_M\rangle = \frac{1}{\sqrt{M}}(|00,\ldots,01\rangle + \text{cyclic permutations}) \quad (34)$$

(so W_2 is an EPR pair, W_3 is a W, etc.). The W_M state is initially shared between M parties, all of whom perform the unitary (9) on their qubit, followed by the projection (11), repeating as necessary until one party gets outcome B, as with the W. This party announces their result and the remaining parties repeat the protocol.

After one successful application of the protocol one random party has made an announcement and the remainder share an W_{M-1} state and so on. After $M-2$ such rounds the two remaining parties share an EPR pair, thus

$$E_t(W_M) \geq 1, \quad (35)$$

but for a W_M state

$$E_s^\infty(W_M) = H_2(1/M), \quad (36)$$

which $\rightarrow 0$ as $M \rightarrow \infty$. □

In the future, clearly we would like to prove or disprove our conjecture regarding the optimality of the random distillation for the W state by finding a tight upper bound for E_t^∞, as well as tightly bounding E_t^∞ for more general tripartite states. Though our operational measure E_t^∞ is based on distillation in the many-copy limit, our present random distillation protocols work on single copies of states—it is not clear whether distillation rates could be improved by operating on multiple copies.

In addition, a more discriminating quantity for tripartite states is the range of obtainable values of $\{N_{AB}, N_{BC}, N_{AC}\}$ in the distillation (3)—an interesting problem is to tightly bound this range for, say, general W'. It would likewise be worth investigating the reverse process—the required number of shared EPRs between parties for formation of W'. We also note that the condition $E_t^\infty \geq E_s^\infty$ is not always appropriate to consider, as it can sometimes be trivially satisfied, e.g., by a multiparty state of several EPRs shared between different pairs of parties.

Thus far we have only investigated random distillation of a particular class of pure states. It would be interesting to study random distillation for other types of output states including the W and GHZ states. One might even study the random distillation and irreversibility in distillation and formation between a whole hierarchy of states. We note that there have been two recent papers on distillation of mixed stabilizer states ([20,21]—note that the W is not a stabilizer state)—it would be interesting to find the achievable random distillation rates for such states as well as for more general multipartite states.

We thank Matthias Christandl, Andreas Winter, Debbie Leung, and, particularly, Daniel Gottesman and Martin Plenio for elightening discussions. Financial support from NSERC, CIFAR, CRC Program, CFI, OIT, PREA, MITACS, and CIPI is gratefully acknowledged.

[1] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[2] B. Groisman, N. Linden, and S. Popescu, Phys. Rev. A **72**, 062322 (2005).
[3] A. Miyake and H. J. Briegel, Phys. Rev. Lett. **95**, 220501 (2005).
[4] Z.-L. Cao and M. Yang, J. Phys. B **36**, 4245 (2003).
[5] M. Horodecki, J. Oppenheim, and A. Winter, Nature (London) **436**, 673 (2005).
[6] J. A. Smolin, F. Verstraete, and A. Winter, Phys. Rev. A **72**, 052317 (2005).
[7] G. Gour, Phys. Rev. A **72**, 042318 (2005).
[8] T. Laustsen, F. Verstraete, and S. J. Van Enk, Quantum Inf. Comput. **3**, 64 (2003).
[9] Daniel Gottesman (private communication).
[10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[11] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, Quant. Info. Proc. **4**, 241 (2005).
[12] M. J. Donald and M. Horodecki, Phys. Lett. A **264**, 257 (1999).
[13] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[14] M. B. Plenio (private communication).
[15] M. B. Plenio and V. Vedral, J. Phys. A **34**, 6997 (2001).
[16] M. B. Plenio, V. Vedral, and P. Papadopoulos, J. Phys. A **33**, L193 (2000).
[17] The bound also leads to the same numerical bound for W as above, as shown in [18], which gives $E_r^\infty(W) \leq E_r(W) = \log_2(9/4)$. In addition, since [19] showed that $E_r^\infty(W) \geq \log_2 3 - 5/9 \approx 1.03$, any numerical upper bound on $E_t^\infty(W)$ derived from (30) cannot be less than 1.03 and hence would not be sufficient in itself to prove our conjecture.
[18] E. F. Galvão, M. B. Plenio, and S. Virmani, J. Phys. A **33**, 8809 (2000).
[19] S. Ishizaka and M. B. Plenio, Phys. Rev. A **72**, 042325 (2005).
[20] C. Kruszynska, A. Miyake, H. J. Briegel, and W. Dür, Phys. Rev. A **74**, 052316 (2006).
[21] S. Glancy, E. Knill, and H. M. Vasconcelos, Phys. Rev. A **74**, 032319 (2006).