

Entanglement Combing

Dong Yang^{1,2} and Jens Eisert^{1,3}

¹*Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany*

²*Laboratory for Quantum Information, China Jiliang University Hangzhou, Zhejiang 310018, China*

³*Institute for Advanced Study Berlin, 14193 Berlin, Germany*

(Received 5 August 2009; published 23 November 2009)

We show that all multipartite pure states can, under local operations, be transformed into bipartite pairwise entangled states in a “lossless fashion”: An arbitrary distinguished party will keep pairwise entanglement with all other parties after the asymptotic protocol—decorrelating all other parties from each other—in a way that the degree of entanglement of this party with respect to the rest will remain entirely unchanged. The set of possible entanglement distributions of bipartite pairs is also classified. Finally, we point out several applications of this protocol as a useful primitive in quantum information theory.

DOI: [10.1103/PhysRevLett.103.220501](https://doi.org/10.1103/PhysRevLett.103.220501)

PACS numbers: 03.67.Mn, 03.65.Ca, 03.67.Hk

In what way is multipartite entanglement different from bipartite entanglement? Instances of this question have featured prominently in the quantum information literature, motivated by the central role entanglement plays in quantum information theory [1]. Yet, in many ways, the understanding of multiparticle entanglement and its applications is still unsatisfactory: Quite pragmatically speaking, while many quantum communication and cryptographic protocols have been identified between two separated laboratories, fewer practical protocols, say, in key distribution, are known that directly rely on genuinely multipartite correlations. Since then, progress on the “traditional questions” on multiparticle entanglement seems to have slowed down, such as the problem of what ingredients are eventually needed to prepare an arbitrary state (meant in a local, asymptotically reversible fashion) [2,3]. What is more, it still seems not quite clear what the exact role of multipartite entanglement is in the known communication protocols, and even—quite prominently—in quantum computation. All this motivates the question of in what sense can one think of multipartite correlations as being different from bipartite ones, or more specifically, in what sense can the former just be translated into the latter.

In this work we will introduce a protocol for transforming arbitrary multiparticle entanglement into a simple, in fact, bipartite normal form. This protocol, referred to as entanglement combing, shows in what sense bipartite correlations are contained in any state, and can be viewed as a primitive in quantum information that can be used to construct new protocols, a perspective that we outline.

The indeed surprising feature of this primitive is that this transformation can be done in a lossless fashion: One can simply decorrelate multipartite entanglement always into bipartite one, without losing any of the entanglement between the party holding the bipartite entanglement and the rest. We will first discuss the protocol, as usual under asymptotic local operations and classical communication (LOCC). Then, we fully classify the region of entanglement distribution that can be achieved in the combing

process. Finally, we will outline a number of possible applications of the protocol.

The task.—Consider an arbitrary pure $m + 1$ -partite state $|\phi\rangle_{A,B_1,\dots,B_m}$ (of finite dimension) shared among an arbitrary distinguished party (Alice) and the other parties (here many Bobs). Obviously, in any such state the multipartite entanglement structure can be very intricate. The goal is to distill tensor products $|\phi_1\rangle_{A_1,B_1} \otimes \dots \otimes |\phi_m\rangle_{A_m,B_m}$ of bipartite entangled states with respect to Alice and many Bobs under LOCC; see Fig. 1. This protocol hence complements recently studied protocols for multipartite states: One is entanglement of assistance [4] and the other is random distillation [5]. Entanglement of assistance asks how much entanglement between two specified parties can be distilled for a pure m -partite state under helpful LOCC operations of the other $m - 2$ parties [4]. Random distillation in turn asks how much pairwise entanglement can be obtained by LOCC whichever two parties would share the final entanglement. Here we show that in fact the entanglement between a fixed party with the rest can actually be divided into pure bipartite states shared between the fixed party and the rest ones individually. What is more, the final bipartite entanglement content can be taken to be same. It should be emphasized that as in any protocol discussing rates of entanglement trans-

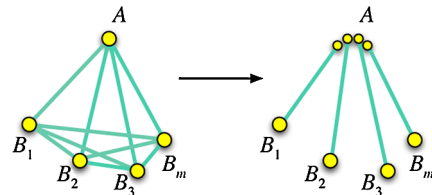


FIG. 1 (color online). Entanglement combing: An arbitrary multipartite entangled pure state $|\phi\rangle_{A,B_1,\dots,B_m}$ can be asymptotically deterministically transformed into a tensor product of bipartite states $|\phi_1\rangle_{A_1,B_1} \otimes \dots \otimes |\phi_m\rangle_{A_m,B_m}$ under LOCC operations, in a way such that the bipartite entanglement between A on the one hand and $B_1, \dots, B_m$ on the other hand is preserved.

formations, all results in this work are meant in the asymptotic setting. As usual, we simply write $|\psi\rangle^{\otimes s} \rightarrow |\phi\rangle^{\otimes r}$ for some $r, s \geq 0$ if there is a sequence $\{i_n\}$ of integers such that $|\psi\rangle^{\otimes i_n} \rightarrow |\phi_n\rangle$ under LOCC and $\lim_{n \rightarrow \infty} \|\phi_n - |\phi\rangle^{\otimes i_n}\| = 0$ with $\limsup_{n \rightarrow \infty} i_n/n = r/s$. We will now carefully state the first main conclusion:

Proposition 1 (Entanglement combing).—Any pure state shared between $m + 1$ parties $A, B_1, \dots, B_m$ can be locally transformed, “combed”, into a tensor product of bipartite states shared between A and $B_1, \dots, B_m$, i.e., $|\phi\rangle_{A,B_1,\dots,B_m} \rightarrow |\phi_1\rangle_{A,B_1} \otimes \dots \otimes |\phi_m\rangle_{A,B_m}$ under LOCC. This can be done in a way such that the entanglement of A with respect to $B_1, \dots, B_m$ is left unchanged, $\sum_k E_k = \sum_k S(\rho_{A_k}) = S(A)$.

Here, $S(A)$ is the initial von Neumann entropy of A , and the entanglement of a bipartite pure state is measured as the usual entanglement entropy $E(|\phi_k\rangle_{A_k,B_k}) := S(\rho_{A_k}) =: E_k$, ρ_{A_k} denoting the respective reduced state. In the proof of this statement—delayed to the proof of possible distributions—two techniques feature strongly: One is the protocol quantum state merging [6] and the other is a Lemma [6] that implies the entanglement of assistance. All technicalities when identifying the reachable set are related to appropriately generating appropriate resources using these protocols in substeps, then using them in later steps, to again create suitable resources and so on, subtly balancing trade offs, in a way that yields asymptotically the correct rates.

T1 (Quantum state merging).—For a pure tripartite state $|\phi\rangle_{A,B,C}$, the entanglement cost of merging A to B under the reference C is equal to the conditional entropy $S(A|B) = S(AB) - S(B)$. When $S(A|B)$ is positive, $S(A|B)$ entanglement has to be consumed to perform merging. When $S(A|B)$ is negative, merging can be performed under LOCC, and moreover $-S(A|B)$ entanglement is obtained.

T2 (Assisting).—For a pure tripartite state $|\phi\rangle_{A,B,C}$, if $S(B) > S(A)$, then there exists a complete measurement on C such that the resulting state of ABC is the ensemble $\{p_k, |\psi^k\rangle_{A,B} \otimes |k\rangle_C\}$ satisfying $S(\rho_A^k) \approx S(A)$.

Distribution of entangled pairs.—Now we know that entanglement between an arbitrary distinguished party Alice and all other parties as a whole can be “combed” under LOCC into pairwise entanglement such that the sum of the pairwise entanglement is just the initial entanglement. Clearly, there is no reason to assume that this final distribution is unique: This very distribution is, however, important when thinking of new protocols based on this primitive. We now turn to giving a complete answer to the possible distributions of entangled pairs:

Proposition 2 (Distribution of entangled pairs).—The feasible set of different entanglement distributions in entanglement combing $F = \{(E_1, E_2, \dots, E_m)\}$ for a given initial state $|\phi\rangle_{A,B_1,\dots,B_m}$ is a polytope: It is the positive part of the polytope the extreme points of which being given by merging the states of m parties to A in different orders.

Proof.—It is clear that, if such a protocol exists, $\sum_k E(|\phi_k\rangle_{A_k,B_k}) \leq S(\rho_A)$, as the degree of entanglement

between Alice and the multiple Bobs cannot increase [7]. The surprising fact is that the upper bound can indeed be achieved. Let us first briefly see that such a protocol exists (although this protocol not being constructive). Suppose we consider to deal with B_m first. If $S(A) \geq S(B_1 \dots B_{m-1})$, then we perform T1 that will merge B_m into A and, additionally, $-S(B_m|A) = S(A) - S(B_m A) = S(A) - S(B_1 \dots B_{m-1})$ of entanglement between A and B_m will be obtained as an asymptotic rate, where we use the fact that for a pure state $|\phi\rangle_{X,Y}$, $S(X) = S(Y)$. That is, $|\phi\rangle_{A,B_1,\dots,B_m} \rightarrow |\psi\rangle_{(B_m A),B_1,\dots,B_{m-1}} \otimes |\xi\rangle_{A_m,B_m}$ such that $S(B_m A) + E(|\xi\rangle_{A_m,B_m}) = S(A)$, $S(A)$ denoting the initial local entropy of A . If $S(A) < S(B_1 \dots B_{m-1})$, then we perform T2 to achieve the ensemble $\{p_k, |\phi\rangle_{A,B_1,\dots,B_{m-1}}^k \otimes |k\rangle_{B_m}\}$ such that $S(\rho_A^k) \approx S(A)$. In both cases the entropy of the A remains invariant up to asymptotically negligible corrections, and B_m is decoupled. However, now we are left with a m -partite state among A and $B_1, \dots, B_{m-1}$. Next we deal with B_{m-1} and iterate the strategy until we obtain the final state of the form $|\phi_1\rangle_{A,B_1} \otimes \dots \otimes |\phi_m\rangle_{A,B_m}$. During each step the entropy of A remains invariant, again up to corrections not relevant for the rate.

We now turn to the actual proof of the possible distributions. There are two steps of the argument to arrive at the conclusion. In the first step, we formulate a convex outer approximation $F' \supset F$ of the set, noting that we get better rates if we allow negative quantity of entanglement shared between Alice and the Bobs. A negative value means that entanglement is actually consumed instead of being obtained at the final stage, or in other words entanglement should be borrowed in order to accomplish the task [8]. If negative values are allowed, the combing can be regarded as merging process and the extreme points of the convex set F' are obtained by merging the states of all Bobs except the last one to that of Alice in different orders. Convexity of F' is readily shown by the time-sharing technique [9]. For the $m + 1$ -partite state, one point $(E_1, \dots, E_m)$ is obtained by the merging order: Say, first merging B_m to A , second B_{m-1} to AB_m , third B_{m-2} to $AB_{m-1}B_m$, and so on. So we get $E_1 = S(B_1)$, $E_2 = S(AB_3 \dots B_m) - S(B_1)$, until $E_{m-1} = S(AB_m) - S(B_1 \dots B_{m-2})$, $E_m = S(A) - S(B_1 \dots B_{m-1})$, evidently summing to $S(A)$. These $m!$ points are the extreme points of F' : The reason comes from quantum distributed compression. Imagine that if after the merging protocol Bobs compress their parts and send to a new party, say Z , then Z is capable to recover the original state $\rho_{B_1,\dots,B_m}$ while preserving the coherence with Alice. $(E_1, \dots, E_m)$ is an extreme point in the distributed compression [6]: First compressing and sending B_1 , then $B_2, \dots, B_m$ in a sequence. All other extreme points are found similarly, and F' is a polytope. $F \subset F'$ or a contradiction will arise.

In the second step, we show that the combing region is just the intersection of this polytope with the positive cone: That is, each non-negative point can be achieved without borrowing entanglement beforehand. At the final stage of

combing, obviously only non-negative quantities of entanglement are allowed. We know how to achieve any point in F' with borrowing, and know that F must contain only positive points; hence, we are left to show that there exists a nonborrowed protocol approximating all non-negative points arbitrarily well. We will use the techniques of time sharing in information theory [9] and “breeding” in entanglement distillation [10]. Moreover, it will be a sequential scheme labeled by rounds r , where each is an asymptotic protocol. The entire procedure is meant as a sequence of protocols on more and more input copies, where the rates in the asymptotic versions of each round are preserved. The main idea is to prepare just the right resources for the next round, amplify the output and find that initially borrowed resources become asymptotically negligible.

Denote any point $V \in F$ in its interior. Using Caratheodory’s theorem, we know that V can be written as a convex combination of no more than m extreme points of the polytope, labeled $P, Q, \dots, S$, $V = pP + qQ + \dots + sS$, which is pointwise strictly positive by assumption. Let us denote with P^+ the positive part of P and with P^- the negative part, and similarly for $Q, \dots, S$. Let us denote with $|+\rangle_{A,B_k}$ a maximally entangled qubit pair between A and B_k .

In the first round $r = 1$, we will consider the (asymptotic protocol) that performs entanglement assistance on some number of initial copies of $|\phi\rangle_{A,B_1,\dots,B_m}$ in order to prepare the integer number $[n_1]$ of maximally entangled pairs $|+\rangle_{A,B_1}$ between A and B_1 , of with n better and better approximation, where

$$n_1 := n(pP_1^- + qQ_1^- + \dots + sS_1^-). \quad (1)$$

n will then be the quantifier of the asymptotic limit of the protocol, and analogously for parts 2, $\dots, m$. This process, which may be inefficient, then yields $[n_1]$ specimens of $|+\rangle_{A,B_1}$ shared between A and B_1 , $[n_2]$ of $|+\rangle_{A,B_2}$ between A and B_2 , asymptotically perfectly, with arbitrarily small norm error in each round, and so on.

For the second round, $r = 2$, we now know that from the protocols at $P, Q, \dots, S$ under borrowing, and the technique of time sharing, grouping the prepared bipartite entanglement, using asymptotic reversibility of pure-state bipartite state transformations,

$$|\phi\rangle_{A,B_1,\dots,B_m}^{\otimes n} |+\rangle_{A,B_1}^{\otimes n_1} \dots |+\rangle_{A,B_m}^{\otimes n_m} \rightarrow |+\rangle_{A,B_1}^{\otimes k_1} \dots \rightarrow |+\rangle_{A,B_m}^{\otimes k_m} \quad (2)$$

holds as an asymptotic transformation, where $k_j := n(pP_j^+ + qQ_j^+ + \dots + sS_j^+)$, for $j = 1, \dots, m$. This can be reached by performing the borrowing merging protocol P with a relative weight of p , then Q with a relative weight of q , until S with a relative weight of s , and then combining the resulting maximally entangled pairs appropriately. This is possible, as the resources needed in the borrowing are available. Define now $x_j := k_j/n_j$, as the amplification ratio. By definition, $x_j > 1$ for all j ; due to positivity, there

will be more entangled pairs available after this step at any position. Hence, $[nk_1]$ specimens of $|+\rangle_{A,B_1}$ will be available after this step, asymptotically perfectly, and similarly for the other parties.

For the third step, $r = 3$, define $x := \min\{x_j; j = 1, \dots, m\} > 1$. Now one again borrows maximally entangled pairs to assist the next step: We will use $[nx]$ copies of maximally entangled pairs to perform P again on $[npx]$ copies, Q on $[nqx]$ copies, until S on $[nsx]$ copies. This in turn is used in the next steps r . At large r we calculate the relative weight of the initially consumed nn_0 copies from assisting. The total number of consumed copies in r rounds is then $nn_0 + \sum_{i=0}^{r-1} nx^i = n(n_0 + (x^r - 1)/(x - 1))$. Since $x > 1$, the initially consumed copies from assisting will have a logarithmic weight in r asymptotically in r that is negligible at large r . The entire asymptotic protocol amounts to taking the $r, n \rightarrow \infty$ limit, in that the appropriate rate and the norm approximation can be achieved to arbitrary accuracy. In the end we can obtain the rate at the interior point $V \in F$ without borrowing.

Notice that for the protocol to continue it is required that $x > 1$. If $x < 1$, less and less entanglement is gained at one position such that less and less copies can be activated further. The condition that the activation can be amplified is just the requirement that V lies in the positive part of F . Now, if we are at a boundary point of F , at a face of the polytope, one can approximate V with a sequence of efficient protocols arbitrarily well, and the actual set of asymptotically reachable points is closed. Notably, the argument established here can also be used in other protocols with borrowed resources.

Applications.—We will now turn to sketching potential applications of this protocol in quantum information theory.

i. Distributed compression.—Multipartite entangled states can be employed as a resource in quantum distributed compression. From Schumacher compression [11], it is known that a source emitting states with ρ can be faithfully compressed into a Hilbert space of dimension $S(\rho)$. In quantum distributed compression, quantum data are distributed among many Bobs who are required to separately compress their data and send their parts to a common party Alice who can decode the whole data faithfully. It has just recently been proven [6] that the qubits that are required to transmit is still $S(\rho)$ though the classical scenario was known for a long time [12]. Notice that the compressed data are transmitted either through ideal channels or teleported via ebits shared between Bobs and Alice. The entanglement combining provides a way how the parties can employ their shared multipartite state as a resource to complete the task. The multipartite can be used to replace the ideal quantum channels and the bipartite entangled states. The whole protocol works like this: First we apply the combining entanglement to obtain bipartite entanglement between Alice and many Bobs. Then we apply distributed compression to

compressing the quantum data. Finally, we teleport the compressed data. The region of distributed compression and that of the combing are therefore both known. If there exists an overlap between these regions, the compressed data can be transmitted by the state.

ii. New criteria for multipartite LOCC transformations.—Entanglement combing provides a lower bound for the rate of multipartite states transformation under LOCC operations. The entanglement of a multipartite state can be combing at any party. For pure $(m + 1)$ -partite states we actually have $m + 1$ different regions for different combing processes. Consider two $m + 1$ -partite states $|\phi\rangle_{A,B_1,\dots,B_m}$ and $|\psi\rangle_{A,B_1,\dots,B_m}$. If $r(S(\psi_1), S(\psi_2), \dots, S(\psi_m))$ lies in the region F of the combing protocol of $|\phi\rangle_{A,B_1,\dots,B_m}$, then a single copy of $|\phi\rangle_{A,B_1,\dots,B_m}$ can asymptotically be transformed into r copies of $|\psi\rangle_{A,B_1,\dots,B_m}$ under LOCC that immediately gives a lower bound for the rate, ψ_k denoting reduced states. First we perform the combing protocol on $|\phi\rangle_{A,B_1,\dots,B_m}$ to obtain the bipartite entangled states between, then Alice prepares the multipartite state $|\psi\rangle_{A,B_1,\dots,B_m}$ and compresses different parts of B_k by Schumacher compression, and then teleports the compressed data of B_k to different Bobs. After having received the data, the Bobs decode the data such that $|\psi\rangle_{A,B_1,\dots,B_m}$ appears among the parties.

iii. Quantifying the multipartite character of entanglement.—The intuition is that there should exist nontrivial bipartite entanglement distribution in a genuine multipartite entangled state. We know that the region is convex set in a hyperplane in high dimension space. The geometry of the region of entanglement distribution could provide the information of genuine multipartite entanglement. A simple example is that if the state $|\psi\rangle_{A,B_1,\dots,B_m}$ is of the form $|\phi\rangle_{A,B_1,\dots,B_k} \otimes |\psi\rangle_{A,B_{(k+1)},\dots,B_m}$, then no genuine $m + 1$ -multipartite entanglement should exist. This fact is reflected in the rate region is that the hyperplane will have lower dimension while generically it has dimension $m - 1$. A simple geometric quantity is the volume of the polytope which we conjecture would be a potential quantity for genuine multipartite entanglement (but also lower-dimensional quantities could possibly be used).

iv. Relationship to the quantum marginal problem.—The protocol reminds us in several ways of the celebrated quantum marginal problem, one way of formulating it for qubits being as such: Given $m + 1$ parties $A, B_1, \dots, B_m$ and a vector $(s_1, \dots, s_{m+1})$ with entries from $[0, 1/2]$. Is there a pure state $|\psi\rangle_{A,B_1,\dots,B_m}$ such that the spectra of the local reductions of A and B_1 to B_m are $\{s_k, 1 - s_k\}$, $k = 1, \dots, m + 1$? In fact, the feasible region of possible $(s_1, \dots, s_{m+1})$ with a yes answer is a polytope [13]. There are two connections to the marginal problem: On the one hand, the possible combing polytopes are governed by the entropies of collections of subsystems that are consistent with a pure state. On the other hand, one can ask a similar question in entanglement combing: Given one positive point, we easily know there exists one state on which we

comb and obtain the distribution of bipartite states corresponding to this point. A compatibility question is then, given two (or several) points, whether a single pure state exists giving rise to both points under combing.

v. Multipartite quantum communication.—Quite clearly, any multipartite task of quantum communication based on known resources, one can always first bring the multipartite state into a “combed” bipartite form. Then, using the powerful machinery of bipartite pure-state entanglement manipulation, one immediately arrives at bounds of rates to the original protocol. In this sense, we expect this protocol also to be a helpful tool for getting bounds to a number of multipartite quantum communication protocols.

Summary and outlook.—In summary, we have established a new protocol for multipartite pure states, showing that all pure multipartite pure states can be transformed into a bipartite form, entirely preserving the bipartite entanglement with a party. We also identified the convex set of attainable final configurations, giving rise to a new toolbox useful in constructing multipartite tasks and assessing rates for known ones, a perspective that seems quite promising when further fleshing out the potential of multipartite quantum information processing.

We would like to thank D. Gross, M. Christandl, J. Oppenheim, and M. Horodecki for interesting remarks. D.Y. acknowledges the support from NNSF of China (Grant No. 10805043), J.E. support from the EU (QAP, COMPAS, MINOS) and the EURYI.

-
- [1] R. Horodecki *et al.*, Rev. Mod. Phys. **81**, 865 (2009); M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007); J. Eisert and D. Gross, in *Lectures on Quantum Information*, edited by D. Bruss and G. Leuchs (VCH, Weinheim, 2006).
 - [2] This is the celebrated MREGS problem of identifying the *minimal reversible entanglement generating sets* [3].
 - [3] C.H. Bennett *et al.*, Phys. Rev. A **63**, 012307 (2000); N. Linden *et al.*, arXiv:quant-ph/9912039.
 - [4] J.A. Smolin, F. Verstraete, and A. Winter, Phys. Rev. A **72**, 052317 (2005).
 - [5] B. Fortescue and H.-K. Lo, Phys. Rev. Lett. **98**, 260501 (2007); Phys. Rev. A **78**, 012348 (2008).
 - [6] M. Horodecki, J. Oppenheim, and A. Winter, Nature (London) **436**, 673 (2005); Commun. Math. Phys. **269**, 107 (2006).
 - [7] C.H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).
 - [8] D. Leung, J. Oppenheim, and A. Winter, arXiv:quant-ph/0608223.
 - [9] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, New Jersey, 2006).
 - [10] C.H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
 - [11] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
 - [12] D. Slepian and J. K. Wolf, IEEE Trans. Inf. Theory **19**, 471 (1973).
 - [13] A. Klyachko, arXiv:quant-ph/0409113; M. Christandl, A. Harrow, and G. Mitchison, Commun. Math. Phys. **270**, 575 (2007).