AIP Journal of Mathematical Physics

Correlated entanglement distillation and the structure of the set of undistillable states

F. G. S. L. Brandão and J. Eisert

Citation: Journal of Mathematical Physics **49**, 042102 (2008); doi: 10.1063/1.2888925
View online: http://dx.doi.org/10.1063/1.2888925
View Table of Contents: http://scitation.aip.org/content/aip/journal/jmp/49/4?ver=pdfcov
Published by the AIP Publishing

JOURNAL OF MATHEMATICAL PHYSICS **49**, 042102 (2008)

Correlated entanglement distillation and the structure of the set of undistillable states

F. G. S. L. Brandão and J. Eisert[a)]

Institute for Mathematical Sciences, Imperial College London, London SW7 2PE, United Kingdom and QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, United Kingdom

(Received 7 October 2007; accepted 24 January 2008; published online 9 April 2008)

We consider entanglement distillation under the assumption that the input states are allowed to be correlated among each other. We hence replace the usually considered independent and identically distributed hypothesis by the weaker assumption of merely having identical reductions. We find that whether a state is then distillable or not is only a property of these reductions, and not of the correlations that are present in the input state. This is shown by establishing an appealing relation between the set of copy-correlated undistillable states and the standard set of undistillable states: The former turns out to be the convex hull of the latter. As an example of the usefulness of our approach to the study of entanglement distillation, we prove a new activation result, which generalizes earlier findings: It is shown that for every entangled state σ and every k, there exists a copy-correlated k-undistillable state ρ such that $\sigma \otimes \rho$ is single-copy distillable. Finally, the relation of our results to the conjecture about the existence of bound entangled states with a nonpositive partial transpose is discussed. © *2008 American Institute of Physics.* [DOI: 10.1063/1.2888925]

I. INTRODUCTION

The concept of entanglement is at the root of the field of quantum information science. Entanglement is thought to render the envisioned quantum computer more powerful than its classical counterpart and has in some sense to be present to make sure that one can distill a secure classical key in quantum key distribution. Yet, entangled quantum states are not defined via their immediate usefulness for quantum information purposes, but rather via the way they are prepared: A quantum state is called *entangled* if it is not merely *classically correlated*, so it cannot be prepared—in a distributed laboratory paradigm—with local quantum operations alone, making use of classical shared randomness.[1,2] These classically correlated states are hence exactly those states that can be prepared with local distributed physical devices. This definition in terms of the very preparation procedure, needless to say, does not imply *per se* the usefulness of the entanglement.

In turn, "useful entanglement" in a distant laboratories paradigm may be identified with the concept of *distillable entanglement:*[3] a quantum state ρ is called distillable if a supply of states which are independent and identically distributed—in other words $\rho^{\otimes n}$—can be transformed into fewer almost perfect maximally entangled states, again using only local quantum operations and classical communication. Such maximally entangled states of qubit pairs give immediately rise to a secret bit of key in quantum key distribution or may form the resource in quantum state teleportation. A key assumption in such a distillation process is that the source produces identical uncorrelated specimens.

An interesting generalization of this paradigm is the one in which the several copies of the state ρ are not completely independent.[4] It is worthwhile both from a fundamental and practical

[a)]Electronic mail: j.eisert@imperial.ac.uk.

point of view to study the effects of correlations among the copies of ρ on its distillability properties. For each natural number n, instead of considering the usual n uncorrelated copies of the state in question, $\rho^{\otimes n}$, we consider that arbitrary correlations exist among those. Hence, the full state is characterized by a density matrix ω_n with the requirement that $\mathrm{tr}_{\backslash k}(\omega_n)=\rho$ for every $1 \leq k \leq n$, where $\mathrm{tr}_{\backslash k}$ stands for the partial trace of all the copies except kth. Clearly, there are several distinct choices for ω_n, representing the different ways in which the n copies might be correlated. An interesting question in this respect is to classify the set of states for which correlations among its copies can rule out the possibility of obtaining useful entanglement by means of entanglement distillation. It is natural to expect that such correlations could have quite a drastic effect and, hence, that the set of *copy-correlated undistillable states* would be much larger than the usual set of undistillable states. Somewhat surprisingly, it turns out that the existence of correlations do not influence to a very large extend whether distillation can be successfully implemented or not. In fact, the state ω_n does not even have to be assumed to the permutation symmetric: Whether the correlated input is distillable or not merely depends on the reduction ρ, and not on the correlations. We prove that the set of copy-correlated undistillable states is given by the convex hull of the set of undistillable states, therefore providing a new characterization for the latter.

At the core of this result is, of course, the characterization of the set of undistillable states. One of the key results in entanglement theory is that not every entangled state is distillable, demonstrating that there is a kind of *bound entanglement* in nature.[7] In turn, a certain very simple criterion was found to be intimately related to distillability: that of the positivity of the partial transposition, obtained by transposition in only one part of a composite bipartite system.[7,8] A state that has a positive partial transposition is never distillable. What remained a quite notorious question is whether so-called nonpositive partial transpose (NPPT) bound entangled states exist, so states which are not distillable but nevertheless exhibit a NPPT. Its existence has various ramifications in quantum information science[2,9–13] and would rule out the appealing feature of being able to test for undistillability by means of such a simple test as by computing the spectrum of the partial transpose.

One direct implication of our result is that if every undistillable state is PPT (has a positive partial transpose), then arbitrary correlations among the copies of the state in question have no effect at all whether distillation can be successfully implemented. We, however, find that the characterization of the set of copy-correlated undistillable states we establish actually gives strong indications on the existence of NPPT bound entangled states. This is accomplished by proving a new entanglement activation result, which generalizes previous findings[14] and points toward an activation process involving two undistillable states which would, in particular, imply the existence of NPPT states.

Entanglement activation[11–20] is the process in which an entangled state, which by itself would be useless for a given task, e.g., teleportation, can be activated and used as an a resource when processed together with a second state. In the first example of such a phenomenon,[15] it was shown that a certain PPT bound entangled state could be employed in order to increase the fidelity of teleportation of a second state. In Ref. 14, in turn, this result was shown to be a general feature of bound entangled states: Any entangled state can increase the fidelity of teleportation of a second state. In this work, we generalize such a result, proving that for every k, the set of copy-correlated k-undistillable states, which are states for which correlations among k copies of them can prevent the possibility of obtaining a two qubit entangled state by stochastic local operations and classical communication (SLOCC), contains states capable of activating every entangled state. This new activation result we demonstrate then strongly suggests that a similar result might hold true by considering the set of copy-correlated undistillable states itself, which together with its identification with the convex hull of the set of undistillable states, would be sufficient to prove the existence of NPPT states.

The structure of this paper is the following. In Sec. II we define the main quantities which we will be concerned with. In Sec. III, in turn, we state our main results, which are proved subsequently in Secs. IV–VI. In Sec. VII, we discuss the connections of our results with the conjecture about the existence of NPPT bound entangled states. Finally, we present the summary of this work together with some further conclusions in Sec. VIII.

II. DISTILLABILITY AND COPY-CORRELATED DISTILLABILITY

We start by defining the objects we will be using frequently. $\mathcal{H}=\mathbb{C}^d\otimes\mathbb{C}^d$ will denote the Hilbert space of a bipartite $d\times d$-dimensional quantum system. The state space over $\mathcal{H}$ is written as $\mathcal{D}(\mathcal{H})$. Of central interest will be states ρ on $\mathcal{H}^{\otimes k}$ for some k that are *permutation symmetric:* This means that when permuting any of the k bipartite quantum states, the state is left unchanged under the standard representation of the symmetric group S_k over $\mathcal{H}^{\otimes k}$,

$$\rho = P_\pi \rho P_\pi, \tag{1}$$

where P_π is the representation in $\mathcal{H}^{\otimes k}$ of an arbitrary element π of S_k. We define the symmetrization operation as

$$\hat{S}_k(\rho) := \frac{1}{n!}\sum_{\pi\in S_k} P_\pi \rho P_\pi. \tag{2}$$

The set of permutation-symmetric states will be denoted as $\mathcal{S}_k(\mathcal{H}^{\otimes k})\subset\mathcal{D}(\mathcal{H}^{\otimes k})$. We will also freely make use of partial traces over part of systems: $\mathrm{tr}_{\backslash 1}$, for example, will refer to the partial trace over all but the first $d\times d$-dimensional bipartite quantum system.

Note that an early example of entanglement distillation of permutation-symmetric states has been considered in Ref. 21. There, permutation symmetry was even considered when permuting each of the k subsystems individually,

$$\rho' := \frac{1}{n!^2}\sum_{\pi,\pi'\in S_k} (P_\pi\otimes P_{\pi'})\rho(P_\pi\otimes P_{\pi'}), \tag{3}$$

which induces an even higher degree of symmetry than randomly permuting the k bipartite systems, but is included in the above case.

The distillability problem can be cast in terms of a notion that renders it more accessible using the techniques presented later in this work: It is related to the so-called SLOCC *singlet fraction*,

$$F_2(\rho) := \sup_{A,B}\frac{\mathrm{tr}[(A\otimes B)^\dagger \rho(A\otimes B)\phi_2]}{\mathrm{tr}[(A\otimes B)^\dagger \rho(A\otimes B)]}, \tag{4}$$

where A and B act on local parts of a bipartite system with Hilbert space $\mathcal{H}$ and $\phi_2 := \Sigma_{i,j=0}^1 |i,i\rangle\langle j,j|/2$ is the projector onto the two qubit maximally entangled state. In this language, a state ρ is distillable if and only if $F_2(\rho^{\otimes n})>1/2$ for some $n\in\mathbb{N}$. In turn, a state ρ is called n-undistillable if $F_2(\rho^{\otimes n})=\frac{1}{2}$. Finally, the set of undistillable states is composed of all the states that are n-undistillable for all $n\in\mathbb{N}$. We denote the set of n-undistillable states by $\mathcal{C}_n$ and the set of undistillable states by $\mathcal{C}$.

The central object of this work is the generalization of such sets to the case where correlations among the several copies of the state might be present. We are interested in the worst case scenario and say that a state ρ is copy-correlated k-undistillable if there is a one-undistillable state $\omega_k \in \mathcal{D}(\mathcal{H}^{\otimes k})$ such that $\mathrm{tr}_{\backslash m}(\omega_k)=\rho$ for every $1\leq m\leq k$. In other words, if we can add correlations to the k copy state $\rho^{\otimes k}$, forming the state ω_k, such that no two qubit entanglement can be extracted from ω_k, we say that ρ is copy-correlated k-copy undistillable. It is clear that if such an extension exists, then $\hat{S}_k(\omega_k)$ is also a valid extension. It hence follows that without loss of generality we can define the set of copy-correlated k-undistillable states as follows.

Definition 1. (copy-correlated k-undistillable): We say that a bipartite state $\rho\in\mathcal{D}(\mathcal{H})$ is copy-correlated k-undistillable if it has a permutation-symmetric extension $\omega_k\in\mathcal{D}(\mathcal{H}^{\otimes k})$ which is single-copy undistillable. We denote the set of all such states by $\mathcal{T}_k$, i.e.,

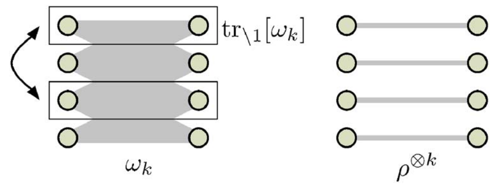

FIG. 1. (Color online) This figure represents the setting of copy-correlated k-undistillable states. The reduction to the first bipartite system is $\mathrm{tr}_{\setminus 1}[\omega_k]$ and the state is invariant under permutations of the bipartite systems. On the right side is the independent and identically distributed case $\rho^{\otimes k}$.

$$\mathcal{T}_k := \{\rho \in \mathcal{D}(\mathcal{H}) : \exists\, \omega_k \in \mathcal{S}_k(\mathcal{H}^{\otimes k}) \cap \mathcal{C}_1(\mathcal{H}^{\otimes k}) \quad \text{such that } \rho = \mathrm{tr}_{\setminus 1}(\omega_k)\}. \tag{5}$$

In the same way as one defines undistillability as k-undistillability for all k, one can introduce an analogous definition in the copy-correlated case (Fig. 1).

In more physical terms, the setting of copy-correlated distillation is the following: One considers sequences of sources, each producing permutation-symmetric correlated bipartite states entailing k pairs each. This is the natural setting when the source produces entangled pairs at once, but the physical process achieving this leads to not entirely uncorrelated specimens. Still, for the reductions to be identical and equal to some ρ is still a reasonable assumption (and the state can also be twirled over the symmetric group to make the reductions identical). In Ref. 22, this concept of formation and distillation beyond independent and identically distributed sources has also been discussed in the pure-state case. Note also that the correlations between the copies can be arbitrarily strong (except that due to monogamy constraints, the resulting state will eventually become copy-correlated undistillable). We do not impose any restrictions to the kind of correlations allowed. If there are no correlations, the usual concept of distillation is recovered.

The parties doing the distillation based on such a source will for a finite k clearly not be able to do a quantum state tomography to find out ρ: They will simply be promised the source to have that property. This is the natural setting of discussing entanglement distillation in the presence of cross-copy correlations and memory effects. Note that we will not be interested in distillation rates in this work, but just in distillability as such. This naturally links to the concept of undistillability.

Definition 2. (copy-correlated undistillable): A state $\rho \in \mathcal{D}(\mathcal{H})$ is said to be copy-correlated undistillable if it is copy-correlated k-undistillable for every $k \in \mathbb{N}$. We denote the set of copy-correlated undistillable states by $\mathcal{T}$, i.e.,

$$\mathcal{T} := \bigcap_{k \in \mathbb{N}^*} \mathcal{T}_k. \tag{6}$$

In other words, a state ρ belongs to $\mathcal{T}$ if for every number of copies of the state one can add correlations among them so that no useful entanglement can be established at all.

This approach seems interesting for two reasons: On the one hand, this is a natural setting to consider, as the assumption of having entirely uncorrelated specimen at hand in entanglement distillation may be an unacceptably restrictive one. On the other hand, as we will see, we can use this concept as a novel mathematical tool to grasp the structure of the set of undistillable states.

Equipped with these definitions, we are now in the position to state our main results and present the proofs.

III. MAIN RESULTS

The first result concerns the relationship between copy-correlated undistillable states and the undistillable states in the ordinary independent and identically distributed sense: We find that the set of copy-correlated undistillable states is nothing but the convex hull of the set of undistillable states. Since the latter set is possibly nonconvex (a property related to the existence of NPPT bound entanglement[11]), the convex hull of this set might, however, indeed be different of the set itself.

Theorem 1. (undistillable and copy-correlated undistillable states): The set of copy-correlated undistillable states is equal to the convex-hull of the set of undistillable states,

$$\mathcal{T} = \mathrm{co}(\mathcal{C}). \tag{7}$$

Our proofs will make repeated use of convex analysis[23] and extend ideas of employing convex cones of Refs. 14 and 20 to the asymptotic setting. The *dual cone* of the set $\mathcal{C}$, for example, is defined as

$$\mathcal{C}^* \coloneqq \{X \geqslant 0 : \mathrm{tr}[X\rho] \geqslant 0 \ \forall \ \rho \in \mathcal{C}\}. \tag{8}$$

Theorem 1 then has the following immediate consequence.

Corollary 1. (characterization of the set of undistillable states): The dual cone of the set of undistillable states can be characterized as follows:

$$\mathcal{C}^* = \overline{\bigcup_{k \in \mathbb{N}^*} \mathcal{T}_k^*}. \tag{9}$$

In other words, we have fully characterized the dual cone of the set of undistillable states in terms of sets which are easily specified.

In the above framework, a standard maximally entangled state of dimension $\mathbb{C}^2 \otimes \mathbb{C}^2$ is taken, as the *singlet fraction* is taken as the figure of merit. Note that we aim for the question of obtaining such a singlet in a distillation protocol, but do not study rates of distillation here. We emphasize, however, that once $\rho \notin \mathcal{T}$, one can distill an arbitrary good approximation of a maximally entangled output of arbitrary dimension. This is the content of the next corollary.

Corollary 2. (distillation with arbitrary output dimension): Let $\rho \in \mathcal{D}(\mathcal{H})$ be a state for which $\rho \notin \mathcal{T}$. Then, for every sequence of states $\{\omega_n\}$ with reductions equal to ρ, every integer D, and every $\lambda \in [1/D, 1)$, there is an integer n and an SLOCC map such that

$$F_D(\omega_n) > \lambda. \tag{10}$$

The second main result is a generalization of the activation result proved in Ref. 14. It indicates the power of copy-correlated k-undistillable states to serve as activators to make states distillable. In fact, this is true on the single-shot level, so the resulting states are even single-copy distillable.[24] Again, the interesting aspect of this result is that it is a statement on asymptotic entanglement manipulation. However, the whole asymptotic aspect is hidden in the characterization of the set of copy-correlated undistillable states: As an activation result, it refers to an operation on a single specimen alone.

Theorem 2. (main result on activation of entanglement): For every entangled state $\rho \in \mathcal{D}(\mathcal{H})$ and every $k \in \mathbb{N}^*$ there is a copy-correlated k-undistillable state σ such that the joint state $\rho \otimes \sigma$ is single-copy distillable, i.e.,

$$F_2(\rho \otimes \sigma) > \tfrac{1}{2}. \tag{11}$$

As $\mathcal{C}_1 = \mathcal{T}_1$, the main result of Ref. 14 is a particular case of Theorem 2. There is an immediate corollary of the previous result which we can state as follows.

Corollary 3. (activation using convex combinations): For every entangled state $\rho \in \mathcal{D}(\mathcal{H})$ and any $\varepsilon > 0$, there is a single-copy undistillable state σ such that the following hold.

(1) *We can find a probability distribution $\{p_i\}$ and a set of undistillable states $\{\rho_i\}$, satisfying*

$$\left\| \sigma - \sum_i p_i \rho_i \right\|_1 \leqslant \varepsilon, \tag{12}$$

(2) *The joint state $\rho \otimes \sigma$ is single-copy distillable.*

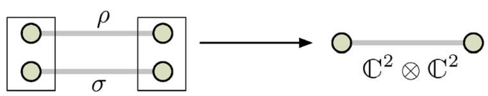

FIG. 2. (Color online) Activation of entanglement: For any entangled state ρ, one can find a copy-correlated k-undistillable activator σ such that the joint state is single-copy distillable. This holds true for any k.

This corollary is a direct consequence of Theorem 2 and a standard result of convex analysis stating that a family of closed convex sets $\{A_i\}$ such that $A_{i+1} \subseteq A_i$ converges to their intersection with respect to the Hausdorff distance.[25]

Motivated by these findings, we are–once again—led to the following conjecture. Note that recent work on the existence of NPPT bound entangled states has introduced interesting ideas,[31] but the argument as such is not correct in its conclusion. To assume that the extreme points of the convex sets constructed in Ref. 31 are pure is a restriction of generality. For a discussion, see also Ref. 2. Note the strong similarity with the previous statement (Fig. 2).

Conjecture 1 (existence of NPPT bound entanglement): For every entangled state $\rho \in \mathcal{D}(\mathcal{H})$, *there is an undistillable state* σ *such that the joint state* $\rho \otimes \sigma$ *is single-copy distillable, i.e.*,

$$F_2(\rho \otimes \sigma) > \tfrac{1}{2}. \tag{13}$$

This statement would clearly indicate the existence of NPPT bound entangled states. To see this, let us assume that the contrary is true, which all undistillable states have a positive partial transpose. Yet, according to the above conjecture, for any PPT bound entangled state σ, there exists an undistillable state ρ—hence also a PPT state—for which $F_2(\rho \otimes \sigma) > \frac{1}{2}$. This leads to a contradiction, as $\rho \otimes \sigma$ has in turn a positive partial transpose, which implies that

$$F_2(\rho \otimes \sigma) = \tfrac{1}{2}, \tag{14}$$

in contradiction to the assumption. Hence, our above result is also aimed at providing a new instrument in tackling the old conjecture on the existence of NPPT bound entanglement. For recent progress on the question of the existence of NPPT distillable entanglement, see also Ref. 32.

IV. PROOF OF THEOREM 1

We will now proceed by proving the validity of the two theorems. We start with the preparation of the proof of Theorem 1. This argument will make use of de Finetti and large deviation techniques.[33–35] The first statement that is of use is borrowed from Ref. 34. Note that here it is stated with respect to bipartite systems, which is responsible for the obvious difference in the scaling in the dimension d.

Theorem 3 (quantum finite de Finetti theorem[34]): Let ω_n *be a permutation-symmetric state* $\omega_n \in \mathcal{S}_n(\mathcal{H}^{\otimes n})$ *and let* $k \leq n$. *Then there exists a probability distribution P over state space* $\mathcal{D}(\mathcal{H})$ *such that*

$$\left\| \mathrm{tr}_{k+1,\ldots,n}(\omega_n) - \int P(\rho)\rho^{\otimes k} d\rho \right\|_1 \leq \frac{4d^4 k}{n}. \tag{15}$$

With the help of the previous statement, we can characterize the set of copy-correlated undistillable states. Note that the following lemma does not constitute an assumption on the specific form of the correlations between the copies produced by the source, but it is a result that holds true as a consequence to any input states having such correlations.

Lemma 1 (set of copy-correlated undistillable states): A state $\sigma \in \mathcal{D}(\mathcal{H})$ *belongs to* $\mathcal{T}$ *if and only if there exists a probability distribution P over state space* $\mathcal{D}(\mathcal{H})$ *such that*

$$\sigma = \int P(\rho)\rho d\rho \tag{16}$$

and

$$\pi_k := \int P(\rho)\rho^{\otimes k} d\rho \in \mathcal{C}_1(\mathcal{H}^{\otimes k}) \tag{17}$$

for every $k \in \mathbb{N}^*$.

Proof: Let $\sigma \in \mathcal{T}$, then, for each $k \in \mathbb{N}^*$, there exists a state $\omega_k \in \mathcal{C}_1(\mathcal{H}^{\otimes k})$ such that $\mathrm{tr}_{\backslash 1}(\omega_k) = \sigma$. This is a direct consequence of the definition of $\mathcal{T}$. From Theorem 3, it follows that for each $k \geqslant 1$, there exists a probability distribution $P_k(\rho)$ such that

$$\left\| \mathrm{tr}_{k+1,\ldots,k^2}(\omega_{k^2}) - \int P_k(\rho)\rho^{\otimes k} d\rho \right\|_1 \leqslant \frac{4d^4}{k}. \tag{18}$$

Let us define

$$\pi_j^k := \mathrm{tr}_{j+1,\ldots,k^2}(\omega_{k^2}). \tag{19}$$

From the property that the trace norm is contractive under completely positive maps, and hence under partial tracing, we have that for each $j \leqslant k$,

$$\left\| \pi_j^k - \int P_k(\rho)\rho^{\otimes j} d\rho \right\|_1 \leqslant \frac{4d^4}{k}. \tag{20}$$

Moreover, as locally discarding some part of a state amounts to a LOCC operation, we have that each

$$\pi_j^k \in \mathcal{C}_1(\mathcal{H}^{\otimes j}). \tag{21}$$

The set of probabilities on the state space is compact in the weak topology. So there is a probability measure P and a net $k(\alpha)$ of integers such that $k(\alpha) \to \infty$ and $P_{k(\alpha)} \to P$. The map

$$P \to \int P(\rho)\rho^{\otimes j} d\rho \tag{22}$$

is continuous, so it also follows that

$$\int P_{k(\alpha)}(\rho)\rho^{\otimes j} d\rho \to \int P(\rho)\rho^{\otimes j} d\rho. \tag{23}$$

Then, by Eq. (20), we find that for every $j \in \mathbb{N}^*$,

$$\pi_j^{k(\alpha)} \to \int P(\rho)\rho^{\otimes j} d\rho. \tag{24}$$

As for every $k(\alpha)$ and j,

$$\mathrm{tr}_{\backslash 1}(\pi_j^{k(\alpha)}) = \sigma \quad \text{and } \pi_j^{k(\alpha)} \in \mathcal{C}_1, \tag{25}$$

it follows that

$$\mathrm{tr}_{\backslash 1}\left(\int P(\rho)\rho^{\otimes j} d\rho \right) = \sigma \quad \text{and } \int P(\rho)\rho^{\otimes j} d\rho \in \mathcal{C}_1 \tag{26}$$

hold true for every $j \in \mathbb{N}^*$. The converse direction of the proof follows directly from the definition of $\mathcal{T}$. □

The next concept that we need is that of a minimal informationally complete positive operator valued measure (POVM). An *informationally complete POVM* in $\mathcal{B}(\mathbb{C}^m)$ is defined as a set of positive semidefinite operators A_i forming a resolution of the identity, i.e., satisfying

$$\sum_i A_i = \mathbb{I}. \tag{27}$$

In addition, $\{A_i\}$ has to form a basis for $\mathcal{B}(\mathbb{C}^m)$. An informationally complete POVM is said to be *minimal*, in turn, when each operator $X \in \mathcal{B}(\mathbb{C}^m)$ is uniquely determined by the expectation values $\mathrm{tr}[A_i X]$. We will make use of a construction of minimal informationally complete POVMs presented in Ref. 35, valid for all dimensions m.

We say that a family $\{A_i\}$ of elements from $\mathcal{B}(\mathbb{C}^m)$ is a *dual* of the a family $\{A_i^*\}$ if for all $X \in \mathcal{B}(\mathbb{C}^m)$,

$$X = \sum_i \mathrm{tr}[A_i X] A_i^*. \tag{28}$$

The above equation implies, in particular, that the operator X is fully determined by the expectations values $\mathrm{tr}[A_i X]$. Finally, if $\{A_i\}$ and $\{B_j\}$ are informationally complete POVMs on $\mathcal{B}(\mathbb{C}^m)$ and $\mathcal{B}(\mathbb{C}^l)$, then $\{M_{i,j}\}$, defined by

$$M_{i,j} := A_i \otimes B_j, \tag{29}$$

is an informationally complete POVM on $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^l)$. Before now turning to the proof of Theorem 1, there is one last ingredient that we need for our argument: It may be viewed as a variant of a Chernoff bound. Note that this is a statement on classical probability distributions, not on quantum states.

Lemma 2 (variant of Chernoff's bound[36]): Let P_X be a probability distribution on $\mathcal{X}$ and let x be chosen according to the n-fold product distribution $(P_X)^n$. Then, for any $\delta > 0$,

$$\mathrm{Pr}_x[\|\lambda_x - P_X\|_1 > \delta] \leq 2^{-n((\delta^2/2\ \ln 2) - |\mathcal{X}|(\log(n+1)/n))}. \tag{30}$$

Here, $\|\cdot\|_1$ is the trace distance of two probability distributions and $|\mathcal{X}|$ is the cardinality of $\mathcal{X}$.

Proof of Theorem 1: We proceed by showing that both $\mathrm{co}(\mathcal{C}) \subseteq \mathcal{T}$ and $\mathcal{T} \subseteq \mathrm{co}(\mathcal{C})$ hold true. We start with the first inclusion, which is quite straightforward. Let $\rho \in \mathcal{C}(\mathcal{H})$ be an undistillable state. By symmetry, it is clearly true that the state $\rho^{\otimes n}$ belongs to $\mathcal{S}_n(\mathcal{H}^{\otimes n})$ for all n. Moreover, $\rho^{\otimes n}$ is by definition not single-copy distillable. Therefore, $\rho^{\otimes n}$ belongs to $\mathcal{C}_1(\mathcal{H}^{\otimes n})$. Hence, for all n, $\rho^{\otimes n} \in \mathcal{S}_n(\mathcal{H}^{\otimes n}) \cap \mathcal{C}_1(\mathcal{H}^{\otimes n})$, from which it follows that $\rho \in \mathcal{T}$. As $\mathcal{T}$ is a closed convex set, one finds that indeed $\mathrm{co}(\mathcal{C}) \subseteq \mathcal{T}$.

Let us now consider the converse inclusion. To this aim, let $\pi \in \mathcal{T}$. Then, for each $n \in \mathbb{N}^*$, there exists a π_n given by Eq. (17) such that

$$\mathrm{tr}_{\backslash 1}[\pi_n] = \pi. \tag{31}$$

Also, Lemma 1 defines a probability distribution P for π, independent of n. Similarly, for any $n, m \in \mathbb{N}^*$, we find a π_{n+m}.

We will now show that this probability distribution P is up to a set of measure zero supported only on undistillable states. We do this proving that for every $n \in \mathbb{N}^*$, the probability function $P(\rho)$ vanishes for all n-distillable states, except from a set of measure zero. The ideas of the argument is as follows: We consider π_{n+m} and construct a SLOCC that performs measurements based on an informationally complete POVM in the last m systems. Based on this information, one performs a further operation on the first n systems depending whether it is distillable or not.

More specifically, for any $n, m \in \mathbb{N}^*$, we define the SLOCC map $\Lambda_{m,n} : \mathcal{B}(\mathcal{H}^{\otimes(m+n)}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ as follows.

- We first measure the informationally complete POVM $\{M_{i,j}\} := \{M_k\}$ of Eq. (29) individually on each of the last m bipartite systems, where k is the joint index labeling the outcomes. This

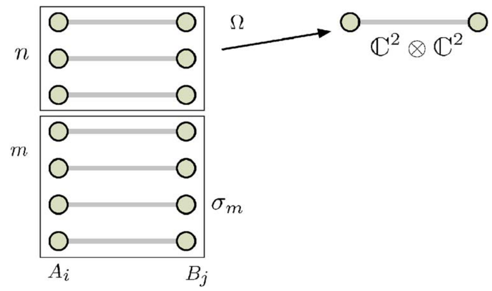

FIG. 3. (Color online) Procedure followed to define the SLOCC map Ω.

is clearly an operation that can be implemented by means of LOCC: One has to perform the local POVM on each side. In this way, one can estimate an empirical probability distribution $P_m(k)$ from the relative frequency of the outcomes k of the POVM.

- Then, using Eq. (28), we form the operator

$$X_m = \sum_k P_m(k) M_k^* \in \mathcal{B}(\mathcal{H}). \tag{32}$$

Of course, this might not be a valid density operator.

- Thus, we define $\sigma_m \in \mathcal{D}(\mathcal{H})$ as the state which is closest in trace norm to X_m, so as the state that minimizes

$$\{\|\sigma_m - X_m\|_1 : \sigma_m \in \mathcal{D}(\mathcal{H})\}. \tag{33}$$

This is done based on the measurement outcomes obtained above. If σ_m defined in this way is not unique, we select one from the respective set of solutions. The state σ_m can now either be n-distillable or n-undistillable. Note that so far the only physical operation performed was the measurement in the last m systems.

- In the first case, so if $\sigma_m \in \mathcal{D}(\mathcal{H})$ is n-distillable, we apply the trace preserving LOCC map Ω on the remaining n systems which minimizes the following expectation value (Fig. 3):

$$\mathrm{tr}[\Omega(\sigma_m^{\otimes n})(\mathbb{I}/2 - \phi_2)]. \tag{34}$$

This is the optimal distillation procedure on n copies, $\Omega : \mathcal{B}(\mathcal{H}^{\otimes n}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. The map $\rho \mapsto \mathrm{tr}[\Omega(\rho^{\otimes n})(\mathbb{I}/2 - \phi_2)]$, where Ω is the trace-preserving LOCC that minimizes $\mathrm{tr}[\Omega(\rho^{\otimes n})(\mathbb{I}/2 - \phi_2)]$, is trace-norm continuous.

- In the second case, so if $\sigma_m \in \mathcal{D}(\mathcal{H})$ is n-undistillable, we discard the state and replace it by the zero operator on $\mathcal{H}^{\otimes n}$.

This procedure defines our family of SLOCC operations $\Lambda_{m,n} : \mathcal{B}(\mathcal{H}^{\otimes (m+n)}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. We know that

$$\mathrm{tr}[\Lambda_{n,m}(\pi_{n+m})(\mathbb{I}/2 - \phi_2)] \geqslant 0 \tag{35}$$

for all m, as, by Lemma 1, $\pi_{n+m} \in \mathcal{C}_1(\mathcal{H}^{\otimes (n+m)})$.

From Lemma 2, we can infer that the probability that the trace norm difference of the estimated state with the real state is larger than ε, for any $\varepsilon > 0$, goes to zero when m goes to infinity. So we find that the family of functions, defined for states $\rho \in \mathcal{D}(\mathcal{H})$ as

$$f_m(\rho) = \mathrm{tr}[\Lambda_{m,n}(\rho^{\otimes (n+m)})(\mathbb{I}/2 - \phi_2)] \tag{36}$$

for fixed $\Lambda_{m,n}$ for any n, m, converge pointwise to

$$f(\rho) := \begin{cases} \mathrm{tr}[\Xi_\rho(\rho^{\otimes n})(\mathbb{I}/2 - \phi_2)] & \text{if } \rho \text{ is } n\text{-distillable} \\ 0 & \text{otherwise,} \end{cases} \tag{37}$$

where $\Xi_\rho : \mathcal{B}(\mathcal{H}^{\otimes n}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is the optimal LOCC map for $\rho^{\otimes n}$, i.e., the LOCC map that minimizes

$$\mathrm{tr}[\Xi(\rho^{\otimes n})(\mathbb{I}/2 - \phi_2)]. \tag{38}$$

To proceed, we clearly have the upper bound

$$|f_m(\rho)| = |\mathrm{tr}[\Lambda_{m,n}(\rho^{\otimes(n+m)})(\mathbb{I}/2 - \phi_2)]| \leq 1 \tag{39}$$

for every $\rho \in \mathcal{D}(\mathcal{H})$. This means that the family of functions $\{f_m\}$ satisfies the requirements of the Lebesgue dominated convergence theorem. Therefore, we get from Eq. (35) that

$$0 \leq \lim_{m\to\infty} \int P(\rho)\mathrm{tr}[\Lambda_{m,n}(\rho^{\otimes(n+m)})(\mathbb{I}/2 - \phi_2)]d\rho = \lim_{m\to\infty} \int P(\rho) f_m(\rho) d\rho = \int P(\rho) \lim_{m\to\infty} f_m(\rho) d\rho$$

$$= \int P(\rho) f(\rho) d\rho = \int_{\mathcal{D}(\mathcal{H})\backslash\mathcal{C}_n(\mathcal{H})} P(\rho)\mathrm{tr}[\Xi_\rho(\rho^{\otimes n})(\mathbb{I}/2 - \phi_2)]d\rho, \tag{40}$$

where $\mathcal{D}(\mathcal{H})\backslash\mathcal{C}_n(\mathcal{H})$ are the n-distillable states. By definition, we have that for each n-distillable state ρ,

$$\mathrm{tr}[\Omega(\rho^{\otimes n})(\mathbb{I}/2 - \phi_2)] < 0. \tag{41}$$

So we find from Eq. (40) that P can be nonzero only in a zero measure subset of the set of n-distillable states. As this is true for an arbitrary n, we find that $P(\rho)$ must be supported on the set of undistillable states. □

Proof of Corollary 2: We can prove the Corollary by contradiction. Suppose conversely that for every $n \in \mathbb{N}$ and every SLOCC Ω, $\mathrm{tr}[\Omega(\omega_n)(\lambda\mathbb{I} - \phi_D)] \geq 0$. Then, we can follow the proof of Theorem 1 to show that $\rho \in \mathcal{T}$, in contradiction with the assumption that it is not.

The key point is to notice that Theorem 1 also holds if we replace the single copy undistillability condition $F_2(\omega_n) = \frac{1}{2}$ by $F_D(\omega_n) \leq \lambda$ for any integer D and $\lambda \in [1/D, 1)$. We only have to modify the fourth step of the SLOCC map we defined as follows: we now discard the state if the estimated state σ_m is such that $\mathrm{tr}[\Omega(\sigma_m^{\otimes n})] \leq \lambda$ for every SLOCC map Ω or apply the optimal SLOCC map Ω minimizing $\mathrm{tr}[\Omega(\sigma_m^{\otimes n})(\lambda\mathbb{I} - \phi_D)]$ otherwise. The proof then proceeds in a completely analogous way. □

V. PROOF OF THEOREM 2

We now turn to the proof of Theorem 2. We start by proving two auxiliary Lemmas, which give a characterization for the elements of the dual cones of the sets $\mathcal{S}_k(\mathcal{H}^{\otimes k})$ and $\mathcal{T}_k(\mathcal{H}^{\otimes k})$, which will again sometimes be abbreviated as $\mathcal{S}_k$ and $\mathcal{T}_k$.

Lemma 3 (dual cone of symmetric states): If $Q \in (\mathcal{S}_k)^*$, then

$$\hat{S}_k(Q) = \frac{1}{n!} \sum_{\pi \in S_k} P_\pi Q P_\pi \geq 0. \tag{42}$$

Proof: As $Q \in (\mathcal{S}_k)^*$, we have that for every positive semidefinite operator $X \geq 0$ acting on $\mathcal{H}^{\otimes k}$,

$$\mathrm{tr}[X\hat{S}_k(Q)] = \mathrm{tr}[\hat{S}_k(X)Q] \geq 0. \tag{43}$$

This can only be true, however, if $\hat{S}_k(Q) \geq 0$. □

Lemma 4 (dual cone of k-copy undistillable states): For each $k \in \mathbb{N}$ and for every element X of $\mathcal{T}_k^*$, there exist an SLOCC map Λ and an operator $Q \in (\mathcal{S}_k)^*$ such that

$$X \otimes \mathbb{I}^{\otimes(k-1)} = \Lambda(\mathbb{I}/2 - \phi_2) + Q. \tag{44}$$

Proof: In Ref. 37, it has been shown that for any two closed convex cones A and B defined on a finite dimensional Hilbert space, $(A \cap B)^* = A^* + B^*$. It is easily seen that $\text{cone}(\mathcal{S}_k \cap \mathcal{C}_1) = \text{cone}(\mathcal{S}_k) \cap \text{cone}(\mathcal{C}_1)$, where the *conic hull* is defined for a set C as

$$\text{cone}(A) := \left\{ \sum_j \lambda_j W_j : \lambda_j \geq 0, W_j \in C \right\}. \tag{45}$$

Therefore,

$$(\mathcal{S}_k \cap \mathcal{C}_1)^* = [\text{cone}(\mathcal{S}_k \cap \mathcal{C}_1)]^* = [\text{cone}(\mathcal{S}_k) \cap \text{cone}(\mathcal{C}_1)]^* = \mathcal{S}_k^* + \mathcal{C}_1^*. \tag{46}$$

This in turn implies that every element Y of $(\mathcal{S}_k \cap \mathcal{C}_1)^*$ can be written as the right hand side of Eq. (44). We find that if

$$X \in \mathcal{T}_k^*, \tag{47}$$

then $X \otimes \mathbb{I}^{\otimes(k-1)}$ is an element of $(\mathcal{S}_k \cap \mathcal{C}_1)^*$. Indeed,

$$\text{tr}[X\rho] \geq 0 \;\forall\; \rho \in \mathcal{T}_k \Rightarrow \text{tr}[X \text{tr}_{\setminus 1}(\pi)] \geq 0 \;\forall\; \pi \in \mathcal{S}_k \cap \mathcal{C}_1 \Rightarrow \text{tr}[(X \otimes \mathbb{I}^{\otimes(k-1)})\pi] \geq 0 \;\forall\; \pi \in \mathcal{S}_k \cap \mathcal{C}_1. \tag{48}$$

Hence, any element of the dual cone of $\mathcal{T}_k$ can be written as a sum of an element of the dual cone of $\mathcal{S}_k$ and an element of the dual cone of $\mathcal{C}_1$, which is nothing but $\Lambda(\mathbb{I}/2 - \phi_2)$. □

The next Lemma is the key result for the proof of Theorem 2. It makes a connection between separability and the structure of the dual sets $(\mathcal{T}_k)^*$. Before, we turn to its formulation and proof, let us introduce some notation, departing from earlier conventions. This will make render the argument more transparent, however. In this lemma, we will set $\mathcal{H} := \mathbb{C}^{2d} \otimes \mathbb{C}^{2d}$. If we have a tensor product between a $d \times d$-system and a 2×2 system, the latter is thought to be embedded in a $d \times d$-dimensional system. We denote with $\mathbb{I}$ the identity operator acting on $\mathcal{H}$. The identity operator acting on $\mathbb{C}^m \otimes \mathbb{C}^m$ for every other m different from $2d$ will be denoted by $\mathbb{I}_{m^2}$.

Lemma 5 (dual cone of $\mathcal{T}_k$ and separability): Let $\sigma \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ and $k \in \mathbb{N}^*$. If

$$\sigma \otimes (\mathbb{I}_4/2 - \phi_2) \in (\mathcal{T}_k)^*, \tag{49}$$

then σ is separable.

Proof: By Lemma 4, we can write

$$\sigma \otimes (\mathbb{I}_4/2 - \phi_2) \otimes \mathbb{I}^{\otimes(k-1)} = \Lambda(\mathbb{I}_4/2 - \phi_2) + Q \tag{50}$$

for some SLOCC map Λ and an operator $Q \in \mathcal{S}_k^*$. Applying the symmetrizing operator $\hat{S}$ to both sides of the previous equation, we find

$$\sigma \otimes (\mathbb{I}_4/2 - \phi_2) \otimes \mathbb{I}^{\otimes(k-1)} + \sum_{j=1}^{k} \mathbb{I}^{\otimes j} \otimes (\sigma \otimes (\mathbb{I}_4/2 - \phi_2)) \otimes \mathbb{I}^{\otimes(k-j-1)} = (\hat{S} \circ \Lambda)(\mathbb{I}_4/2 - \phi_2) + \hat{S}(Q). \tag{51}$$

We now multiply both sides from the left with $\mathbb{I} \otimes (\mathbb{I}_{d^2} \otimes |0,0\rangle\langle 0,0|)^{\otimes(k-1)}$ and take the partial trace with respect to all systems except the first $\mathbb{C}^{2d} \otimes \mathbb{C}^{2d}$-dimensional subsystem. Defining

$$P := \text{tr}_{\setminus 1}[\mathbb{I} \otimes (\mathbb{I}_{d^2} \otimes |0,0\rangle\langle 0,0|)^{\otimes(k-1)} \hat{S}(Q)], \tag{52}$$

$$\Upsilon(.) := \text{tr}_{\setminus 1}[\mathbb{I} \otimes (\mathbb{I}_{d^2} \otimes |0,0\rangle\langle 0,0|)^{\otimes(k-1)} (\hat{S} \circ \Lambda)(.)], \tag{53}$$

it follows that

$$\sigma \otimes (\mathbb{I}_4/2 - \phi_2) = \Upsilon(\mathbb{I}_4/2 - \phi_2) + P, \tag{54}$$

since

$$\mathrm{tr}[(\mathbb{I}_{d^2} \otimes |0,0\rangle\langle 0,0|)(\mathbb{I}_4/2 - \phi_2)] = 0. \tag{55}$$

By Lemma 3, we find that $P \geqslant 0$.

The quantum operation Υ can easily be seen to be a SLOCC, as it is a concatenation of the SLOCC map Ω with the symmetrizing operation—which is LOCC—and finally with the projection of the qubit part of the final $k-1$ copies in the local state $|0,0\rangle$, followed by tracing over them. Each of these steps can be done locally. The statement of the lemma then follows from the results presented in Ref. 14, where it was shown that Eq. (54) implies the separability of the bi-partite state $\sigma \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$. □

Proof of Theorem 2: Theorem 2 can now be easily established by Lemma 5, together with the argument presented in Ref. 14. Let us consider states $\sigma \in \mathcal{D}((\mathcal{H}_{A_2} \otimes \mathcal{H}_{A_3}) \otimes (\mathcal{H}_{B_2} \otimes \mathcal{H}_{B_3}))$, where

$$\mathcal{H}_{A_2} = \mathcal{H}_{B_2} = \mathbb{C}^d, \quad \mathcal{H}_{A_3} = \mathcal{H}_{B_3} = \mathbb{C}^2. \tag{56}$$

The Hilbert spaces $\mathcal{H}_{A_1} = \mathbb{C}^d$ and $\mathcal{H}_{B_1} = \mathbb{C}^d$ will serve as the Hilbert spaces on which the activator ρ is defined. This might seem like an undesirable complication of notation; as in Ref. 14, the discussion of the process will become more transparent in this way, however.

We aim at activating entanglement. It hence suffices to show that for all $k \in \mathbb{N}^*$, there exists a $\rho \in \mathcal{T}_k \subset \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ and a SLOCC operation Λ such that

$$\mathrm{tr}[\Lambda(\sigma \otimes \rho)\phi_2] > \mathrm{tr}[\Lambda(\sigma \otimes \rho)]/2. \tag{57}$$

The state ρ then serves as an activator in this single-copy distillation process.

We are free to show that Eq. (57) is true for a particular choice of a SLOCC operation. This does not necessarily have to be one that would give the optimal rate or in the single-copy regime the optimal overlap, as long as we can show that the activation has been successful. We choose Λ as follows: As a first step, the parties perform a local measurement—on subsystems A_1A_2 and B_1B_2—in a basis of maximally entangled states, postselecting when both systems are projected onto the projectors associated with the unnormalized state vectors $|\phi_{A_1A_2}\rangle = \Sigma_{i=1}^d |i,i\rangle$ and $|\phi_{B_1B_2}\rangle = \Sigma_{i=1}^d |i,i\rangle$, respectively. The implemented SLOCC is then given by

$$\rho \otimes \sigma \mapsto (A \otimes B)(\rho \otimes \sigma)(A \otimes B)^\dagger, \tag{58}$$

where

$$A = \langle \phi_{A_1A_2}| \otimes \mathbb{I}_{A_3}, \quad B = \langle \phi_{B_1B_2}| \otimes \mathbb{I}_{B_3}, \tag{59}$$

and $|\phi_{A_1A_2}\rangle$ is the state vector of a maximally entangled state in the Schmidt basis.

This construction is nothing but the extended Jamiolkowski isomorphism between bipartite states and nonlocal operations, see, e.g., Ref. 38: By performing two joint measurements locally on the states ρ and σ, a nonlocal quantum operation, determined by ρ, will be performed in σ. For our purposes, it is sufficient to consider the following relation:

$$\mathrm{tr}[(A \otimes B)(\rho \otimes \sigma)(A \otimes B)^\dagger Z] = c\ \mathrm{tr}[\rho(\sigma^T \otimes Z)] \tag{60}$$

for every positive operator Z on $\mathcal{H}_{A_3} \otimes \mathcal{H}_{B_3}$ and for some $c > 0$.

The condition $\mathrm{tr}[\Lambda(\rho \otimes \sigma)\phi_2] > \mathrm{tr}[\Lambda(\sigma \otimes \rho)]/2$ can clearly be written as

$$\mathrm{tr}[\Lambda(\rho \otimes \sigma)(\mathbb{I}/2 - \phi_2)] < 0. \tag{61}$$

Hence, from Eq. (60), we get

$$\mathrm{tr}[\rho\sigma^T \otimes (\mathbb{I}/2 - \phi_2)] < 0. \tag{62}$$

To complete the proof it suffices to note that by Lemma 5, if σ is entangled then there must be a state $\rho \in \mathcal{T}_k$ satisfying Eq. (62). Indeed, if this were not true, then $\sigma^T \otimes (\mathbb{I}/2 - \phi_2)$ would have to belong to the dual cone of $\mathcal{T}_k$, which was shown in Lemma 5 to imply the separability of σ. This proves the validity of Theorem 2. □

VI. PROOF OF COROLLARY 3

Proof of Corollary 3: It is easy to see that it is sufficient to prove that

$$\mathrm{cl}(\mathrm{cone}(\bigcup_{k\in\mathbb{N}^*} \mathcal{T}_k^*)) = \mathcal{T}^*, \tag{63}$$

where $\mathrm{cl}(A)$ is the closure of A. Let us first show that

$$\mathrm{cl}(\mathrm{cone}(\bigcup_{k\in\mathbb{N}^*} \mathcal{T}_k^*)) \subseteq \mathcal{T}^*. \tag{64}$$

Choose an element Y of $\mathcal{T}_k^*$. Then, $\mathrm{tr}[XY] \geq 0$ for all $X \in \mathcal{T}_k$ and, therefore, for all $X \in \cap_{k\in\mathbb{N}^*}\mathcal{T}_k = \mathcal{T}$. Hence, Y is an element of $\mathcal{T}^*$ as well. Thus, for all $k \geq 1$,

$$\mathcal{T}_k^* \subseteq \mathcal{T}^*, \tag{65}$$

from which follows that

$$\bigcup_{k\in\mathbb{N}^*} \mathcal{T}_k^* \subseteq \mathcal{T}^*. \tag{66}$$

As $\mathcal{T}^*$ is a closed convex cone, we get Eq. (64).

To prove the converse inclusion, we show the following relation:

$$(\bigcup_{k\in\mathbb{N}^*} \mathcal{T}_k^*)^* \subseteq \bigcap_{k\in\mathbb{N}^*} \mathrm{cone}(\mathcal{T}_k). \tag{67}$$

Then, using that $\mathrm{cl}(\mathrm{cone}(B)) \subseteq \mathrm{cl}(\mathrm{cone}(A))$ if $A^* \subseteq B^*$ together with the easily established relation

$$\mathrm{cone}(\bigcap_{k\in\mathbb{N}^*} \mathcal{T}_k) = \bigcap_{k\in\mathbb{N}^*} \mathrm{cone}(\mathcal{T}_k), \tag{68}$$

we find the announced result.

Let us then turn to prove Eq. (67). Choose an element X of $(\cup_{k\in\mathbb{N}^*}\mathcal{T}_k^*)^*$. Then,

$$\mathrm{tr}[XY] \geq 0 \tag{69}$$

for all $Y \in \cup_{k\in\mathbb{N}^*}\mathcal{T}_k^*$, which implies that $\mathrm{tr}[XY] \geq 0$ for all $Y \in \mathcal{T}_k^*$ and for all $k \geq 1$. Therefore,

$$X \in (\mathcal{T}_k^*)^*, \tag{70}$$

which is equal to $\mathrm{cone}(\mathcal{T}_k)$. As this is true for all $k \geq 1$, we arrive at Eq. (67) □.

VII. ON THE EXISTENCE OF NPPT BOUND ENTANGLEMENT

Before we conclude this work, we would like to comment on the applicability on this approach to the conjecture on the existence of bound entangled states with a nonpositive partial transpose and, in particular, to Conjecture 1. The kind of statement that we would need is very similar to the one established here: We have introduced an idea of how to grasp asymptotic entanglement manipulation in the form of a single-copy activation argument. It is clear that if we could prove the validity of Lemma 5 for the full set $\mathcal{T}$, then Conjecture 1 would in fact be true.

Indeed, if the activation procedure outlined in the proof of Theorem 2 works for a convex combination of undistillable states, then it has to work at least for one of the states appearing in the convex combination, as it is made explicit by the linearity of Eq. (62).

However, although the presented methods seem applicable to this question, a significant further step seems to be necessary, and a naive extension of Lemma 5 to $\mathcal{T}$ does not seem to work. Indeed, if we assume that $\sigma\otimes(\mathbb{I}_4/2-\phi_2)\in\mathcal{T}^*$, then, by Corollary 3, for every $\varepsilon>0$, there exists an integer n_ε such that

$$\sigma\otimes(\mathbb{I}_4/2-\phi_2)+\varepsilon\mathbb{I}\in(\mathcal{T}_{k_\varepsilon})^*. \tag{71}$$

If we followed the steps taken in the proof of Lemma 5, we would find, instead of Eq. (54), the following:

$$\sigma\otimes(\mathbb{I}_4/2-\phi_2)+(n_\varepsilon-1)\varepsilon\mathbb{I}=\Omega_\varepsilon(\mathbb{I}/2-\phi_2)+P_\varepsilon, \tag{72}$$

where $P_\varepsilon\geqslant 0$ and Ω_ε is a SLOCC operation for every $\varepsilon>0$. Hence, in order to be able to carry over with the approach similar to one outlined in Ref. 14, we would have to be able to show that we can choose the sequence $\{n_\varepsilon\}$ to be such that

$$\lim_{\varepsilon\to 0}(n_\varepsilon-1)\varepsilon=0. \tag{73}$$

Although it could well be the case that such relation hold, we could not find a way either to prove it nor to disprove it, despite considerable effort.

From a different perspective, it seems that the rate of convergence of an arbitrary element of $\mathcal{T}^*$ by elements of the inner approximations given by $\mathcal{T}_k^*$ matters when it comes to the activation properties of the elements of $\mathcal{T}$. Note that it is exactly the closure in

$$\mathcal{T}^*=\overline{\bigcup_{k\in\mathbb{N}^*}\mathcal{T}_k^*} \tag{74}$$

that is responsible for this behavior. Indeed, Lemma 5 can straightforwardly be applied if we require only that

$$\sigma\otimes(\mathbb{I}_4/2-\phi_2)\in\bigcup_{k\in\mathbb{N}^*}\mathcal{T}_k^*. \tag{75}$$

So the question of the existence of NPPT bound entanglement can be related and reduced to the question of the necessity of the convex hull in Eq. (74).

VIII. SUMMARY AND CONCLUSIONS

In this work, we have introduced the notion of copy-correlated entanglement distillation. In this setting, one allows for correlations between different specimens in entanglement distillation. We have proven a relationship between copy-correlated undistillable states and undistillable states, hence establishing a new way of characterizing the set of undistillable states. We have also introduced a new entanglement activation result which, on one hand, generalizes previous ones and, on the other hand, might be of use to the study of the properties of the undistillable state set.

After all, it is not a too unrealistic hope that the methods this work has introduced may pave an avenue to prove the validity of the conjecture on the existence of NPPT bound entanglement. With new results on almost independent and identically distributed properties of many subsystems of permutation invariant being just available,[39] this goal may be within reach. Beyond this specific question of entanglement distillation, we hope that the presented methods and tools open up a new way of grasping asymptotic entanglement manipulation.

ACKNOWLEDGMENTS

We acknowledge fruitful and interesting conversations with a number of people on these and very closely related topics, among them D. Gottesman, D. Gross, M. Horodecki, Ll. Masanes, B. Terhal, J. Oppenheim, M. Piani, M.B. Plenio, S. Virmani, K. G. H. Vollbrecht, and R. F. Werner. This work has been supported by the EU (QAP), the Royal Society, the QIP-IRC, Microsoft Research, the Brazilian agency CNPq, and the EURYI Award Scheme.

[1] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, e-print arXiv:quant-ph/0702225.
[3] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[4] The case of arbitrary nonindependent and identically distributed sequences of states has been considered, e.g., in Refs. 5 and 6.
[5] G. Bowen and N. Datta, e-print arXiv:quant-ph/0610199.
[6] K. Matsumoto, e-print arXiv:0708.3129.
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998); Phys. Rev. A **60**, 1888 (1999).
[8] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[9] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
[10] D. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A **61**, 062313 (2000).
[11] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
[12] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf, Phys. Rev. Lett. **87**, 257902 (2001).
[13] K. G. H. Vollbrecht and M. M. Wolf, Phys. Rev. Lett. **88**, 247901 (2002).
[14] Ll. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
[15] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).
[16] B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. A **65**, 042327 (2002).
[17] S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004).
[18] S. Ishizaka and M. B. Plenio, Phys. Rev. A **71**, 052303 (2005).
[19] Ll. Masanes, e-print arXiv:quant-ph/0510188.
[20] F. G. S. L. Brandão, Phys. Rev. A **76**, 030301 (2007).
[21] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens, Phys. Rev. Lett. **84**, 1611 (2000).
[22] G. Bowen and N. Datta, e-print arXiv:quant-ph/0610199.
[23] R. T. Rockafellar, *Convex Analysis* (Princeton University Press, Princeton, 1970).
[24] The set of single-copy undistillable states forms a convex set and membership can easily be tested in a one-sided test with a witness, see, e.g., Ref. 26. Also, ideas of relaxations (Refs. 27–29) to robust semidefinite programs can be applied to study the distillability of Werner states (Ref. 30).
[25] C. Kuratowski, *Topologie* (PWN, Warszawa, 1958), Vol. I.
[26] L. Clarisse, Quantum Inf. Comput. **6**, 539 (2006).
[27] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[28] J. Eisert, P. Hyllus, O. Gühne, and M. Curty, Phys. Rev. A **70**, 062317 (2004).
[29] F. G. S. L. Brandão and R. O. Vianna, Phys. Rev. Lett. **93**, 220503 (2004).
[30] R. O. Vianna and A. C. Doherty, Phys. Rev. A **74**, 052306 (2006).
[31] R. Simon, e-print arXiv:quant-ph/0608250.
[32] Problem 2, Undistillability implies ppt?, on the problem page maintained by R. F. Werner's quantum information group at the Technical University of Braunschweig (http://www.imaph.tu-bs.de/qi/problems/2.html).
[33] C. A. Fuchs, R. Schack, and P. F. Scudo, Phys. Rev. A **69**, 062305 (2004).
[34] M. Christandl, R. König, G. Mitchison, and R. Renner, e-print arXiv:quant-ph/0602130.
[35] R. König and R. Renner, J. Math. Phys. **46**, 122108 (2005).
[36] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[37] O. Hernandez-Lerma and J. B. Lasserre, J. Convex Anal. **4**, 164 (1997).
[38] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[39] R. Renner, e-print arXiv:quant-ph/0703069.