Robustness of entanglement

Guifré Vidal and Rolf Tarrach
Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, 08028 Barcelona, Spain

(Received 27 July 1998)

In the quest to completely describe entanglement in the general case of a finite number of parties sharing a physical system of finite-dimensional Hilbert space an entanglement magnitude is introduced for its pure and mixed states: robustness. It corresponds to the minimal amount of mixing with locally prepared states which washes out all entanglement. It quantifies in a sense the endurance of entanglement against noise and jamming. Its properties are studied comprehensively. Analytical expressions for the robustness are given for pure states of two-party systems, and analytical bounds for mixed states of two-party systems. Specific results are obtained mainly for the qubit-qubit system (qubit denotes quantum bit). As by-products local pseudomixtures are generalized, a lower bound for the relative volume of separable states is deduced, and arguments for considering convexity a necessary condition of any entanglement measure are put forward. [S1050-2947(99)03701-4]

PACS number(s): 03.67.−a

I. INTRODUCTION

Entanglement [1,2] is arguably the most nonclassical feature of quantum mechanics. For it to show up, the physical system has to consist of different local parts, which we will call *local subsystems*, in one-to-one correspondence with different physicists, which we will call *parties*. Each party acts locally on its respective local subsystem. Each local subsystem will, in general, consist of further parts, *local partial subsystems* or *objects*, which may be entangled among themselves, locally. We are only concerned here with nonlocal entanglement, involving more than one local subsystem. The system might also be partitioned into *nonlocal subsystems*, which are shared by several parties (see Appendix A).

Entanglement refers thus to states shared by more than one party. It is behind (or depending on the definitions, equivalent to) nonlocality, nonseparability, and the existence of nonclassical or quantum correlations, as seen by the parties. It plays a central role in quantum communication and quantum computation. A huge effort is being put into quantifying entanglement. This is an extremely difficult undertaking, mainly because of the intricate interplay between classical and quantum correlations. What one would like to have is a minimal set of independent, physically meaningful magnitudes, which completely characterize entanglement.

Consider, e.g., a two-party system consisting of two three-state local subsystems (each one being, say, a spin 1 particle). As far as entanglement is concerned, any pure state of this system is completely determined by two of the three coefficients of its Schmidt decomposition [3]:

$$|\Psi\rangle = a_1|1\rangle\otimes|1\rangle + a_2|2\rangle\otimes|2\rangle + a_3|3\rangle\otimes|3\rangle,$$

$$a_i \geqslant 0, \quad \sum_{i=1}^{3} a_i^2 = 1, \tag{1}$$

say, the two largest ones. Thus two independent magnitudes will suffice to completely characterize its entanglement. Suppose one chooses one of them to be the entropy of entanglement [4],

$$E(\Psi) = -\sum_{i=1}^{3} a_i^2 \log_2 a_i^2 . \tag{2}$$

Consider now two pure states with different Schmidt coefficients, $|\Psi_1\rangle \neq |\Psi_2\rangle$, which have the same entropy of entanglement, $E(\Psi_1)=E(\Psi_2)$. As we will see, there are physically meaningful entanglement magnitudes which quantify differently these two states. Any such magnitude, together with the entropy of entanglement we chose to start with, determines the two largest Schmidt coefficients and thus characterizes entanglement for pure states completely (provided they are bijective).

As the local subsystems become more complex, involving more states and more partial subsystems, as the number of local subsystems and thus parties grows, so does the number of entanglement magnitudes needed to completely characterize entanglement [5].

The measures of entanglement proposed up to now are examples of entanglement magnitudes. Foremost is the entanglement of formation or creation [6]. Others are the entanglement of distillation [6] and the relative entropy of entanglement [7], but several more have been proposed recently (e.g., entanglement of assistance [8]). It has been argued that for pure states there is a unique measure of entanglement [9], but certainly one sole magnitude will, in general, not be enough for characterizing entanglement completely.

The aim of this contribution is to propose an entanglement magnitude which we will call *robustness* and to study it in some detail. It has several appealing features. Its definition is simple and valid for any state of a composite system composed by any finite number of local subsystems of finite dimension. It is based on a simple physical operation: mixing with locally prepared states. It does not increase on average when the parties, classically communicated, act locally on the subsystems. The *robustness* quantifies the endurance of entanglement with respect to local mixing by asking about the minimal amount of entanglement-free mixing needed to wipe out all entanglement. It can be interpreted as a quantification of intelligent jamming of entanglement, intelligent meaning that the parties know the entangled state and thus tailor the jamming accordingly, so that a minimal amount suffices. An auxiliary and useful magnitude will be the *random robustness*, which can be interpreted as the robustness of entanglement with respect to mixing with white noise. While we explain and analyze robustness a few more general results will be presented: convexity of entanglement measures is put on firmer grounds, a set of necessary and sufficient conditions for consistency with the fundamental law of quantum information processing [10] is presented, and a weak version for the composition law of entanglement magnitudes for a state describing a system which consists of two uncorrelated nonlocal entangled subsystems is suggested.

The paper is organized as follows. In Sec. II, after analyzing some features of mixing, we introduce, following [11], *local pseudomixtures* and prove their existence for the most general, finite-dimensional, case, thus generalizing local descriptions of entanglement. A universal local pseudomixture is given for any state of this general case. *Relative robustness* and *random robustness* are also introduced and their physical meaning discussed. In Sec. III we introduce *robustness*, and prove eight general properties that make it a potentially useful entanglement magnitude. In Sec. IV a number of results for the robustness of two-party systems are presented, whose proofs can be found in Appendixes B and C. They include explicit expressions for the robustness and the random robustness of any pure state, and bounds for mixed states. For the two simplest two-party systems more accurate results are presented and a numerical method for the computation of the robustness is discussed. We present an application of some of the results of the preceding section in Sec. V by obtaining a universal lower bound for the relative volume of separable states, thus completing Ref. [12].

One of the main questions concerning entanglement measures is, what are the necessary and what are the sufficient conditions they have to fulfill? Much progress has been achieved in the last few years (see, e.g., [7–9]) although many questions still remain, in particular concerning additivity. We hope this and further studies of robustness will also contribute to the understanding of these issues.

II. LOCAL PSEUDOMIXTURES

A. Mixing of shared states and local operations

Since the mixing of states that are shared by several parties will play a major role throughout this contribution, we find it convenient to begin with a few comments on how one can obtain a density matrix from one of its *realizations*, without resorting to nonlocal operations. This will, as a by-product, lead to a new condition any measure of entanglement has to satisfy.

We will call a set of states $\{\rho_k\}_{k=1,\ldots,l}$ with associated probabilities $\{p_k\}_{k=1,\ldots,l}$ a realization[1] $\Upsilon\equiv\{\rho_k,p_k\}_{k=1,\ldots,l}$ of the density matrix $\rho\equiv\Sigma_{k=1}^{l}p_k\rho_k$. Consider a device Σ that is known to supply a system $\mathcal{Q}$ in the state ρ_k with probability p_k, for $k=1,\ldots,l$. The state of the system $\mathcal{Q}$ the parties obtain from such a device depends on the amount of extra information Σ supplies together with the prepared system $\mathcal{Q}$. Thus, if (a) no extra information is supplied, then the state of $\mathcal{Q}$ is ρ, whereas this is not the case if (b) Σ casts a message stating which specific state $\rho_k\mathcal{Q}$ has been prepared in, such an event having an *a priori* probability p_k. These two situations lead to states of $\mathcal{Q}$ that are clearly inequivalent even in a statistical sense, and this fact is exemplified if one adopts a utilitarian approach: consider any function $\mu(\rho)$ defined on the set of states that quantifies somehow some resources contained in ρ. [Alternatively $\mu(\rho)$ could quantify the cost of preparing the state ρ, and so on.] Then, in situation (a) the parties obtain a state ρ, from which they can extract, maybe after some manipulations, an amount $\mu(\rho)$ of resources, whereas in situation (b) the expected amount of resources the parties can extract is an average, over the realization Υ, of the amounts $\mu(\rho_k)$, i.e., $\mu(\Upsilon)\equiv\Sigma_{k=1}^{l}p_k\mu(\rho_k)$, the extra information supplied together with $\mathcal{Q}$ allowing for a conditional treatment of this system depending on the concrete ρ_k the parties get. Moreover, whatever is done to $\mathcal{Q}$ in situation (a) in order to use it as a resource, the very same manipulations can be done in (b) regardless of the extra information supplied, obtaining, in a statistical sense, the same results as in (a), so that one gets, *on average*, at least as many resources in case (b) as in case (a). Therefore

$$\mu(\rho)\leqslant\mu(\Upsilon). \tag{3}$$

(Were $\mu(\rho)$ a quantification of the minimal cost of preparation of ρ, one could reach the same conclusion by noticing that Υ is not the only realization which leads to ρ, and that there may be cheaper ones, that is, $\mu(\Upsilon)\geqslant\min_{\Upsilon'}\mu(\Upsilon')$ [$\equiv\mu(\rho)$], where Υ' is any realization of ρ.)

Notice, moreover, that since the only difference between situation (a) and (b) consists of the extra information supplied in (b), if this extra information is irreversibly lost by the parties, the largest amount of resources that they can obtain from $\mathcal{Q}$ becomes $\mu(\rho)$, even if initially the expected amount has been $\mu(\Upsilon)$.

Let us translate the above considerations to the case where μ is any measure of entanglement, which we will do with a concrete example. Suppose Σ prepares two particles in the global state ρ_k with probability p_k and then sends one to Alice and the other to Bob (and thus $\mathcal{Q}$ is a two-party system). What we want to remark here is that the loss of the extra information supplied in case (b), which forces a transition of the state of $\mathcal{Q}$ from a ρ_k to ρ, can occur without Alice and Bob having to put the two particles back together, so that to all effects it can be regarded as a local process. Then, in particular, we have argued that any measure $\mathcal{E}$ of the entanglement of a shared state ρ has to be a convex function (see also [7]), that is,

$$\mathcal{E}(\rho)\leqslant\sum_{k=1}^{l}p_k\mathcal{E}(\rho_k) \tag{4}$$

if $\rho=\Sigma_{k=1}^{l}p_k\rho_k$, otherwise one would be creating, on average, entanglement by means of local operations (as losing

[1] We will not call it an ensemble because we construe the state ρ from it by dismissing information, not by choosing randomly one item out of an ensemble of states ρ_k populated proportionally to p_k.

information is something one can always do locally). Notice that the entanglement of assistance [8] is concave, not convex (it also is generally nonvanishing for separable states). We interpret it as a measure of the entanglement of ρ when supplemented with further information (assisted), and thus more as a measure for maximally entangled ensembles of pure states realizing a density matrix, rather than as a proper measure for a single system described by the density matrix alone.

Once a possible way of (locally) obtaining a state from any of its information-supplied realizations has been discussed, we would like to address a question motivated by the fact that a mixture of shared states, even if they all are entangled, may contain no entanglement at all, so that the procedure of mixing often implies the disappearance of quantum correlations: specifically, given an arbitrary entangled state of a composite system shared by N parties, we would like to know whether it is always possible to wash out all its quantum correlations by mixing it with an adequate separable state. This will be our starting point to derive an entanglement magnitude: the *robustness* of entangled states.

B. Erasing quantum correlations by mixing with a separable state: A local description of entangled states

Consider a composite system $\mathcal{Q}$ with N local subsystems such that the dimension n of its Hilbert space $\mathcal{H}$ is finite. Let us recall that, according to whether they can be expressed as a convex combination of pure product states or not, one can distinguish between separable and entangled states. Thus for $\{\mathcal{H}^i\}_{i=1,\ldots,N}$ the Hilbert spaces of the local subsystems $(\mathcal{H}=\otimes_{i=1}^{N}\mathcal{H}^i)$, separable states ρ_s can be written as

$$\rho_s = \sum_k p_k |\Psi_k\rangle\langle\Psi_k|, \tag{5}$$

where $p_k > 0$, $\Sigma_k p_k = 1$ and $|\Psi_k\rangle = \otimes_{i=1}^{N}|\Psi_k^i\rangle \in \mathcal{H}$, $|\Psi_k^i\rangle \in \mathcal{H}^i$. We will now introduce the concept of robustness of a state $\rho \in \mathcal{T}(\mathcal{H})$ relative to a separable state $\rho_s \in \mathcal{S}(\mathcal{H})$ [by $\mathcal{T}(\mathcal{H})$ we denote the set of states of $\mathcal{Q}$, and by $\mathcal{S}(\mathcal{H}) \subset \mathcal{T}(\mathcal{H})$ that of separable states of the same system].

Definition: Given a state $\rho \in \mathcal{T}(\mathcal{H})$ and a separable state $\rho_s \in \mathcal{S}(\mathcal{H})$, we call *robustness* of ρ *relative* to ρ_s, $R(\rho||\rho_s)$, the minimal $s \geqslant 0$ for which

$$\rho(s) \equiv \frac{1}{1+s}(\rho + s\rho_s) \tag{6}$$

is separable. It might be infinite.

We will single out a particular case of the relative robustness and name it accordingly.

Definition: We call *random robustness* of ρ its robustness relative to the (separable) maximally random state $(1/n)I$.

Thus $R(\rho||\rho_s)$ is the minimal amount of ρ_s that has to be mixed with ρ in order to wipe out all the entanglement initially contained in ρ. Notice that $R(\rho||\rho_s)$ is zero if, and only if, ρ is separable itself. Our previous question, which Theorem 1 will answer, reduces now to see whether one can always find a separable ρ_s such that ρ has finite relative robustness $R(\rho||\rho_s)$. Equivalently, in terms of the local pseudomixtures introduced in [11], we would like to know whether one can always express any state $\rho \in \mathcal{T}(\mathcal{H})$ as

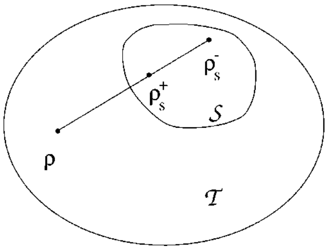

FIG. 1. Local pseudomixture for the entangled state ρ. Since there always exists a $\rho_s^- \in \mathcal{S}$ and a finite $t > 0$ such that $\rho_s^+ \equiv [1/(1+t)](\rho + t\rho_s^-)$ belongs to $\mathcal{S}$, one can express ρ in terms of two separable states and the weight t as $\rho = (1+t)\rho_s^+ - t\rho_s^-$.

$$\rho = (1+t)\rho_s^+ - t\rho_s^-, \quad 0 \leqslant t < \infty \tag{7}$$

for some $\rho_s^+, \rho_s^- \in \mathcal{S}(\mathcal{H})$, that is, whether one can always describe a state as a local pseudomixture (see [13] for a recent proof for $N=2$). Notice that expressing ρ_s^+ and ρ_s^- in Eq. (7) as *finite* statistical mixtures of pure product states $|\Psi_k\rangle = \otimes_{i=1}^{N}|\Psi\rangle$, $|\Psi_k^i\rangle \in \mathcal{H}^i$ [14], one gets

$$\rho = \sum_{k=1}^{l<\infty} r_k |\Psi_k\rangle\langle\Psi_k|, \tag{8}$$

where $\Sigma_{k=1}^{l<\infty} r_k = 1$ and $r_k \in \mathcal{R}$. That is, a state ρ of $\mathcal{Q}$ is expressed as a sum of pure product states, in a similar way to how separable states are as statistical mixtures, but with the difference that now the probabilistic weights p_k in Eq. (5) have been replaced by real numbers r_k, still restricted by $\Sigma_{k=1}^{l<\infty} r_k = 1$. It is this resemblance with mixtures that motivates calling the right hand sides of Eqs. (7) and (8) *local pseudomixtures*, the adjective *local* reflecting the fact that all states intervening in such expressions are separable.

Theorem 1. Any entangled state ρ of a generic composite system (with finite-dimensional Hilbert space) can be expressed in terms of two separable states and a non-negative finite real number, $\{\rho_s^+, \rho_s^-, t\}$, as $\rho = (1+t)\rho_s^+ - t\rho_s^-$ (see Fig. 1).

Proof: In Appendix C an explicit upper bound for the random robustness of any state ρ,

$$R\left(\rho \middle\| \frac{1}{n}I\right) \leqslant \left(1 + \frac{n}{2}\right)^{N-1} - 1 \equiv \tilde{t}, \tag{9}$$

will be obtained. Then one can write

$$\rho = (1+\tilde{t})\rho_s^+ - \tilde{t}\frac{1}{n}I, \quad \rho_s^+ \equiv \frac{1}{1+\tilde{t}}\left(\rho + \tilde{t}\frac{1}{n}I\right), \tag{10}$$

where ρ_s^- in Eq. (7) is $(1/n)I$ and ρ_s^+ is separable by construction. □

Notice that this means, in particular, that $(1/n)I \in \mathcal{S}$ is not on the frontier of $\mathcal{S}$ and $\mathcal{T} \setminus \mathcal{S}$, but in the interior of $\mathcal{S}$, as was proved in [12]. Our proof, which is independent of that presented in [12], provides offhand an explicit pseudomixture for any state ρ and implies, from a physical point of view, that one can always erase all quantum correlations by mixing

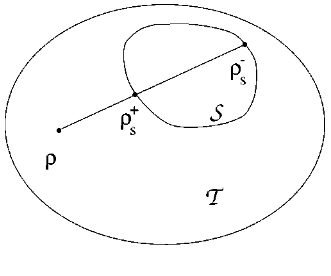

FIG. 2. An optimal local pseudomixture for the state ρ is such that the weight $t=R(\rho||\rho_s^-)$ is minimal. Thus the robustness $R(\rho||\mathcal{S})$ is a geometrical quantity that relates the element $\rho\in\mathcal{T}$ with the subset $\mathcal{S}\subset\mathcal{T}$, as $p=1/[1+R(\rho||\mathcal{S})]$ is the maximal weight of ρ in a convex combination $p\rho+(1-p)\rho_s^-$ involving an element $\rho_s^-\in\mathcal{S}$ such that it belongs to the subset $\mathcal{S}$.

with the maximally random state. Let us remark that mixing with $(1/n)I$ can be regarded as a model for the study of the effect of white noise on the quantum correlations contained in an entangled state. We will come back to the study of the random robustness in Sec. IV B, where it will be computed for any pure state of a two-party (i.e., $N=2$) system and for any state of two-party systems of dimension $n\leqslant 6$, whereas for any mixed state of a generic two-party system lower and upper bounds will be presented. Finally, the random robustness will be used in Sec. V to obtain an explicit lower bound for the volume of separable states.

III. ROBUSTNESS OF SHARED STATES

A. Definition of robustness

We have established so far that for any state ρ there is at least one separable state ρ_s such that $R(\rho||\rho_s)$ is finite. In addition we have seen that this ρ_s can be chosen to be independent of ρ. We now prove the existence of a minimal value of $R(\rho||\rho_s)$ as a function of $\rho_s\in\mathcal{S}$. This quantity, $R(\rho||\mathcal{S})$, will prove to be, on average, nonincreasing under any transformation of the shared system involving only local operations on the subsystems and classical communication between the parties. Analogously to $R(\rho||\rho_s)$, $R(\rho||\mathcal{S})$ is the minimal amount of any separable state that has to be mixed with ρ in order to wash out its quantum correlations, and has a neat geometrical meaning (see Fig. 2). Notice that no metric in $\mathcal{T}$ has been used to define $R(\rho||\mathcal{S})$.

Let us consider, then, a state ρ of $\mathcal{Q}$ and all its possible pseudomixtures $\{\rho_s^+,\rho_s^-,t\}$ of separable states.

Lemma 1. There always exists a non-negative $t(\rho;\rho_s^+,\rho_s^-)$ satisfying Eq. (7) which is the minimal one.

Proof: It follows from the fact that (ρ_s^+,ρ_s^-) must belong to a compact subset of $\mathcal{S}\times\mathcal{S}$ [since they are constrained by Eq. (7)] and that $t(\rho;\rho_s^+,\rho_s^-)\geqslant 0$ is a continuous function of them. □

Definition: We call (*absolute*) *robustness* of $\rho\in\mathcal{T}$ the quantity

$$R(\rho||\mathcal{S})\equiv\min_{\rho_s\in\mathcal{S}}R(\rho||\rho_s). \tag{11}$$

Definition: We call a local pseudomixture with $t(\rho;\rho_s^+,\rho_s^-)=R(\rho||\mathcal{S})$ an *optimal* one.

B. Some properties of robustness

Next we will discuss eight properties the robustness of a state satisfies. Some of them are necessary if one wants to guarantee that an entanglement magnitude cannot be increased locally (that is, by means of the combined use of local transformations and classical communication) (cf. [7,9]). Another assures that the magnitude allows one to distinguish between separable and entangled states. The last property is a weak version of a composition law, which replaces additivity.

Recall that the robustness has been defined for states of a generic composite system, so that it can be applied to states shared by an unrestricted (but finite) number of parties N. We associate parties with local subsystems, so that a local subsystem consists of all the physical objects (particles, for instance) a party holds and can act on. We also require each of these local sets of objects to have a Hilbert space $\mathcal{H}^i$ of finite dimension n_i, so that ρ will be an $n\times n$ matrix acting on $\mathcal{H}=\otimes_{i=1}^{N}\mathcal{C}^{n_i}$, with $n=\dim(\mathcal{H})=\Pi_{i=1}^{N}n_i$. In analogy with pure product states, product operators will be those that can be expressed as $O=\otimes_{i=1}^{N}O^i$, with O^i an operator in $\mathcal{H}^i$, and a product subspace of $\mathcal{H}$ will be a space $\tilde{\mathcal{H}}\subseteq\mathcal{H}$ such that $\tilde{\mathcal{H}}=\otimes_{i=1}^{N}\tilde{\mathcal{H}}^i$ with $\tilde{\mathcal{H}}^i$ a subspace of $\mathcal{H}^i$. The robustness of a state, from now on simply $R(\rho)$, satisfies the following conditions.

(i) If range$(\rho)\subseteq\tilde{\mathcal{H}}\subset\mathcal{H}$, then $R(\rho)$ is independent of the Hilbert space, $\tilde{\mathcal{H}}$ or $\mathcal{H}$, ρ acts on.[2]

(ii) $R(\rho)\geqslant 0$; $R(\rho)=0\Leftrightarrow\rho\in\mathcal{S}$.

(iii) $R(\rho)=R(U_L\rho U_L^\dagger)$ for any unitary product operator $U_L=\otimes_{i=1}^{N}U^i$.

(iv) $R(\mathrm{Tr}_{\tilde{\mathcal{Q}}}[\rho])\leqslant R(\rho)$, where $\mathrm{Tr}_{\tilde{\mathcal{Q}}}[.]$ is a partial trace over $\tilde{\mathcal{Q}}$, $\tilde{\mathcal{Q}}$ denoting any subset, local or not, of the whole set of objects held by the parties.

(v) $R(\rho\otimes\rho_s)=R(\rho)$, where ρ_s is any separable state.

(vi) $R(\rho)\leqslant\Sigma_k p_k R(\rho_k)$, where $\{\rho_k,p_k\}$ is any realization of ρ, i.e., $\rho=\Sigma_k p_k\rho_k$.

(vii) $R(\rho)\geqslant\Sigma_k p_k R(\rho_k)$ if as a result of a local, not necessarily complete, von Neumann measurement ρ becomes the state ρ_k with probability p_k.

(viii) $m(R(\rho_x),R(\rho_y))\leqslant R(\rho_x\otimes\rho_y)\leqslant M(R(\rho_x),R(\rho_y))$, where m and M are two known functions of $R(\rho_x)$ and $R(\rho_y)$.

The meaning of property (i) is that the robustness of a state is not an intensive quantity in the dimension n of the Hilbert space of the shared system $\mathcal{Q}$, since it is independent of n. The following example should clarify the meaning of (i): the two-party pure entangled state $|\Psi\rangle=(1/\sqrt{2})(|1\rangle\otimes|1\rangle+|2\rangle\otimes|2\rangle)$, where $|1\rangle$ and $|2\rangle$ are two normalized orthogonal vectors, has a density matrix $|\Psi\rangle\langle\Psi|$ that can act, for instance, on $\mathcal{C}^2\otimes\mathcal{C}^2$ [a two-qubit (quantum bit) system] or on $\mathcal{C}^3\otimes\mathcal{C}^3$ [a two-qutrit (quantum trit) system]. What property (i) assures is that $R(\Psi)$ does not depend on whether $|\Psi\rangle$ is the state of two qubits or of two qutrits, and it is not obviously satisfied [later on, for instance, it will be seen that

[2] The support or range of a density matrix is the subspace spanned by its eigenvectors of nonvanishing eigenvalue. The dimension of the range is the rank.

the random robustness of $|\Psi\rangle$, $R(\Psi\|(1/n)I)$, does depend on n].

A generic ρ in $\mathcal{H}=\otimes_{i=1}^{N}\mathcal{H}^{i}$ may have support only on a product subspace of $\mathcal{H}$. Let us call $\tilde{\mathcal{H}}\subseteq\mathcal{H}$ the smallest of such product subspaces ($\tilde{\mathcal{H}}=\otimes_{i=1}^{N}\tilde{\mathcal{H}}^{i}$ can be constructed by computing, for each party i, its local state $\rho^{i}=\mathrm{Tr}_{\mathcal{Q}\setminus\mathcal{Q}^{i}}[\rho]$, and by taking $\tilde{\mathcal{H}}^{i}\subseteq\mathcal{H}^{i}$ to be the subspace spanned by the eigenvectors of ρ^{i} with nonvanishing eigenvalue). Taking up the previous example involving $|\Psi\rangle\in\mathcal{C}^{3}\otimes\mathcal{C}^{3}$, one can see that the projection of $|\Psi\rangle\langle\Psi|$ onto the product subspace $\tilde{\mathcal{H}}=\langle|1\rangle,|2\rangle\rangle\otimes\langle|1\rangle,|2\rangle\rangle\cong\mathcal{C}^{2}\otimes\mathcal{C}^{2}$ by means of the product projector $P=(|1\rangle\langle1|+|2\rangle\langle2|)\otimes(|1\rangle\langle1|+|2\rangle\langle2|)$ leaves the state unchanged, that is, $P|\Psi\rangle\langle\Psi|P=|\Psi\rangle\langle\Psi|$, and no other product projector of equal or smaller rank does so.

If we now show that any optimal local pseudomixture of ρ, $\{\rho_s^{+},\rho_s^{-},t=R(\rho)\}$, satisfies that both ρ_s^{+} and ρ_s^{-} have support only on $\tilde{\mathcal{H}}$, then it will be irrelevant, in terms of $R(\rho)$, whether ρ acts on the whole $\mathcal{H}$ or only on $\tilde{\mathcal{H}}$.

Theorem 2. For any optimal pseudomixture of ρ, $\{\rho_s^{+},\rho_s^{-},R(\rho)\}$, if $\tilde{\mathcal{H}}$ is the smallest product subspace supporting ρ and P is a projector onto it, then $P\rho_s^{+}P=\rho_s^{+}$ and $P\rho_s^{-}P=\rho_s^{-}$.

Proof: Notice first that for a normalized pure product state $|\Psi\rangle=\otimes_{i=1}^{N}|\Psi^{i}\rangle$, its projection onto a product subspace is, if not zero, another pure product state $|\Phi\rangle=P|\Psi\rangle=\otimes_{i=1}^{N}P^{i}|\Psi^{i}\rangle=\otimes_{i=1}^{N}|\Phi^{i}\rangle$, with $\langle\Phi|\Phi\rangle\leqslant1$. Then, since any separable state ρ_s can be expressed as a convex combination of projectors onto pure product states $|\Psi_k\rangle$, i.e., $\rho_s=\Sigma_k p_k|\Psi_k\rangle\langle\Psi_k|$, and $P|\Psi_k\rangle\langle\Psi_k|P=|\Phi_k\rangle\langle\Phi_k|=q_k|\tilde{\Phi}_k\rangle\langle\tilde{\Phi}_k|$, where $0<q_k\equiv\langle\Phi_k|\Phi_k\rangle\leqslant1$ and $|\tilde{\Phi}_k\rangle\equiv(1/\sqrt{q_k})|\Phi_k\rangle$ is a normalized pure product state (unless $P|\Psi_k\rangle=0$), the renormalized restriction of ρ_s on $\tilde{\mathcal{H}}$, $\tilde{\rho}_s\equiv P\rho_sP/\mathrm{Tr}[P\rho_sP]$ ($\mathrm{Tr}[P\rho_sP]=\Sigma_k p_k q_k\leqslant1$) is a separable density matrix as well. Then

$$\rho=P\rho P=[1+R(\rho)]\mathrm{Tr}[P\rho_s^{+}P]\tilde{\rho}_s^{+}-R(\rho)\mathrm{Tr}[P\rho_s^{-}P]\tilde{\rho}_s^{-}. \tag{12}$$

Now suppose that at least one of ρ_s^{+} and ρ_s^{-} (and thus, in fact, both), say ρ_s^{-}, has support not contained in $\tilde{\mathcal{H}}$. Then $\mathrm{Tr}[P\rho_s^{-}P]<1$ and we automatically obtain a new local pseudomixture involving $\tilde{\rho}_s^{-}\neq\rho_s^{-}$, with $t=\mathrm{Tr}[P\rho_s^{-}P]R(\rho)<R(\rho)$, which is a contradiction, for we started from an optimal one. □

Property (ii) says that the robustness of a state ρ indicates whether ρ is entangled or separable. To see (ii), notice that $R(\rho)=0$ implies that $\rho=\rho_s^{+}$, which is separable, and that if ρ is separable, then by choosing ρ_s^{+} to be ρ one gets a local pseudomixture for ρ, with $t=0$.

Property (iii) states that any two states related by a unitary product transformation have the same robustness.

Theorem 3. $R(\rho)=R(U_L\rho U_L^{\dagger})$.

Proof: Notice that $R(U_L\rho U_L^{\dagger})$ cannot be greater than $R(\rho)$, since by transforming an optimal local pseudomixture,

$$\rho=[1+R(\rho)]\rho_s^{+}-R(\rho)\rho_s^{-}, \tag{13}$$

by U_L we find the local pseudomixture

$$U_L\rho U_L^{\dagger}=[1+R(\rho)]U_L\rho_s^{+}U_L^{\dagger}-R(\rho)U_L\rho_s^{-}U_L^{\dagger}, \tag{14}$$

which has $t=R(\rho)$. *Mutatis mutandis* we see that $R(U_L\rho U_L^{\dagger})$ cannot be smaller than $R(\rho)$. □

In order to discuss properties (iv) and (v), recall that if to $\mathcal{Q}$, in the state ρ, we add a set of objects $\tilde{\mathcal{Q}}$ in the state $\tilde{\rho}$, then the state of $\mathcal{Q}\cup\tilde{\mathcal{Q}}$ is $\rho\otimes\tilde{\rho}$ (assuming $\mathcal{Q}$ and $\tilde{\mathcal{Q}}$ are uncorrelated). On the other hand, for $\tilde{\mathcal{Q}}\subset\mathcal{Q}$ a subset of objects, if ρ is the state of $\mathcal{Q}$ then that of $\tilde{\mathcal{Q}}$ is $\mathrm{Tr}_{\mathcal{Q}\setminus\tilde{\mathcal{Q}}}[\rho]$, whereas if we throw $\tilde{\mathcal{Q}}$ away the remaining state is $\mathrm{Tr}_{\tilde{\mathcal{Q}}}[\rho]$.

Point (iv) states that the robustness of the state ρ of a composite system $\mathcal{Q}$ does not increase when throwing away any subset of objects $\tilde{\mathcal{Q}}\subset\mathcal{Q}$.

Theorem 4. $R(\mathrm{Tr}_{\tilde{\mathcal{Q}}}[\rho])\leqslant R(\rho)$.

Proof: It will suffice to analyze the case of $\tilde{\mathcal{Q}}$ being a single object held by one party, since for a general $\tilde{\mathcal{Q}}=\cup_{i,j}\mathcal{Q}^{i,j}$ one can proceed stepwise, each step involving only one object. Take then $\tilde{\mathcal{Q}}=\mathcal{Q}^{1,1}$ (relabeling the parties and objects, if necessary), so that the partial trace is taken over the factor space $\mathcal{H}^{1,1}$ of $\mathcal{H}^{1}$. A rank one product projector $|\Psi\rangle\langle\Psi|$ ($|\Psi\rangle=\otimes_{i=1}^{N}|\Psi^{i}\rangle$, $|\Psi^{i}\rangle\in\mathcal{H}^{i}$) will be transformed into $\mathrm{Tr}_{\mathcal{Q}^{1,1}}[|\Psi\rangle\langle\Psi|]=\mathrm{Tr}_{\mathcal{Q}^{1,1}}[|\Psi^{1}\rangle\langle\Psi^{1}|]\otimes\otimes_{i=2}^{N}|\Psi^{i}\rangle\langle\Psi^{i}|$, which is a product (in general not pure) state of $\mathcal{Q}\setminus\mathcal{Q}^{1,1}$. Therefore $\mathrm{Tr}_{\mathcal{Q}^{1,1}}[\rho_s]$ is a separable state if ρ_s is so, and the expression

$$\rho'\equiv\mathrm{Tr}_{\mathcal{Q}^{1,1}}[\rho]=[1+R(\rho)]\mathrm{Tr}_{\mathcal{Q}^{1,1}}[\rho_s^{+}]-R(\rho)\mathrm{Tr}_{\mathcal{Q}^{1,1}}[\rho_s^{-}] \tag{15}$$

is a local pseudomixture, not necessarily optimal, for the state ρ' of $\mathcal{Q}\setminus\mathcal{Q}^{1,1}$ with $t=R(\rho)$. Consequently, $R(\mathrm{Tr}_{\mathcal{Q}^{1,1}}[\rho])\leqslant R(\rho)$. □

Property (v) assures that the robustness of the state of a shared system is not an intensive quantity in the number of objects $\mathcal{Q}$ consists of. Indeed, this follows from the fact that $R(\rho)$ is left unchanged if we give the parties new objects $\tilde{\mathcal{Q}}$, provided they are in a separable state ρ_s and uncorrelated with the objects of $\mathcal{Q}$. Notice that we need only prove that $R(\rho\otimes\rho_s)\leqslant R(\rho)$, since Theorem 4 will do the rest.

Theorem 5. $R(\rho\otimes\rho_s)\leqslant R(\rho)$.

Proof: For $\rho=[1+R(\rho)]\rho_s^{+}-R(\rho)\rho_s^{-}$ an optimal local pseudomixture of the state of $\mathcal{Q}$, the state of $\mathcal{Q}\cup\tilde{\mathcal{Q}}$, $\rho\otimes\rho_s$, admits the following decomposition:

$$\rho\otimes\rho_s=[1+R(\rho)]\rho_s^{+}\otimes\rho_s-R(\rho)\rho_s^{-}\otimes\rho_s, \tag{16}$$

which is a local pseudomixture, not necessarily optimal. □

Definition: Given a realization $\Upsilon\equiv\{\rho_k,p_k\}_{k=1,\ldots,l}$, we call the quantity $\Sigma_{k=1}^{l}p_kR(\rho_k)$ the (*average*) *robustness* of Υ, $R(\Upsilon)$.

Property (vi) refers to the convexity of $R(\rho)$, and it means that the robustness of any realization of ρ, $\Upsilon\equiv\{\rho_k,p_k\}_{k=1,\ldots,l}$, is not smaller than that of ρ itself. It suffices to prove (vi) for $l=2$, since $l>2$ can be achieved by iterating this case.

Theorem 6. $R[p\rho_1+(1-p)\rho_2]\leqslant pR(\rho_1)+(1-p)R(\rho_2)$, $p\in[0,1]$.

Proof: For each ρ_k ($k=1,2$) consider an optimal local pseudomixture, say

$$\rho_k=[1+R(\rho_k)]\rho_{s,k}^{+}-R(\rho_k)\rho_{s,k}^{-}. \tag{17}$$

Then $\rho=p\rho_1+(1-p)\rho_2$ can be reexpressed as

$$\rho=(1+t)\rho_s^{+}-t\rho_s^{-}, \tag{18}$$

which is a local pseudomixture, not necessarily optimal, with

$$\rho_s^{+}\equiv\frac{1}{1+t}\{p[1+R(\rho_1)]\rho_{s,1}^{+}+(1-p)[1+R(\rho_2)]\rho_{s,2}^{+}\}\in\mathcal{S}, \tag{19}$$

$$\rho_s^{-}\equiv\frac{1}{t}[pR(\rho_1)\rho_{s,1}^{-}+(1-p)R(\rho_2)\rho_{s,2}^{-}]\in\mathcal{S}, \tag{20}$$

$$t\equiv pR(\rho_1)+(1-p)R(\rho_2). \tag{21}$$

Then $R[\rho=p\rho_1+(1-p)\rho_2]\leqslant t$ by the definition of $R(\rho)$. □

Let us explain property (vi) a bit further. Recall the device Σ introduced in Sec. II A. If Alice and Bob are each given a particle which together are, with equal probability, either in state $\rho_1=|\Psi_1\rangle\langle\Psi_1|$ or $\rho_2=|\Psi_2\rangle\langle\Psi_2|$, with $|\Psi_1\rangle=|1\rangle\otimes|1\rangle$ and $|\Psi_2\rangle=(1/\sqrt{2})(|1\rangle\otimes|1\rangle+|2\rangle\otimes|2\rangle)$, then if they get them in the separable state $\rho_1=|\Psi_1\rangle\langle\Psi_1|$ together with a message stating this fact, their shared state has null robustness. However, if they destroy the message and forget its content, the new state of the system is $\rho=\frac{1}{2}(\rho_1+\rho_2)$, which can be checked to be entangled and consequently contains some robustness. This means Alice and Bob have increased the robustness of their system by acting locally. Notice, however, that if the process is repeated many times (each repetition consisting of first getting a couple of particles along with a message stating their global state, and then destroying the message and forgetting its content), on average the robustness of the freshly obtained couples is $\frac{1}{2}R(\rho_1)+\frac{1}{2}R(\rho_2)$, whereas the robustness of the state the couples finally end up in is $R(\rho)\leqslant\frac{1}{2}[R(\rho_1)+R(\rho_2)]$. Therefore (vi) states that one cannot, in a statistical sense, increase the robustness of a shared state by mixing.

Let us now discuss property (vii), which assures that the output of a local measurement on ρ is a realization $\Upsilon=\{\rho_k,p_k\}_{k=1,\ldots,l}$ (of the *averaged* final state $\rho_f\equiv\Sigma_k p_k\rho_k$) that cannot have more robustness than ρ, so that the robustness of a system $\mathcal{Q}$ cannot be increased, on average, by performing a local measurement on it.

Although property (vii) refers to a local, not necessarily complete, von Neumann measurement (that is, one implemented by a set of orthogonal product projectors, not necessarily of rank one but which correspond to a resolution of the identity), we will prove it for local measurements of the most general nature. In addition to being complete or incomplete, they may include the temporary use of ancillas [local positive operator valued measurements (POVM's)] and classical communication between the parties, and contemplate conditional rejection of the system depending on the output. A general local measurement is implemented by a set $\{A_k\}_{k=1,\ldots,l}$ of product operators that satisfy $0\leqslant\Sigma_k A_k^{\dagger}A_k\leqslant I$. As a result of such a measurement the state of the system becomes, with probability $p_k=\mathrm{Tr}[A_k\rho A_k^{\dagger}]$, $\rho_k=A_k\rho A_k^{\dagger}/\mathrm{Tr}[A_k\rho A_k^{\dagger}]$. Notice that $\Sigma_k p_k\leqslant 1$. Thus the realization $\Upsilon=\{\rho_k,p_k\}_{k=1,\ldots,l}$ and the averaged final state ρ_f are in general unnormalized.

Theorem 7. If the (unnormalized) realization $\Upsilon=\{\rho_k,p_k\}_{k=1,\ldots,l}$ describes the potential final states of a general local measurement performed on $\mathcal{Q}$ in the state ρ, then $R(\rho)\geqslant R(\Upsilon)$.

Proof: One can check that for $\rho_s\in\mathcal{S}$, any resulting state $\rho_{s,k}$ is separable as well (as is to be expected, otherwise we would get some entanglement out of a separable state, even in a statistical sense). Then, for $\rho=[1+R(\rho)]\rho_s^{+}-R(\rho)\rho_s^{-}$ an optimal local pseudomixture of ρ, we can write

$$\rho_k=\frac{1}{\mathrm{Tr}[A_k\rho A_k^{\dagger}]}\{[1+R(\rho)]A_k\rho_s^{+}A_k^{\dagger}-R(\rho)A_k\rho_s^{-}A_k^{\dagger}\}, \tag{22}$$

which implies that if $\rho_k=[1+R(\rho_k)]\rho_{s,k}^{+}-R(\rho_k)\rho_{s,k}^{-}$ is an optimal local pseudomixture, then $R(\rho_k)\leqslant R(\rho)\mathrm{Tr}[A_k\rho_s^{-}A_k^{\dagger}]/\mathrm{Tr}[A_k\rho A_k^{\dagger}]$. Therefore $R(\Upsilon)=\Sigma_k p_k R(\rho_k)=\Sigma_k\,\mathrm{Tr}[A_k\rho A_k^{\dagger}]R(\rho_k)\leqslant R(\rho)\,\mathrm{Tr}[\Sigma_k A_k^{\dagger}A_k\rho_s^{-}]\leqslant R(\rho)\mathrm{Tr}[I\rho_s^{-}]=R(\rho)$. □

We want to stress here that properties (i) and (iii)–(vii) must be satisfied by any magnitude $\mu(\rho)$ consistent with the fundamental law of quantum information processing [10,9], that is, nonincreasing under local actions of the parties, which are allowed to communicate classically. Properties (iii)–(vii) must be obviously satisfied [for property (vi), see discussion in Sec. II A], whereas property (i) is also necessary, but it can be proved to follow from properties (iii)–(v). Notice that properties (iii)–(vii), which we claim to be a set of *necessary and sufficient properties a magnitude μ has to fulfill in order to be consistent with the fundamental law of quantum information processing,* do not mention the fact that the parties can share information using a classical channel. The reason for this is that the use of classical communication simply allows for a wise selection of a local action conditioned to the result of previous local measurements, each of these local actions not increasing, on average, the magnitude μ. Properties (iii)–(vii) are sufficient because any operation the parties can perform locally on the local subsystems can be decomposed into elementary steps taken into account in (iii)–(vii).

Finally, property (viii) is a very weak version of a composition law.[3] Consider a state of the form $\rho_x\otimes\rho_y$, where, for instance, ρ_x may be the global state of a nonlocal system which consists of four particles shared by Alice, Bob, and Claire, whereas ρ_y may be that of five other particles shared by Alice and Denis. The lack of correlations between ρ_x and ρ_y allows on one hand Alice, Bob, and Claire to mix ρ_x with a separable state $\rho_{s,x}^{-}$ with weight $R(\rho_x)$ and on the other Alice and Denis to mix ρ_y with a separable state $\rho_{s,y}^{-}$ with weight $R(\rho_y)$. These operations transform $\rho_x\otimes\rho_y$ into $\rho_{s,x}^{+}\otimes\rho_{s,y}^{+}$, a separable state different from any separable

[3] Additivity of the robustness, that is, $R(\rho_x\otimes\rho_y)=R(\rho_x)+R(\rho_y)$, would be a particular form of a composition law. We already know, however, that the robustness is not an additive quantity, as will be shown elsewhere, though a function of it could well be additive.

state associated with $R(\rho_x \otimes \rho_y)$. Whether $R(\rho_x \otimes \rho_y)$ is determined or not by $R(\rho_x)$ and $R(\rho_y)$, we will now show that the knowledge of $R(\rho_x)$ and $R(\rho_y)$ leads to bounds on $R(\rho_x \otimes \rho_y)$, which is what property (viii) announces. These bounds are

$$\max(R(\rho_x),R(\rho_y)) \leqslant R(\rho_x \otimes \rho_y) \leqslant R(\rho_x)+R(\rho_y) + 2R(\rho_x)R(\rho_y), \tag{23}$$

and can be obtained as follows: the lower bound results from taking the partial trace over the Hilbert space of either ρ_x or ρ_y in an optimal local pseudomixture for $\rho_x \otimes \rho_y$, and is a consequence of property (iv), whereas to deduce the upper bound one needs to take into consideration the tensor product of two optimal local pseudomixtures for the two shared states ρ_x and ρ_y $[x \equiv R(\rho_x),\ y \equiv R(\rho_y)]$, which is a local pseudomixture for $\rho_x \otimes \rho_y$, not necessarily optimal, with weight $t = x+y+2xy$,

$$\begin{aligned}\rho_x \otimes \rho_y &= [(1+x)\rho_{s,x}^{+} - x\rho_{s,x}^{-}] \otimes [(1+y)\rho_{s,y}^{+} - y\rho_{s,y}^{-}] \\ &= (1+x)(1+y)\rho_{s,x}^{+} \otimes \rho_{s,y}^{+} + xy\rho_{s,x}^{-} \otimes \rho_{s,y}^{-} \\ &\quad - \{x(1+y)\rho_{s,x}^{-} \otimes \rho_{s,y}^{+} + (1+x)y\rho_{s,x}^{+} \otimes \rho_{s,y}^{-}\}.\end{aligned} \tag{24}$$

C. Numerical computations and convexity

We end the exposition of general properties of the robustness $R(\rho)$ by mentioning a property of the relative robustness $R(\rho||\rho_s)$ which is most valuable for the numerical computation of the absolute robustness of a state ρ, $R(\rho)$, namely, that $R(\rho||\rho_s)$ is a convex function of ρ_s.

Indeed, if

$$\rho = (1+R_k)\rho_{s,k}^{+} - R_k \rho_{s,k} \equiv [k] \quad (k=1,2) \tag{25}$$

is the local pseudomixture for ρ that, involving the separable state $\rho_{s,k}$, has minimum non-negative weight $R_k \equiv R(\rho||\rho_{s,k})$ [cf. Eq. (6)], then the convex combination

$$\frac{1}{p/R_1+(1-p)/R_2}\left(\frac{p}{R_1}[1]+\frac{1-p}{R_2}[2]\right) \tag{26}$$

is another local pseudomixture for ρ, involving $\rho_s \equiv p\rho_{s,1} + (1-p)\rho_{s,2}$, with weight $t=[1/p/R_1+(1-p)/R_2]$. Since $[p/R_1+(1-p)/R_2][pR_1+(1-p)R_2] = p^2+(1-p)^2 + (R_1/R_2+R_2/R_1)p(1-p) \geqslant 1$, it follows that

$$R(\rho||\rho_s) \leqslant t \leqslant pR(\rho||\rho_{s,1}) + (1-p)R(\rho||\rho_{s,2}). \tag{27}$$

This means that if $R(\rho)$ is computed by searching in the set of separable states $\mathcal{S}$ for the absolute minimum of $R(\rho||\rho_s)$ as a function of ρ_s, then the search can finish as soon as a local minimum is found, for any local minimum of $R(\rho||\rho_s)$ is also the absolute one. We will use this fact in Sec. IV A to explain a way of numerically computing $R(\rho)$ for states of the two simplest two-party systems.

IV. ROBUSTNESS AND RANDOM ROBUSTNESS OF TWO-PARTY SYSTEMS

So far all our considerations have referred to composite systems with an unrestricted number of parties N. We consider in what follows a composite system $\mathcal{Q}$ shared by two parties, Alice and Bob, so that from now on $N=2$. Recall that, as before, $\mathcal{H}^i \cong \mathcal{C}^{n_i}$ is the Hilbert space of all the physical objects party i can act locally on.

A. Robustness of two-party systems

We present here a list of bounds and exact results concerning the robustness of states of a two-party system. A method for numerically computing this quantity for the two simplest two-party systems is also discussed. These results make the robustness of states of two-party systems useful as an entanglement magnitude. And thus, for instance, from its expression for pure states one can see that robustness, together with the entropy of entanglement, can be used to completely characterize the entanglement of pure states of a two-qutrit system (see the Introduction).

1. Robustness of pure states of two-party systems

It turns out that for two-party systems with Hilbert space $\mathcal{C}^m \otimes \mathcal{C}^m$ a set of $m-1$ ordered non-negative parameters $\{a_i\}_{i=1,\ldots,m-1}$ suffices to completely specify any element of the set of locally inequivalent pure states,[4]

$$\frac{(\mathcal{C}^m \otimes \mathcal{C}^m \backslash \{|0\rangle\})/R^+}{\mathcal{U}(m) \quad \times \quad \mathcal{U}(m)} \tag{28}$$

(that is the space of the orbits, in the subset of normalized elements of the complex vector space $\mathcal{C}^m \otimes \mathcal{C}^m$, of the action of all unitary product transformations). This set $\{a_i\}$ can easily be obtained for any normalized vector $|\Psi\rangle$ from its ordered Schmidt decomposition,

$$|\Psi\rangle = \sum_{i=1}^{m} a_i |i\rangle \otimes |i\rangle, \quad a_i \geqslant a_{i+1} \geqslant 0, \ \sum_{i=1}^{m} a_i^2 = 1, \tag{29}$$

after excluding a_m. It will be more convenient, however, to keep all m coefficients. Then, in terms of $\{a_i\}$, the robustness R of the pure state Ψ is

$$R[\Psi(\{a_i\})] = \left(\sum_{i=1}^{m} a_i\right)^2 - 1. \tag{30}$$

This result is proved in Appendix B, and indicates how $R(\Psi)$ can be systematically computed: given a rank one projector corresponding to a pure state, $\rho = |\Psi\rangle\langle\Psi|$, one needs only to perform a partial trace over any of the two parties, and get the eigenvalues of the remaining matrix. These eigenvalues are a_i^2, so that the sum of their square roots will immediately lead to $R(\Psi)$.

Notice that the sets

[4] In general, any two states ρ_1 and ρ_2 are said to be locally equivalent if they are related by a unitary product transformation, i.e., if $\rho_1 = U_L \rho_2 U_L^{\dagger}$.

$$\frac{\mathcal{C}^m \otimes \mathcal{C}^m}{\mathcal{U}(m) \quad \times \; \mathcal{U}(m)} \quad \text{and} \quad \frac{\mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}}{\mathcal{U}(n_1) \quad \times \; \mathcal{U}(n_2)} \tag{31}$$

for any n_1, n_2 satisfying $m = \min(n_1, n_2)$ are equivalent (since the Schmidt decomposition of $|\Psi\rangle \in \mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}$ contains at most m terms), so that Eq. (30) is also valid for any state in $\mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}$ if $m = \min(n_1, n_2)$.

One can check that, as previously announced, for $m=3$ the entropy of entanglement $E(\Psi)$ given in Eq. (2) and the robustness $R(\Psi)$ are independent functions of the two greatest Schmidt coefficients a_1 and a_2, and that there is a one-to-one correspondence between (a_1, a_2) and (E, R), so that (E, R) can be used to label unambiguously the elements of the set of locally inequivalent pure states of a two-qutrit system, and therefore suffices to completely characterize their entanglement.

2. Bounds for the robustness of mixed states of two-party systems

It can be proved (see Appendix C) that for any state of a two-party system the following inequalities hold:

$$\left|\min\left(\left\{\frac{\lambda_j}{a_{j,1}^2}\right\}, 0\right)\right| \leqslant R(\rho) \leqslant \min\left(\tilde{m}-1, R\left(\tilde{\rho} \,\middle\|\, \frac{1}{\tilde{n}}\tilde{I}\right)\right), \tag{32}$$

where λ_j is the jth negative eigenvalue of ρ^{T_B},[5] $a_{j,1}$ is the biggest coefficient of the Schmidt decomposition of the eigenvector corresponding to λ_j, $\tilde{n}$ is the rank of $\rho^A \otimes \rho^B \equiv \mathrm{Tr}_B[\rho] \otimes \mathrm{Tr}_A[\rho]$ (i.e., the dimension of the minimum product space $\tilde{\mathcal{H}} \subseteq \mathcal{H}$ such that ρ is entirely supported in it), $\tilde{m} = \min(\mathrm{rank}[\rho^A], \; \mathrm{rank}[\rho^B])$, and $\tilde{\rho}$ and $\tilde{I}$ are the restrictions of ρ and I to $\tilde{\mathcal{H}}$.

3. Robustness of a two-qubit system

For the simplest two-party system, the $\mathcal{C}^2 \otimes \mathcal{C}^2$ case, we present simpler bounds for the robustness of a general mixed state and an exact result for a class of mixed states, which includes all Werner states. These results are proved in Appendix C.

First, for λ the negative eigenvalue of ρ^{T_B} and $|n\rangle$ its corresponding eigenvector, with $|n\rangle = \cos\theta|1\rangle \otimes |1\rangle + \sin\theta|2\rangle \otimes |2\rangle$ ($\theta \in [0, \pi/4]$) its ordered Schmidt decomposition, the following inequalities hold for any state ρ:

$$\frac{|\lambda|}{\cos^2\theta} \leqslant R(\rho) \leqslant 2|\lambda|, \tag{33}$$

which in particular means that whenever $\cos^2\theta = \frac{1}{2}$, $R(\rho) = 2|\lambda|$. The lower bound corresponds to Eq. (32), and the upper bound can be seen to be an improvement on that in Eq. (32) by taking into account the result in Eq. (44) and that $|\lambda| \leqslant \frac{1}{2}$ [12], $\tilde{m} = 2$ for any entangled ρ.

Another upper bound for the robustness comes from the fact that for pure states of $\mathcal{C}^2 \otimes \mathcal{C}^2$ the concurrence $C(\Psi)$ (see [15]) equals the robustness, and it reads

$$R(\rho) \leqslant C(\rho), \tag{34}$$

where $C(\rho)$ was explicitly computed for any state of this system in [15].

Finally, we have computed the robustness for a family of mixed states: consider the rank one projector $|\theta\rangle\langle\theta|$, where $|\theta\rangle \equiv \cos\theta|1\rangle \otimes |1\rangle + \sin\theta|2\rangle \otimes |2\rangle$, $\theta \in [0, \pi/4]$, and the (separable) diagonal state

$$\rho_D \equiv \begin{pmatrix} q_1 & 0 & 0 & 0 \\ 0 & \frac{q_2}{2} & 0 & 0 \\ 0 & 0 & \frac{q_2}{2} & 0 \\ 0 & 0 & 0 & q_3 \end{pmatrix}, \quad q_i \geqslant 0, \quad \sum_i^3 q_i = 1, \tag{35}$$

then, for any $0 \leqslant p \leqslant 1$, the state $\rho \equiv p\rho_D + (1-p)|\theta\rangle\langle\theta|$ has robustness

$$R(\rho) = \begin{cases} 0 & \text{if} \quad \rho^{T_B} \geqslant 0 \\ (1-p)\sin 2\theta - pq_2 & \text{otherwise.} \end{cases} \tag{36}$$

A Werner state with fidelity F [16] is locally equivalent to the ρ resulting from taking $q_1 = q_3 = q_2/2 = \frac{1}{4}$, $\theta = \pi/4$, and $p = 4(1-F)/3$, and in terms of its fidelity we have $R(\rho) = 2F - 1$ for entangled Werner states, that is, for Werner states with fidelity $F > \frac{1}{2}$.

4. Numerical computation of the robustness for mixed states of two qubits and of a qubit-qutrit system

In $\mathcal{C}^2 \otimes \mathcal{C}^2$ and $\mathcal{C}^2 \otimes \mathcal{C}^3$ one can easily check whether a state ρ is separable by computing the eigenvalues of ρ^{T_B} and seeing whether they are all non-negative, since for these systems $\rho \in \mathcal{S} \Leftrightarrow \rho^{T_B} \geqslant 0$ [17,18]. Therefore given a ρ which is known to be entangled, one can choose a separable state ρ_s and compute $R(\rho \| \rho_s)$ by requiring that s in Eq. (6) be minimum with $\rho(s)^{T_B} \geqslant 0$. Consequently to find $R(\rho)$ one can perform, say, a conditional random walk, in the 16- (or 36-) dimensional real vector space of Hermitian 4×4 (or 6×6) matrices $s\rho_s$, searching for the minimum of its trace s, requiring

$$\rho_s \geqslant 0, \tag{37}$$

$$\rho_s^{T_B} \geqslant 0, \tag{38}$$

$$(\rho + s\rho_s)^{T_B} \geqslant 0, \tag{39}$$

and that at each step s diminishes. Conditions (37) and (38) assure that ρ_s is a separable state, and then condition (39) assures that $[1/(1+s)](\rho + s\rho_s)$ is also separable. For each $s\rho_s$ satisfying conditions (37)–(39), s is greater than or equal to $R(\rho \| \rho_s)$, and from the convexity of this function (see Sec. III C) we know the search will finish as soon as a local minimum is reached for s, for it is the global one.

[5] ρ^{T_B} is the partial transposed of ρ with respect to the party B (which has the same spectrum as ρ^{T_A}, its eigenvectors also having the same Schmidt coefficients).

In $\mathcal{C}^2\otimes\mathcal{C}^2$ the effectiveness of this method is notably enhanced by the fact that, as a consequence of some results of [11], a state ρ of this system is entangled if, and only if, $\det\rho^{T_B}<0$, that is,

$$\rho\in\mathcal{S}\Leftrightarrow\det\rho^{T_B}\geqslant 0. \tag{40}$$

Then, whereas the eigenvalues of ρ_s must be computed to check constraint (37), for constraints (38) and (39) one only needs to compute the determinant of $\rho_s^{T_B}$ and that of $(\rho+s\rho_s)^{T_B}$.

B. Random robustness of two-party systems

The random robustness of two-party systems, that we shall compute exactly for pure states of a system $\mathcal{C}^{n_1}\otimes\mathcal{C}^{n_2}$ and for any state of the systems $\mathcal{C}^2\otimes\mathcal{C}^2$ and $\mathcal{C}^2\otimes\mathcal{C}^3$, and for which we will present lower and upper bounds for any state in any system, is a quantity that will be very useful for two different purposes. We proved in Sec. II B that any state of any composite system can be expressed in terms of two separable states, ρ_s^+ and ρ_s^-, and a non-negative number *t*, i.e., as a local pseudomixture. Moreover, we provided an explicit offhand example of local pseudomixture for any state ρ. However, we did not prove this last result, and this is what we will do with the help of the random robustness of mixed states. On the other hand, this quantity will allow us to obtain an explicit lower bound for the volume of separable states of a generic composite system in Sec. V.

1. Random robustness of pure states of two-party systems

Given a pure state Ψ of a two-party system $\mathcal{C}^{n_1}\otimes\mathcal{C}^{n_2}$ with ordered nonlocal parameters $\{a_i\}_{i=1,m}$ $[m=\min(n_1,n_2)]$, its random robustness is (Appendix B)

$$R\left(\Psi\left|\left|\frac{1}{n_1n_2}I\right.\right.\right)=n_1n_2a_1a_2, \tag{41}$$

which manifestly depends not only on the two largest coefficients a_1 and a_2 (that is, on the state itself), but also on the dimension $n=n_1n_2$ of the Hilbert space of the system [cf. property (i) of $R(\rho)$]. Notice that for any dimensions the most robust pure state, as far as white noise is concerned, has $a_1=a_2=1/\sqrt{2}$, and thus is locally equivalent to a singlet state in a $\mathcal{C}^2\otimes\mathcal{C}^2$ product subspace of $\mathcal{C}^{n_1}\otimes\mathcal{C}^{n_2}$.

2. Bounds for the random robustness of mixed states of two-party systems

For any ρ of a two-party system with Hilbert space $\mathcal{C}^{n_1}\otimes\mathcal{C}^{n_2}$ of dimension $n=n_1n_2$, and for λ the smallest eigenvalue of ρ^{T_B}, the following bounds hold (Appendix C):

$$n|\min(\lambda,0)|\leqslant R\left(\rho\left|\left|\frac{1}{n}I\right.\right.\right)\leqslant\frac{n}{2}. \tag{42}$$

The upper bound is of some interest, for it indicates how any state of a two-party system can be offhand explicitly written in terms of a local pseudomixture, and it can be generalized to the *N*-party case, where it reads

$$R\left(\rho\left|\left|\frac{1}{n}I\right.\right.\right)\leqslant\left(1+\frac{n}{2}\right)^{N-1}-1, \tag{43}$$

as was already mentioned at the end of Sec. II B.

3. Random robustness of a two-qubit system and of a qubit-qutrit system

Because in $\mathcal{C}^2\otimes\mathcal{C}^2$ and $\mathcal{C}^2\otimes\mathcal{C}^3$ the condition $\rho^{T_B}\geqslant 0$ is not only necessary but also sufficient for ρ to be separable [17,18], the lower bound in Eq. (42), which was based on this condition, becomes an equality:

$$R\left(\rho\left|\left|\frac{1}{n}I\right.\right.\right)=n|\min(\lambda,0)|. \tag{44}$$

V. APPLICATION: EXPLICIT LOWER BOUND FOR THE VOLUME OF SEPARABLE STATES

In [12] the space of states $\mathcal{T}$ was endowed with a measure, for which it was proved that the volume of the set of separable states $\mathcal{S}$ was nonzero compared to that of the whole set of states $\mathcal{T}$. We will next give an alternative proof of this result by computing an explicit lower bound for this volume. Following the proposal in [12], the set of states of a generic system $\mathcal{Q}$ can be viewed as a Cartesian product of two sets:

$$\mathcal{T}\sim\mathcal{P}\times\Delta, \tag{45}$$

where $\mathcal{P}$ is the set of complete families $\{P_k\}_{1,\ldots,n}$ of orthogonal rank one projectors (i.e., $\Sigma_{k=1}^n P_k=I,\mathrm{Tr}[P_kP_{k'}]=\delta_{k,k'},P_k^2=P_k$), and Δ is the convex subset of $\mathcal{R}^n$ generated by all possible convex combinations of the points $x_i\in\mathcal{R}^n$, $x_i\equiv(0,\ldots,0,1_i,0,\ldots,0)$, $i=1,\ldots,n$ [that is, Δ is the convex hull generated by $\{x_i\}_{i=1,\ldots,n}$ and thus a subset of the $(n-1)$-dimensional hyperplane which contains $\{x_i\}$]. For ν the measure induced on $\mathcal{P}$ by the Haar measure on the unitary group $U(n)$ and $\mathcal{L}_{n-1}$ the Lebesgue measure induced on $\Delta\subset\mathcal{R}^{n-1}$, it was argued in [12] that a natural measure on $\mathcal{T}$ is $\mu=\nu\times\mathcal{L}_{n-1}$. We have then found the following lower bound for the ratio of the volume of the sets $\mathcal{S}$ and $\mathcal{T}$ of an *N*-party system with *n*-dimensional Hilbert space:

$$\frac{V(\mathcal{S})}{V(\mathcal{T})}\geqslant\left(\frac{1}{1+n/2}\right)^{(n-1)(N-1)}, \tag{46}$$

which indeed confirms that the volume of separable states is nonzero for any finite *n*.

Proof: Consider the function

$$\Theta(\{P_k\},\{\Lambda_k\})\equiv\begin{cases}1 & \text{if } \displaystyle\sum_{k=1}^n\Lambda_kP_k\in\mathcal{S}\\ 0 & \text{otherwise,}\end{cases} \tag{47}$$

where $\{\Lambda_k\}\in\Delta$. Then the ratio of the volumes $V(\mathcal{S})$ and $V(\mathcal{T})$ is, with the proposed measure $\mu=\nu\times\mathcal{L}_{n-1}$ on $\mathcal{T}=\mathcal{P}\times\Delta$,

$$\frac{V(\mathcal{S})}{V(\mathcal{T})}=\frac{\displaystyle\int_{U(n)}dU\int_\Delta d\Delta\ \Theta(\{P_k\},\{\Lambda_k\})}{\displaystyle\int_{U(n)}dU\int_\Delta d\Delta}. \tag{48}$$

Consider now another function $\Xi(\{P_k\},\{\Lambda_k\}) \leqslant \Theta(\{P_k\},\{\Lambda_k\})$. Then

$$\frac{V(\mathcal{S})}{V(\mathcal{T})} \geqslant \frac{\int_{U(n)} dU \int_{\Delta} d\Delta\ \Xi(\{P_k\},\{\Lambda_k\})}{\int_{U(n)} dU \int_{\Delta} d\Delta}. \tag{49}$$

If one can choose this function Ξ to be independent of $\{P_k\}$, then the integral over the unitary group in the numerator of Eq. (49) will factor out and will be canceled by that in the denominator. As we will argue, the following one does the job:

$$\Xi(\{\Lambda_k\}) \equiv \begin{cases} 1 & \text{if } \{\Lambda_k\} \in \Delta_p \\ 0 & \text{otherwise,} \end{cases} \tag{50}$$

where $\Delta_p \equiv \text{convexhull}\{y_i \in \mathcal{R}^n; y_i = px_i + (1-p)z_I, i=1,\ldots,n\}$, with $z_I \equiv (1/n,\ldots,1/n)$ and $p=[1/(1+n/2)]^{N-1}$. Then one can see that, since the simplex Δ_p has edges p times smaller than Δ,

$$\int_{\Delta} d\Delta \Xi(\{\Lambda_k\}) = \int_{\Delta_p} d\Delta = p^{n-1} \int_{\Delta} d\Delta, \tag{51}$$

from where the lower bound easily follows.

To see that any state $\Sigma_{k=1}^{n} \Lambda_k P_k$ is separable for any family $\{P_k\}$ provided that $\{\Lambda_k\} \in \Delta_p$ (that is, to see that $\Theta \geqslant \Xi$), one can resort to the upper bound for the random robustness Eq. (C8) computed at the end of Appendix C. Since $R(\rho || (1/n)I) \leqslant (1+n/2)^{N-1} - 1 \equiv \tilde{t}$, we find that a p, independent of ρ, such that

$$p\rho + (1-p)\frac{1}{n}I \tag{52}$$

belongs to the set of separable states $\mathcal{S}$, is $p \equiv 1/(1+\tilde{t}) = [1/1+n/2]^{N-1}$. Each point $\{\Lambda_k\} \in \Delta_p$ has components $\Lambda_k = q_k p + (1-p)/n$ for some $q_k \geqslant 0$ such that $\Sigma_{k=1}^{n} q_k = 1$. Then

$$\begin{aligned} \sum_{k=1}^{n} \Lambda_k P_k &= p \sum_{k=1}^{n} q_k P_k + (1-p) \sum_{k=1}^{n} \frac{P_k}{n} \\ &= \sum_{k=1}^{n} q_k \left[p P_k + (1-p)\frac{1}{n} I \right], \end{aligned} \tag{53}$$

which is a convex combination $\Sigma_{k=1}^{n} q_k \rho_{s,k}$ of separable states $\rho_{s,k} \equiv pP_k + (1-p)(1/n)I$, and therefore is also separable.

ACKNOWLEDGMENTS

G.V. would like to thank the members of the Department of Physics, University of Wales, Swansea, for their hospitality during his stay there, where part of this paper was elaborated. He is especially grateful to Mark Emmett, Ben White, Alex Dougall, and Ho Joon Lee. G.V. also acknowledges CIRIT Grant No. 1997FI-00068 PG. R.T. acknowledges financial support from CICYT, under Contract No. AEN95-0590, and from CIRIT, under Contract No. 1996GR00066. We thank the participants of the Benasque Center for Physics '98 session for comments and criticism.

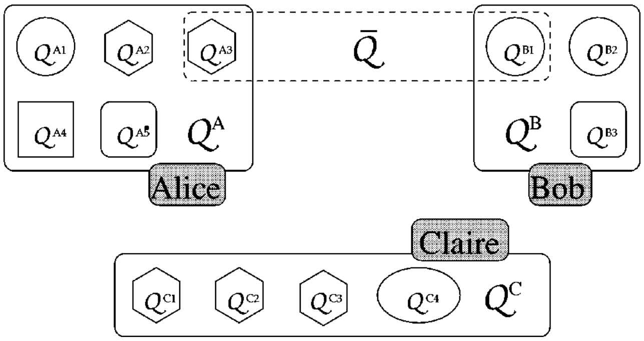

FIG. 3. Example of a composite system shared by parties. Twelve local partial subsystems of five different types, and thus not all identical, are grouped together into three local subsystems, according to which physicist or party—Alice, Bob, or Claire—can act on them. One can also consider nonlocal subsystems, such as $\bar{\mathcal{Q}} \equiv \mathcal{Q}^{A3} \cup \mathcal{Q}^{B1}$, which involve partial subsystems belonging to different local subsystems.

APPENDIX A: NOTATION

Entanglement appears in composite systems, where divisions—and yet subdivisions—into constituent parts easily proliferate. These may imply working with a multitude of Hilbert spaces which, together with having to deal with different types of states, easily leads to confusion. We have chosen to label symbols such as $\mathcal{Q}$, $\mathcal{H}$, ρ (standing for physical systems, Hilbert spaces, states, etc.) with a superindex to refer to a specific local subsystem, the parties being called after the name of a physicist—Alice, Bob, etc.—following the tradition. On the other hand, subindices will denote different elements of a collection of states.

The following list contains some of the symbols we have used, along with a short explanation of their meaning. In some cases we indicate how they are related to each other. See also the example in Fig. 3. $\mathcal{Q}$, physical system, composed of N local subsystems; $\mathcal{H}$, Hilbert space of $\mathcal{Q}$, of dimension n; $\Psi,\Phi,\ldots,$ pure states of $\mathcal{Q}$; ρ, mixed state of $\mathcal{Q}$, or exceptionally of a nonlocal subsystem of $\mathcal{Q}$; $\mathcal{Q}^i$, local subsystem i $(i=1,\ldots,N)$, i.e., subsystem where party i can act without further ado (the index i will often be a capital letter instead of a number, that is $i=A,B,C,\ldots$); $\mathcal{H}^i$, Hilbert space of $\mathcal{Q}^i$, of dimension n_i; Ψ^i,ρ^i, states of $\mathcal{Q}^i$; $\cup_{i=1}^{N}\mathcal{Q}^i = \mathcal{Q}$, $\otimes_{i=1}^{N}\mathcal{H}^i = \mathcal{H}$ $(\Pi_{i=1}^{N} n_i = n)$; $\mathcal{Q}^{i,j}$, local partial subsystem or part j of the local subsystem $i, j=1,\ldots,N_i$; $\mathcal{H}^{i,j}$, Hilbert space of $\mathcal{Q}^{i,j}$; $\cup_{j=1}^{N_i}\mathcal{Q}^{i,j} = \mathcal{Q}^i$, $\otimes_{j=1}^{N_i}\mathcal{H}^{i,j} = \mathcal{H}^i$; $\mathcal{Q}\backslash\tilde{\mathcal{Q}}$, system obtained from $\mathcal{Q}$ by dismissing a (local or nonlocal) subsystem $\tilde{\mathcal{Q}}$; $\rho_k, t_k, \ldots,$ element k of a collection of states, weights, etc. (typically $k=1,\ldots,l$); $\mathcal{T}$, set of states; $\mathcal{S}$, set of separable states; ρ_s, separable state, i.e., $\rho_s \in \mathcal{S}$.

APPENDIX B: ROBUSTNESS AND RANDOM ROBUSTNESS OF PURE STATES OF TWO-PARTY SYSTEMS

Proving that the robustness of any pure state Ψ in $\mathcal{C}^m \otimes \mathcal{C}^m$ is

$$R(\Psi(\{a_i\}))=\left(\sum_{i=1}^{m} a_i\right)^2-1 \tag{B1}$$

will take two steps. In the first step a local pseudomixture $\{\rho_s^+,\rho_s^-,t\}$, such that $t=(\Sigma_i a_i)^2-1$, will be explicitly constructed for Ψ. In the second one it will be proved that this local pseudomixture $\{\rho_s^+,\rho_s^- t\}$ is optimal, so that $t(\Psi;\rho_s^+,\rho_s^-)$ is $R(\Psi)$. Then from Eq. (B1) it will be easy to obtain the random robustness of Ψ,

$$R\left(\Psi(\{a_i\})\middle\|\frac{1}{n}I\right)=na_1a_2, \tag{B2}$$

To further illustrate the issue, the case $\mathcal{C}^2\otimes\mathcal{C}^2$ will be treated in more detail.

1. Proof of Eq. (B1)

Consider, thus, a pure state $\Psi\in\mathcal{C}^m\otimes\mathcal{C}^m$, and its ordered Schmidt decomposition:

$$|\Psi\rangle=\sum_{i=1}^{m} a_i|ii\rangle,\quad a_i\geqslant a_{i+1}\geqslant 0,\quad \sum_{i=1}^{m} a_i^2=1, \tag{B3}$$

where, from now on, $|ef\rangle\equiv|e\rangle\otimes|f\rangle\in\mathcal{C}^m\otimes\mathcal{C}^m$ and, unless otherwise specified, $\{|i\rangle\}_{i=1,\ldots,m}$ is an orthonormal basis in $\mathcal{C}^m$. We are interested in statistically mixing Ψ with pure product states in such a way that the final mixture is separable and the statistical weight of the separable part is minimal. Let us define $R\equiv\Sigma_{i\neq j}a_ia_j=(\Sigma_i a_i)^2-1$ and also

$$\rho_s^-\equiv\frac{1}{R}\sum_{i\neq j} a_ia_j|ij\rangle\langle ij|, \tag{B4}$$

$$\rho_s^+\equiv\frac{1}{1+R}(|\Psi\rangle\langle\Psi|+R\rho_s^-). \tag{B5}$$

Notice that ρ_s^- is a separable state by construction, since it has been built as a convex combination of projectors onto product vectors $|ij\rangle$. Next it will be shown that ρ_s^+ is a separable state as well.

Consider the following convex combination:

$$\rho_s\equiv\frac{1}{\alpha_{m+1}}\sum_{r=1}^{\alpha_{m+1}}|e_re_r^*\rangle\langle e_re_r^*|, \tag{B6}$$

where the components of $|e_r\rangle\in\mathcal{C}^m$ are

$$\langle i|e_r\rangle\equiv\frac{\sqrt{a_i}}{(1+R)^{1/4}}\exp\left(\frac{2\pi J}{\alpha_{m+1}}\alpha_i r\right)\quad (J\equiv\sqrt{-1}), \tag{B7}$$

$\langle i|e_r^*\rangle$ is just the complex conjugate of $\langle i|e_r\rangle$, and the coefficients α_j are defined by

$$\alpha_j\equiv 2\alpha_{j-1}+1, \tag{B8}$$

$$\alpha_1\equiv 0. \tag{B9}$$

To see that $\rho_s^+=\rho_s$, and that therefore ρ_s^+ is separable, consider the matrix element of $\Sigma_{r=1}^{\alpha_{m+1}}|e_re_r^*\rangle\langle e_re_r^*|$:

$$\sum_{r=1}^{\alpha_{m+1}}\langle ij|e_re_r^*\rangle\langle e_re_r^*|kl\rangle$$
$$=\frac{\sqrt{a_ia_ja_ka_l}}{1+R}\sum_{r=1}^{\alpha_{m+1}}\exp\left\{\frac{2\pi Jr}{\alpha_{m+1}}(\alpha_i+\alpha_k-\alpha_j-\alpha_l)\right\}. \tag{B10}$$

Now, since $0\leqslant i,j,k,l<m+1$ (and recalling that $\alpha_{m+1}>2\alpha_m$), the quantity $|\alpha_i+\alpha_k-\alpha_j-\alpha_l|$ is always smaller than α_{m+1}. Taking this into account, and also the fact that

$$\alpha_i+\alpha_k-\alpha_j-\alpha_l=0\Leftrightarrow\left\{\begin{array}{c}\left.\begin{array}{c}i=j\\ k=1\end{array}\right\}\\ \text{and/or}\\ \left.\begin{array}{c}i=l\\ j=k\end{array}\right\}\end{array}\right. \tag{B11}$$

we are left with the only nonvanishing elements

$$\langle ii|\rho_s|jj\rangle=\langle ij|\rho_s|ij\rangle=\frac{a_ia_j}{1+R}. \tag{B12}$$

This proves $\rho_s^+=\rho_s$ and thus that ρ_s^+ is separable.

Let us now see that there is no separable state ρ_s such that

$$\frac{1}{1+t}(|\Psi\rangle\langle\Psi|+t\rho_s) \tag{B13}$$

is separable with $t<R$. Recall that a necessary condition for ρ to be separable is that its partial transposition ρ^{T_i} (in the Hilbert space $\mathcal{H}^i$ of party i, $i=A,B$ in this case) be nonnegative [17], that is,

$$\rho\in\mathcal{S}\Rightarrow\rho^{T_i}\geqslant 0\quad\forall i. \tag{B14}$$

Then ρ_s and t must necessarily satisfy

$$\left\langle\Phi\middle|\frac{1}{1+t}(|\Psi\rangle\langle\Psi|+t\rho_s)^{T_B}\middle|\Phi\right\rangle\geqslant 0 \tag{B15}$$

for any $|\Phi\rangle\in\mathcal{C}^m\otimes\mathcal{C}^m$. Define a set of Bell states:

$$|\Phi_{ij}^+\rangle\equiv\frac{1}{\sqrt{2}}(|ij\rangle+|ji\rangle),\quad P_{ij}^+\equiv|\Phi_{ij}^+\rangle\langle\Phi_{ij}^+|, \tag{B16}$$

$$|\Phi_{ij}\rangle\equiv\frac{1}{\sqrt{2}}(|ij\rangle-|ji\rangle),\quad P_{ij}\equiv|\Phi_{ij}\rangle\langle\Phi_{ij}|. \tag{B17}$$

Then the spectral decomposition of $|\Psi\rangle\langle\Psi|^{T_B}$ can be expressed in terms of Φ_{ij}^+, Φ_{ij}, and $|ii\rangle$:

$$|\Psi\rangle\langle\Psi|^{T_B}=\sum_{i=1}^{m} a_i^2|ii\rangle\langle ii|+\sum_{i=1}^{m}\sum_{j>i}^{m} a_ia_j(P_{ij}^+-P_{ij}). \tag{B18}$$

Now, from Eq. (B15) for $|\Phi\rangle=|\Phi_{ij}\rangle$,

$$\left\langle\Phi_{ij}\middle|\frac{1}{1+t}(|\Psi\rangle\langle\Psi|^{T_B}+t\rho_s^{T_B})\middle|\Phi_{ij}\right\rangle\geqslant 0, \tag{B19}$$

which immediately leads to

$$\mathrm{Tr}(P_{ij}\rho_s^{T_B}) \geqslant \frac{a_i a_j}{t}. \tag{B20}$$

Then, taking into account that $\Sigma_{i,j>i} a_i a_j = \frac{1}{2}(\Sigma_i a_i^2 - 1)$, we get

$$\sum_{i,j>i} \mathrm{Tr}(P_{ij}\rho_s^{T_B}) \geqslant \frac{R}{2t}. \tag{B21}$$

It will next be proved that $\Sigma_{i,j>i}\mathrm{Tr}(P_{ij}\rho_s^{T_B}) \leqslant \frac{1}{2}$, which implies, together with Eq. (B21), that $t \geqslant R$. Thus the proposed local pseudomixture is an optimal one, and $R(\Psi) = R$.

Define the projector $M \equiv \Sigma_{i,j>i} P_{ij}$ and consider a symmetric unitary product transformation $U_\alpha \otimes U_\alpha$.

Theorem B.1. $[M, U_\alpha \otimes U_\alpha] = 0$.

Proof: For any $i,j, M|ij\rangle = P_{ij}|ij\rangle = \frac{1}{2}(|ij\rangle - |ji\rangle)$, and, if $U_\alpha|i\rangle = \Sigma_{i'} b_{i'}^i |i'\rangle$,

$$\begin{aligned} MU_\alpha \otimes U_\alpha |ij\rangle &= \sum_{i',j'} b_{i'}^i b_{j'}^j M|i'j'\rangle \\ &= \sum_{i',j'} b_{i'}^i b_{j'}^j \frac{1}{2}(|i'j'\rangle - |j'i'\rangle) \\ &= U_\alpha \otimes U_\alpha \frac{1}{2}(|ij\rangle - |ji\rangle) \\ &= U_\alpha \otimes U_\alpha M|ij\rangle. \end{aligned} \tag{B22}$$

This proves the theorem, since $\{|ij\rangle\}_{i,j=1,\dots,m}$ is a basis of the whole Hilbert space. □

Theorem B.2 (necessary condition for separability).

$$\rho \in \mathcal{S} \Rightarrow \mathrm{Tr}[\rho M] \leqslant \frac{1}{2}. \tag{B23}$$

Proof: Recall that if ρ is separable, then it can be expressed as a convex combination of (not necessarily orthogonal) projectors onto product vectors $|f_k g_k\rangle$, that is, $\rho = \Sigma_k p_k |f_k g_k\rangle\langle f_k g_k|$. Consider the following quantity:

$$M_{fg} \equiv \langle fg|M|fg\rangle. \tag{B24}$$

It will be proved that $M_{fg} \leqslant \frac{1}{2}$ for any product vector $|fg\rangle$, and that therefore

$$\mathrm{Tr}[\rho M] = \sum_k p_k M_{f_k g_k} \leqslant \frac{1}{2}. \tag{B25}$$

Indeed, by noticing that Theorem B.1 implies that $M_{U_\alpha f U_\alpha g} = M_{fg}$, since

$$\mathrm{Tr}[U_\alpha \otimes U_\alpha \ |fg\rangle\langle fg|U_\alpha^{-1} \otimes U_\alpha^{-1} M] = \mathrm{Tr}[|fg\rangle\langle fg|M], \tag{B26}$$

instead of M_{fg} we can compute $M_{1\tilde{g}}$, where

$$|1\tilde{g}\rangle \equiv \left(\begin{array}{l} 1 \\ 0 \\ \dots \\ 0 \end{array} \left.\vphantom{\begin{array}{l} 1 \\ 0 \\ \dots \\ 0 \end{array}}\right\} m-1 \right) \otimes \begin{pmatrix} \tilde{g}_1 \\ \tilde{g}_2 \\ \dots \\ \tilde{g}_m \end{pmatrix} \tag{B27}$$

for some $|\tilde{g}\rangle = U_\alpha|g\rangle$, where U_α is such that $|1\rangle = U_\alpha|f\rangle$. Then,

$$\begin{aligned} \langle 1\tilde{g}|M|1\tilde{g}\rangle &= \sum_{i,j>i} \langle 1\tilde{g}|P_{ij}|1\tilde{g}\rangle = \sum_{j=2}^{m} \langle 1\tilde{g}|P_{1j}|1\tilde{g}\rangle \\ &= \frac{1}{2}\sum_{j>=2}^{m} |\langle j|\tilde{g}\rangle|^2 \leqslant \frac{1}{2}|\langle \tilde{g}|\tilde{g}\rangle|^2 = \frac{1}{2}. \ \square \end{aligned} \tag{B28}$$

2. Proof of Eq. (B2)

Now the result

$$R\left(\Psi(\{a_i\}) \middle\| \frac{1}{n}I\right) = n a_1 a_2, \tag{B29}$$

where $n \equiv n_1 n_2$ is the dimension of the Hilbert space $\mathcal{H} = \mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}$ of the two-party system, follows straightforwardly from the previous considerations. Indeed, with $m \equiv \min(n_1, n_2)$, $R_r \equiv n_1 n_2 a_1 a_2$, and R given by Eq. (B1) ($R_r \geqslant R$ by construction), the separable state $(1/n)I$ can be written as a convex combination of ρ_s^- from Eq. (B4) and another manifestly separable state $\tilde{\rho}_s$:

$$\begin{aligned} \frac{1}{n}I &= \frac{1}{n}\sum_{i=1}^{n_1}\sum_{j=1}^{n_2} |ij\rangle\langle ij| \\ &= \frac{1}{R_r}\left(\sum_{i=1}^{m}\sum_{j=1}^{m} a_i a_j |ij\rangle\langle ij| + \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} c_{ij}|ij\rangle\langle ij| \right) \\ &= \frac{1}{R_r}[R\rho_s^- + (R_r - R)\tilde{\rho}_s], \end{aligned} \tag{B30}$$

where

$$c_{ij} \equiv \begin{cases} a_1 a_2 - a_i a_j \ \ (\geqslant 0) & \text{if } i,j \leqslant m \\ a_1 a_2 \quad \text{otherwise,} \end{cases} \tag{B31}$$

and

$$\tilde{\rho}_s \equiv \frac{1}{R_r - R}\sum_{i=1}^{n_1}\sum_{j=1}^{n_2} c_{ij}|ij\rangle\langle ij| \in \mathcal{S}. \tag{B32}$$

Then $[1/(1+R_r)][|\Psi\rangle\langle\Psi| + R_r(1/n)I] = [1/(1+R_r)][(1+R)\rho_s^+ + (R_r - R)\tilde{\rho}_s]$, where ρ_s^+ was defined in Eq. (B5), is manifestly separable, whereas one could check that for any $\epsilon > 0$

$$\langle \Phi_{12}||\Psi\rangle\langle\Psi|^{T_B} + (R_r - \epsilon)\frac{1}{n}I^{T_B}|\Phi_{12}\rangle = -\frac{\epsilon}{n} < 0, \tag{B33}$$

so that, recalling the necessary condition for separability discussed in Eq. (B14), R_r is the minimum amount of $(1/n)I$ that mixed with $|\Psi\rangle\langle\Psi|$ makes it separable, that is, $R(\Psi||(1/n)I)=R_r$.

3. Pure state of the smallest composite system

Let us finally consider, as an example, a pure state of the smallest composite system: a system of two qubits. In this case the Hilbert space is $\mathcal{C}^2\otimes\mathcal{C}^2$, and the ordered Schmidt decomposition allows us to express with an adequate choice of basis any pure state Ψ as

$$|\Psi\rangle=a_1|1\rangle\otimes|1\rangle+a_2|2\rangle\otimes|2\rangle=\begin{pmatrix}a_1\\0\\0\\a_2\end{pmatrix}. \tag{B34}$$

Then, using the definitions given in Appendix B1, $R=2a_1a_2$,

$$\rho_s^-\equiv\frac{1}{2}(|12\rangle\langle12|+|21\rangle\langle21|)=\frac{1}{2}\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}, \tag{B35}$$

and

$$\rho_s^+=\frac{1}{1+R}\begin{pmatrix}a_1^2&0&0&a_1a_2\\0&a_1a_2&0&0\\0&0&a_1a_2&0\\a_1a_2&0&0&a_2^2\end{pmatrix}. \tag{B36}$$

To check that $\rho_s^+=\rho_s$ as given by Eq. (B6) let us specify it for our example:

$$\rho_s=\frac{1}{3}\sum_{k=1}^{3}|e_re_r^*\rangle\langle e_re_r^*|, \tag{B37}$$

where

$$|e_re_r^*\rangle\equiv\begin{pmatrix}a_1^{1/2}\\a_2^{1/2}\exp\left\{\dfrac{2\pi J}{3}r\right\}\end{pmatrix}\otimes\begin{pmatrix}a_1^{1/2}\\a_2^{1/2}\exp\left\{\dfrac{-2\pi J}{3}r\right\}\end{pmatrix}. \tag{B38}$$

More explicitly,

$$\rho_s=\frac{1}{3(1+R)}\sum_{r=1}^{3}N_r, \tag{B39}$$

with N_r given by

$$\begin{pmatrix}a_1^2 & a_1^{3/2}a_2^{1/2}\exp\left\{\dfrac{2\pi J}{3}r\right\} & a_1^{3/2}a_2^{1/2}\exp\left\{\dfrac{-2\pi J}{3}r\right\} & a_1a_2\\ a_1^{3/2}a_2^{1/2}\exp\left\{\dfrac{-2\pi J}{3}r\right\} & a_1a_2 & a_1a_2\exp\left\{\dfrac{-2\pi J}{3}2r\right\} & a_1^{1/2}a_2^{3/2}\exp\left\{\dfrac{-2\pi J}{3}r\right\}\\ a_1^{3/2}a_2^{1/2}\exp\left\{\dfrac{2\pi J}{3}r\right\} & a_1a_2\exp\left\{\dfrac{2\pi J}{3}2r\right\} & a_1a_2 & a_1^{1/2}a_2^{3/2}\exp\left\{\dfrac{2\pi J}{3}r\right\}\\ a_1a_2 & a_1^{1/2}a_2^{3/2}\exp\left\{\dfrac{2\pi J}{3}r\right\} & a_1^{1/2}a_2^{3/2}\exp\left\{\dfrac{-2\pi J}{3}r\right\} & a_2^2\end{pmatrix}. \tag{B40}$$

The sum over r now reproduces Eq. (B36) immediately so that $\rho_s=\rho_s^+$. Some of the expressions used in proving that the local pseudomixture $\{\rho_s^+,\rho_s^-,R\}$ is optimal read for our example

$$\begin{aligned}|\Psi\rangle\langle\Psi|^{T_B}&=a_1^2|11\rangle\langle11|+a_2^2|22\rangle\langle22|+a_1a_2(P_{12}^+-P_{12})\\&=\begin{pmatrix}a_1^2&0&0&0\\0&0&a_1a_2&0\\0&a_1a_2&0&0\\0&0&0&a_2^2\end{pmatrix},\end{aligned} \tag{B41}$$

and

$$|\Phi_{12}^+\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix},\quad |\Phi_{12}\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \tag{B42}$$

and Eq. (B21) is

$$\mathrm{Tr}(P_{12}\rho_s^{T_B})\geqslant\frac{a_1a_2}{t}, \tag{B43}$$

which, taking into account that $\langle fg|P_{12}|fg\rangle\leqslant\frac{1}{2}$ for any product vector $|fg\rangle$ (Theorem B.2), and consequently $\mathrm{Tr}(P_{12}\rho)\leqslant\frac{1}{2}$ for any separable ρ, implies that $R(\Psi)=R=(a_1+a_2)^2-1$.

Now $R_r = 4a_1a_2$ and the maximally random state in $\mathcal{C}^2 \otimes \mathcal{C}^2$ can be decomposed, following Theorem B.2, as a mixture of two separable states as follows:

$$\frac{1}{4}I = \frac{1}{R_r}\left\{ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & a_1a_2 & 0 & 0 \\ 0 & 0 & a_1a_2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} a_1a_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_1a_2 \end{pmatrix} \right\}, \tag{B44}$$

so that

$$\tilde{\rho}_s = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{B45}$$

in Eq. (B32).

APPENDIX C: MAINLY BOUNDS FOR ROBUSTNESS AND RANDOM ROBUSTNESS OF MIXED STATES OF TWO-PARTY SYSTEMS

1. $|\min(\{\lambda_j/a_{j,1}^2\},0)| \leqslant R(\rho)$

Proof: Assume that in the spectral decomposition of ρ^{T_B}, $\rho^{T_B} = \Sigma_{j=1}^{n} \lambda_j |\Psi_j\rangle\langle\Psi_j|$, at least one eigenvalue, say λ_j, is negative. Calling the nonlocal coefficients of the ordered Schmidt decomposition of the corresponding eigenvector $|\Psi_j\rangle$, $\{a_{j,i}\}$, one finds that, for $\rho_s \in \mathcal{S}$, if $\langle\Psi_j|(\rho + t\rho_s)^{T_B}|\Psi_j\rangle$ is to be non-negative (which is a necessary condition for $[1/(1+t)](\rho + t\rho_s)$ to be separable), then $t \geqslant -\lambda_j/\langle\Psi_j|\rho_s^{T_B}|\Psi_j\rangle$. We will next prove that $|\langle\Psi_j|p\rangle| \leqslant a_{j,1}$ for any product vector $|p\rangle$, and therefore $\langle\Psi_j|\rho_s^{T_B}|\Psi_j\rangle \leqslant a_{j,1}^2$, which implies the lower bound for the robustness of ρ. If, on the contrary, no $\lambda_j < 0$ exists, no significant bound is obtained.

Theorem C.1. If $|\Psi\rangle = \Sigma_{i=1}^{m} a_i |i\rangle \otimes |i\rangle$ is the ordered Schmidt decomposition of the normalized vector $|\Psi\rangle \in \mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}$ [i.e., $m = \min(n_1, n_2)$, $a_i \geqslant a_{i+1} \geqslant 0$, and $\{|i\rangle\}_{i=1,\ldots,m}$ are othonormal vectors] and $|p\rangle \equiv |p_1\rangle \otimes |p_2\rangle \in \mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}$ is any normalized product vector, then $|\langle\Psi|p\rangle| \leqslant a_1$.

Proof: For $p_{1,i} \equiv \langle i|p_1\rangle$ and $p_{2,i} \equiv \langle i|p_2\rangle$, one gets

$$|\langle\Psi|p\rangle| = \left|\sum_{i=1}^{m} a_i p_{1,i} p_{2,i}\right| \leqslant \sum_{i=1}^{m} a_i |p_{1,i} p_{2,i}| \leqslant a_1 \sum_{i=1}^{m} |p_{1,i} p_{2,i}| \tag{C1}$$

$$\leqslant a_1 \sqrt{\sum_{i=1}^{m} |p_{1,i}|^2} \sqrt{\sum_{i=1}^{m} |p_{2,i}|^2}$$

$$\leqslant a_1 \sqrt{\langle p|p\rangle} = a_1 \ . \ \square \tag{C2}$$

2. $R(\rho) \leqslant \tilde{m} - 1$, where $\tilde{m} = \min(\text{rank}[\rho^A], \quad \text{rank} \ [\rho^B])$

Proof: For $\tilde{\mathcal{H}} \subseteq \mathcal{H}$ the product subspace spanned by the eigenvectors of $\rho^A \otimes \rho^B$ with nonvanishing eigenvalue, any rank one projector in a convex combination of ρ happens to project into $\tilde{\mathcal{H}}$, that is, if $\rho = \Sigma p_k |\Psi_k\rangle\langle\Psi_k|$, then $|\Psi_k\rangle \in \tilde{\mathcal{H}}$. But $R(\Psi_k) = (\Sigma_{i=1}{}^{\tilde{m}} a_i)^2 - 1 \leqslant (\Sigma_{i=1}{}^{\tilde{m}} 1/\sqrt{\tilde{m}})^2 - 1 = \tilde{m} - 1$. Then, since $R(\rho)$ is a convex function, $R(\rho) \leqslant \Sigma p_k R(\Psi_k) \leqslant \tilde{m} - 1$.

3. $R(\rho) \leqslant R(\rho||(1/n)\tilde{I})$

$R(\rho) \leqslant R(\tilde{\rho}||(1/\tilde{n})\tilde{I})$ follows from the fact that $(1/\tilde{n})\tilde{I}$ is a separable state, and $R(\tilde{\rho}) = R(\rho)$ is the minimum of the relative robustness $R(\tilde{\rho}||\rho_s)$.

4. $R(\rho) \leqslant 2|\lambda| \ \ (\mathcal{C}^2 \otimes \mathcal{C}^2)$

Proof: The partially transposed ρ^{T_B} of any inseparable density matrix ρ in $\mathcal{C}^2 \otimes \mathcal{C}^2$ always has a negative eigenvalue λ [11], for a certain eigenvector $|n\rangle = \cos\theta|11\rangle + \sin\theta|22\rangle$. (Here we choose the local basis $\{|ij\rangle\}_{i,j=1,2}$ to be that defined by the Schmidt decomposition of $|n\rangle$). For $\rho_s \equiv \cos^2\theta|11\rangle\langle 11| + \sin^2\theta|22\rangle\langle 22|$ it can be checked that $-|n\rangle\langle n| + 2\rho_s \geqslant 0$, which implies that

$$\frac{1}{1+2|\lambda|}(\rho + 2|\lambda|\rho_s) \tag{C3}$$

is a separable state.

5. $R(\rho) \leqslant C(\rho)(\mathcal{C}^2 \otimes \mathcal{C}^2)$

Proof: The robustness $R(\Psi)$ and the concurrence $C(\Psi)$ are equal for any pure state of $\mathcal{C}^2 \otimes \mathcal{C}^2$, and in [15] it was proved that one can always find a realization $\{\Psi_k, p_k\}$ of four pure states for ρ such that $C(\Psi_k) = C(\rho)$ $\forall k$. Then, using the convexity of $R(\rho)$, we find that for this realization

$$R(\rho) \leqslant \sum_{k=1}^{4} p_k R(\Psi_k) = \sum_{k=1}^{4} p_k C(\Psi_k) = C(\rho). \tag{C4}$$

6. $R(\rho(p,q_1,q_2,\theta)) = (1-p)\sin 2\theta - pq_2$ if $\rho^{T_B} \ngeqslant 0$ $(\mathcal{C}^2 \otimes \mathcal{C}^2)$

Proof: $\langle\Phi|\rho^{T_B}|\Phi\rangle = \frac{1}{2}[pq_2 - (1-p)\sin 2\theta]$ for $|\Phi\rangle \equiv (1/\sqrt{2})(|12\rangle - |21\rangle)$. Then a necessary condition for

$$\frac{1}{1+t}(\rho + t\rho_s) \tag{C5}$$

to be separable for a separable ρ_s is that $\langle\Phi|(\rho + t\rho_s)^{T_B}|\Phi\rangle \geqslant 0$, that is, $-\langle\Phi|\rho^{T_B}|\Phi\rangle \leqslant t\langle\Phi|\rho_s^{T_B}|\Phi\rangle$. But in Appendix B it was proved that $\langle\Phi|\rho_s^{T_B}|\Phi\rangle \leqslant \frac{1}{2}$, so that $t \geqslant (1-p)\sin 2\theta - pq_2$. Moreover one can check that $\rho_s \equiv \frac{1}{2}|12\rangle\langle 12| + |21\rangle\langle 21|$ with weight $t = (1-p)\sin 2\theta - pq_2$ makes the density matrix in Eq. (C5) separable.

7. $R(\rho||(1/n)I) \geqslant n|\min(\{\lambda_k\},0)|$

Proof: For any ρ consider the spectral decomposition of ρ^{T_B},

$$\rho^{T_B}=\sum_{k=1}^{n}\lambda_k|\Psi_k\rangle\langle\Psi_k|, \tag{C6}$$

where we take $\lambda_k\leqslant\lambda_{k+1}$ (and we take into account also eigenvectors with vanishing eigenvalue), and suppose $\lambda_1<0$. Then $[\rho+n|\lambda_1|(1/n)I]^{T_B}=\Sigma_{k=1}^{n}(|\lambda_1|+\lambda_k)|\Psi_k\rangle\langle\Psi_k|$ is manifestly non-negative definite (which is a necessary condition for the separability of $1/(1+n|\lambda_1|)[\rho+n|\lambda_1|(1/n)I]$), whereas for any $\epsilon>0$,

$$\left\langle\Psi_1\left|\left(\rho+(n|\lambda_1|-\epsilon)\frac{1}{n}I\right)^{T_B}\right|\Psi_1\right\rangle=-\frac{\epsilon}{n}<0. \tag{C7}$$

If $\lambda_1\geqslant 0$ no significant bound is obtained.

8. $R(\rho||(1/n)I)\leqslant n/2$

For $N=2$ the bound $R(\rho||(1/n)I)\leqslant n/2$ is a consequence of the fact that for any pure state of a two-party system $R(\Psi||(1/n)I)=na_1a_2\leqslant n/2$, and of the convexity of $R(\rho||(1/n)I)$ as a function of ρ, that the reader can easily prove. Its generalization to N-party systems,

$$R\left(\rho\left|\left|\frac{1}{n}I\right.\right.\right)\leqslant\left(1+\frac{n}{2}\right)^{N-1}-1, \tag{C8}$$

can be derived from the previous result and we will explain it only for $N=3$, the $N>3$ case following straightforwardly. Consider a pure state Ψ^{ABC} shared by Alice, Bob, and Claire. If we first think of Bob and Claire as a single party, then we have seen that the state

$$\frac{1}{1+n/2}\left(|\Psi^{ABC}\rangle\langle\Psi^{ABC}|+\frac{n}{2}\frac{1}{n}I\right) \tag{C9}$$

is separable if considered as belonging to a two-party system, that of Alice as one party and Bob and Claire as the other, and therefore can be expressed as a convex combination $\Sigma_k p_k|\psi_k^A\rangle\langle\psi_k^A|\otimes|\phi_k^{BC}\rangle\langle\phi_k^{BC}|$ of pure states that are product in $\mathcal{H}^A\otimes\mathcal{H}^{BC}$. Now mixing any of these pure states with an amount $n/2$ of $(1/n)I$ we obtain a proper separable state:

$$\frac{1}{1+n/2}\left(|\psi^A\rangle\langle\psi^A|\otimes|\phi^{BC}\rangle\langle\phi^{BC}|+\frac{n}{2}\frac{1}{n}I\right) \tag{C10}$$

$$=\frac{1}{1+n/2}\left[|\psi^A\rangle\langle\psi^A|\otimes\left(|\phi^{BC}\rangle\langle\phi^{BC}|+\frac{n}{2}\frac{1}{n}I^{BC}\right)+\frac{n}{2}\frac{1}{n}(I^A-|\psi^A\rangle\langle\psi^A|)\otimes I^{BC}\right], \tag{C11}$$

where I^i is the identity matrix in $\mathcal{H}^i$. Indeed, $[1/(1+n_Bn_C/2)][|\phi^{BC}\rangle\langle\phi^{BC}|+(n/2)(1/n)I^{BC}]$ is a separable state in $\mathcal{H}^B\otimes\mathcal{H}^C$, whereas $[1/(n_A-1)](I^A-|\psi^A\rangle\langle\psi^A|)$ is a mixed state in $\mathcal{H}^A$, so that the right-hand side of Eq. (C11) is a convex combination of two manifestly separable states. Then, by adding an amount $n/2$ of the separable $(1/n)I$ to the state in Eq. (C9) we make it separable, and therefore mixing the initial pure state Ψ^{ABC} with an amount $n/2+(1+n/2)(n/2)=(1+n/2)^2-1$ of $(1/n)I$ is sufficient to wash out its quantum correlations.

[1] E. Schrödinger, Naturwissenschaften **23**, 807 (1935); **23**, 823 (1935); **23**, 844 (1935).

[2] A. Einstein, B. Podolski, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] E. Schmidt, Math. Ann. **63**, 433 (1906); see also A. Ekert and P. L. Knight, Am. J. Phys. **63**, 415 (1995).

[4] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[5] N. Linden and S. Popescu, Fortsch. Phys. **46**, 567 (1998).

[6] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[7] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1996).

[8] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. Thapliyal, and A. Uhlmann, e-print quant-ph/9803033.

[9] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).

[10] M. B. Plenio and V. Vedral, e-print quant-ph/9804075.

[11] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).

[12] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).

[13] M. Kuna, Acta Phys. Slov. **48**, 1 (1998).

[14] P. Horodecki, Phys. Lett. A **232**, 333 (1997).

[15] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[16] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[17] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[18] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).