

Reduction criterion for separability

N. J. Cerf,^{1,2} C. Adami,¹ and R. M. Gingrich¹

¹*W. K. Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, California 91125*

²*Information Systems Technology Section, Jet Propulsion Laboratory, Pasadena, California 91109*

(Received 31 October 1997; revised manuscript received 14 December 1998)

We introduce a separability criterion based on the positive map $\Gamma: \rho \rightarrow (\text{Tr } \rho) - \rho$, where ρ is a trace-class Hermitian operator. Any separable state is mapped by the tensor product of Γ and the identity into a non-negative operator, which provides a simple necessary condition for separability. This condition is generally not sufficient because it is vulnerable to the dilution of entanglement. In the special case where one subsystem is a quantum bit, Γ reduces to time reversal, so that this separability condition is equivalent to partial transposition. It is therefore also sufficient for 2×2 and 2×3 systems. Finally, a simple connection between this map for two qubits and complex conjugation in the “magic” basis [Phys. Rev. Lett. **78**, 5022 (1997)] is displayed. [S1050-2947(99)00708-8]

PACS number(s): 03.67.-a, 03.65.Bz, 89.70.+c

I. INTRODUCTION

The state of a quantum bipartite system AB is described as *separable* (or classically correlated) if it can be obtained by two parties A and B that prepare their subsystem according to some common instructions (see, e.g., Refs. [1,2]). Mathematically, this means that the density operator ρ characterizing the state of the bipartite system can be written as a convex sum of product states, that is,

$$\rho = \sum_i w_i (\rho_i^{(A)} \otimes \rho_i^{(B)}), \quad (1)$$

where the weights w_i satisfy $\sum_i w_i = 1$ and $0 \leq w_i \leq 1$. The w_i 's can be viewed as the probability distribution of a classical random variable that is known to both parties A and B and used by them to prepare their subsystem. Namely, if the subsystem A (and B) is prepared in state $\rho_i^{(A)}$ (and $\rho_i^{(B)}$) when the classical variable takes on value i , the state of the joint system AB is given by Eq. (1). A separable state ρ satisfies several interesting properties. The joint statistics of any pair of *local* observables O_A and O_B (measured separately on each subsystem) can be described classically, based on an underlying global “hidden” variable. For example, the quantum expectation value of the product $O_A O_B$ is given by

$$\text{Tr}[\rho(O_A \otimes O_B)] = \sum_i w_i \langle a \rangle_i \langle b \rangle_i, \quad (2)$$

where $\langle a \rangle_i = \text{Tr}[\rho_i^{(A)} O_A]$ and $\langle b \rangle_i = \text{Tr}[\rho_i^{(B)} O_B]$. In other words, the joint statistics of O_A and O_B can be understood classically, by assuming that the local statistics of the outcomes can be described separately for each $\rho_i^{(A)}$ and $\rho_i^{(B)}$, and that the correlations originate from a hidden variable i distributed according to w_i . Moreover, a separable system always satisfies Bell's inequalities (the converse is not true), so that the latter represent a *necessary* condition for separability (see, e.g., Ref. [1]). Note that any joint probability distribution can be represented as a convex combination of product distributions, so that classical probabilities are always separable in the above sense.

The decomposition of a separable state ρ into a convex mixture of product states is not unique in general, but the

fact that ρ is separable implies that there must exist at least one such decomposition. If no such decomposition can be found, then ρ is termed inseparable or entangled, and it can be viewed as *quantum* correlated. Except for the special case where ρ describes a pure state, the distinction between separable and inseparable states appears to be an extraordinarily difficult problem. More precisely, some mixed states can be “weakly” inseparable, in the sense that it is very hard to establish with certainty their inseparability. This is basically due to the difficulty of enumerating explicitly *all* the possible convex combinations of product states in order to detect that a state is actually inseparable. Still, it is possible to find some conditions that *all* separable states must satisfy, therefore allowing the detection of inseparability when a state violates one such condition. The most common example of such a *necessary* condition for separability is the satisfaction of Bell's inequalities. A state that violates Bell's inequalities is inseparable, while a state satisfying them may be separable or weakly inseparable [1].

More recently, a surprisingly simple *necessary* condition for separability has been discovered by Peres [2], which has been shown by Horodecki *et al.* [3] to be strong enough to guarantee separability for bipartite systems of dimension 2×2 and 2×3 . If the state ρ is separable, then the operator obtained by applying a *partial* transposition with respect to subsystem A (or B) to ρ must be positive, that is,

$$\rho^{T_A} = (\rho^{T_B})^* \geq 0. \quad (3)$$

Thus, this criterion amounts to checking that all the eigenvalues of the partial transposition of ρ are non-negative, which must be so for all separable states. In Hilbert spaces of dimensions 2×2 and 2×3 , this condition is actually *sufficient*, that is, it suffices for ruling out *all* inseparable states [3]. In larger dimensions, however, it is provably *not* sufficient, in the sense that it does not detect some weakly inseparable states [3,4]. A general necessary and sufficient condition for separability in arbitrary dimensions has been found by Horodecki *et al.* [3], which states that ρ is separable if and only if the tensor product of *any* positive map (a map is defined as positive if it maps positive operators into positive operators) acting on A and the identity acting on B maps ρ into a positive operator. Although very important in

theory, this criterion is hardly more practical than the definition of separability itself since it involves the characterization of the set of all positive maps. It appears to be useful mainly for 2×2 and 2×3 bipartite systems, where such a general characterization has been found [3].

In this paper, we introduce a positive map, $\Gamma: \rho \rightarrow (\text{Tr } \rho) - \rho$, inspired by the structure of the conditional amplitude operator discussed in Refs. [5,6]. This map gives rise to a simple *necessary* condition for separability in arbitrary dimensions. More specifically, it is shown in Sec. II that any separable state is mapped by the tensor product of Γ (acting on one subsystem A) and the identity (acting on the other B) into a non-negative operator. In other words, the eigenvalues of the operator $(\Gamma \otimes I)\rho = (\mathbb{I}_A \otimes \text{Tr}_A \rho) - \rho$ must all be non-negative if the (unit-trace) operator ρ is separable, which provides a simple test for separability called *reduction* criterion. This separability criterion has been independently derived by Horodecki and Horodecki in Ref. [7]. In the case where Γ is applied to a two-state system (quantum bit or spin-1/2 particle), as studied in Sec. III, this criterion corresponds to the time-reversal operation applied on one system with respect to the other one. As Peres' criterion has been shown to be unitarily equivalent to such a “local” time-reversal by Sanpera *et al.* [8], this reduction criterion is simply equivalent to Peres' for $2 \times n$ composite systems. Therefore, it also results in a *sufficient* condition for 2×2 and 2×3 systems, according to Ref. [3]. It also has a very simple geometric representation in the Hilbert-Schmidt representation of a 2×2 bipartite state. Finally, we demonstrate that the map Γ is connected to the complex conjugation operation in the “magic” basis for two qubits introduced recently by Hill and Wootters [9], which underlies an interesting connection with the entropy of formation [10]. In Appendix A, we illustrate the reduction separability condition by applying it to several separable or inseparable states, and compare it to the separability criterion based on partial transposition.

II. SEPARABILITY OF BIPARTITE MIXED STATES OF ARBITRARY DIMENSION

We consider a bipartite quantum system characterized by the density operator ρ_{AB} defined in the joint Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, where \mathcal{H}_A and \mathcal{H}_B have arbitrary dimensions d_A and d_B .

Definition 1. Define a linear map Λ which maps Hermitian operators on \mathcal{H}_{AB} into Hermitian operators on \mathcal{H}_{AB} :

$$\Lambda: \rho_{AB} \rightarrow \lambda_{AB} \equiv \mathbb{I}_A \otimes \rho_B - \rho_{AB} \quad \text{with } \rho_B = \text{Tr}_A[\rho_{AB}]. \quad (4)$$

This map commutes with a unitary transformation acting locally on A and B . Indeed, if ρ_{AB} undergoes a unitary transformation of the product form, i.e.,

$$\rho_{AB} \rightarrow \rho'_{AB} = (U_A \otimes U_B) \rho_{AB} (U_A^\dagger \otimes U_B^\dagger), \quad (5)$$

it is easy to check that $\rho'_B = \text{Tr}_A[\rho'_{AB}] = U_B \rho_B U_B^\dagger$, so that

$$\lambda_{AB} \rightarrow \lambda'_{AB} = (U_A \otimes U_B) \lambda_{AB} (U_A^\dagger \otimes U_B^\dagger), \quad (6)$$

i.e., λ_{AB} transforms just like ρ_{AB} . As a consequence, the spectrum of λ_{AB} is invariant under a $U_A \otimes U_B$ isomorphism on ρ_{AB} .

Theorem 1. A necessary condition for the separability of the state ρ_{AB} of a bipartite system AB is that it is mapped by Λ into a positive semidefinite operator, i.e., $\Lambda \rho_{AB} \geq 0$.

We need to prove that any separable state is mapped into a positive semidefinite operator λ_{AB} . Consider a *separable* bipartite system AB characterized by a convex combination of product states:

$$\rho_{AB} = \sum_i w_i (\rho_A^{(i)} \otimes \rho_B^{(i)}) \quad \text{with } \sum_i w_i = 1 \text{ and } 0 \leq w_i \leq 1, \quad (7)$$

where $\rho_A^{(i)}$ and $\rho_B^{(i)}$ are states in \mathcal{H}_A and \mathcal{H}_B , respectively. It is easy to verify that the operator $\lambda_{AB} = \Lambda \rho_{AB}$ is positive semidefinite,

$$\lambda_{AB} = \sum_i w_i [(\mathbb{I}_A - \rho_A^{(i)}) \otimes \rho_B^{(i)}] \geq 0 \quad (8)$$

since a sum of positive operators is a positive operator. Indeed, the two terms in square brackets are each ≥ 0 . ■

In short, the map Λ reveals nonseparability: if $\lambda_{AB} \neq 0$, then ρ_{AB} is inseparable. This necessary condition for the separability of mixed states is directly related to that based on the conditional amplitude operator (although it is simpler as it does not require the calculation of the latter operator) [6]. Moreover, it is easy to see that Λ conserves separability since it is linear and maps product states into product operators: if ρ_{AB} is separable, then $\lambda_{AB} \geq 0$ is also separable (or, in general, written as a convex sum of direct products). Let us now calculate the partial traces of λ_{AB} :

$$\lambda_A = \text{Tr}_B[\lambda_{AB}] = \mathbb{I}_A - \rho_A, \quad (9)$$

$$\lambda_B = \text{Tr}_A[\lambda_{AB}] = (d_A - 1) \rho_B, \quad (10)$$

where d_A is the dimension of \mathcal{H}_A . This shows that Λ does not preserve the trace in general. Indeed, the trace is scaled by an integer factor under Λ , that is, $\text{Tr}[\lambda_{AB}] = (d_A - 1) \text{Tr}[\rho_{AB}]$. Thus, Λ is *trace preserving* only in the special case where A is a two-state system (i.e., $d_A = 2$). It is also interesting to note that Λ is always *reversible*, the inverse map being given by

$$\Lambda^{-1}: \lambda_{AB} \rightarrow (d_A - 1)^{-1} (\mathbb{I}_A \otimes \lambda_B) - \lambda_{AB} = \rho_{AB}, \quad (11)$$

where λ_B is defined as above. Note that Λ is equal to its inverse Λ^{-1} only if $d_A = 2$. In that case, if λ_{AB} is separable, then $\Lambda^{-1}: \lambda_{AB} \rightarrow \rho_{AB} \geq 0$. (The fact that the inverse map reveals inseparability is true in this case only.)

The separability condition based on Λ is illustrated in Appendix A, where we consider several separable and inseparable states. As we will show in Sec. III, $\lambda_{AB} \geq 0$ results in the same condition as Peres' in the case of two quantum bits, in which case it is *sufficient* (see theorem 4); for larger dimensions, it is only necessary.

Remark 1. Following the approach of Horodecki *et al.* [3], the map Λ can be written as the tensor product of a positive linear map Γ and the identity, that is,

$$\Lambda = \Gamma \otimes I \quad \text{with } \Gamma: \rho \rightarrow (\text{Tr } \rho) - \rho, \quad (12)$$

where Γ acts on Hermitian operators in \mathcal{H}_A and the identity acts on operators in \mathcal{H}_B . Since Γ is a positive map, $\Lambda = \Gamma \otimes I$ maps *separable* states into *positive* operators [3]. It therefore results in a *necessary* condition for separability, according to theorem 1. The map Γ commutes with an arbitrary unitary transformation U , that is,

$$\Gamma(U\rho U^\dagger) = U(\Gamma\rho)U^\dagger, \quad (13)$$

which makes the separability condition based on $\Lambda = \Gamma \otimes I$ independent on the basis chosen for A and B . In the same manner, the inverse map Λ^{-1} can be written as

$$\Lambda^{-1} = \Gamma^{-1} \otimes I \quad \text{with } \Gamma^{-1}: \rho \rightarrow \frac{\text{Tr } \rho}{d-1} - \rho, \quad (14)$$

where d is the dimension of the Hilbert space of ρ . Note that Γ^{-1} is *not* a positive map for $d > 2$, so that Λ^{-1} is in general useless as far as detecting inseparability is concerned. This emphasizes that the reduction separability criterion is quite special in two dimensions (e.g., for a spin-1/2 particle or a quantum bit), as will be studied in Sec. III. Specifically, we will show that Γ applied to a two-dimensional system can be interpreted as time reversal. Consequently, the map Λ amounts to applying time reversal on subsystem A , while leaving subsystem B unchanged. Such a link between “local” time reversal and separability has recently been pointed out by Sanpera *et al.* [8].

Remark 2. It is interesting to consider the classical analog of the maps Γ and $\Lambda = \Gamma \otimes I$ to gain some insight into their physical meaning. First, applying Γ to a classical probability distribution p_i (diagonal ρ) corresponds to the transformation

$$p_i \rightarrow q_i = \sum_k p_k - p_i. \quad (15)$$

(Obviously, $q_j \geq 0$ is not normalized except for a binary distribution.) The classical analog of $\Lambda = \Gamma \otimes I$ is

$$p_{ij} \rightarrow q_{ij} = \left(\sum_k p_{k|j} - p_{i|j} \right) p_j = p_j - p_{ij}. \quad (16)$$

Since $p_{i|j}$ is a probability distribution in i , we always have $1 - p_{i|j} \geq 0$ so that $q_{ij} \geq 0$ and the separability criterion is fulfilled. This emphasizes that quantum inseparability (“ $q_{ij} < 0$ ”) may be viewed as resulting from a conditional probability that exceeds 1 (more precisely, an eigenvalue of $\rho_{A|B}$ which exceeds 1) [6].

Definition 2. Two additional maps from operators on \mathcal{H}_{AB} to operators on \mathcal{H}_{AB} can be defined: the *dual* map

$$\tilde{\Lambda}: \rho_{AB} \rightarrow \tilde{\lambda}_{AB} = \rho_A \otimes \mathbb{I}_B - \rho_{AB} \quad (17)$$

and the *symmetric* map

$$M: \rho_{AB} \rightarrow \mu_{AB} = \mathbb{I}_A \otimes \mathbb{I}_B - \rho_A \otimes \mathbb{I}_B - \mathbb{I}_A \otimes \rho_B + \rho_{AB}, \quad (18)$$

where $\rho_A = \text{Tr}_B[\rho_{AB}]$ and $\rho_B = \text{Tr}_A[\rho_{AB}]$.

The map Λ which we considered until now is related to the conditional amplitude operator of A conditionally on B , that is $\rho_{A|B}$ [6]. Of course, a similar linear map can be de-

fined using the amplitude operator $\rho_{B|A}$, and exactly the same conclusions follow. This is the *dual* map $\tilde{\Lambda}$ defined in Eq. (17). It is trace preserving and self-inverse in the case where $d_B = 2$. It can obviously be written as the tensor product $\tilde{\Lambda} = I \otimes \Gamma$, where Γ now acts on operators on \mathcal{H}_B , and therefore commutes with a $U_A \otimes U_B$ isomorphism. Since Γ is positive, $\tilde{\Lambda}$ maps separable states into positive (separable) operators, which results in another separability condition, i.e., $\tilde{\lambda}_{AB} \geq 0$. As we will see in Sec. III, the operators λ_{AB} and $\tilde{\lambda}_{AB}$ can be shown to have the same spectrum when $d_A = d_B = 2$, in which case they result in the same separability condition. However, this property does not hold in larger dimensions, i.e., λ_{AB} and $\tilde{\lambda}_{AB}$ do not have the same spectrum in general (see Appendix A).

We can also construct another linear map by cascading Λ and $\tilde{\Lambda}$ (the order is irrelevant), which results in the *symmetric* map $M = \tilde{\Lambda}\Lambda = \Gamma \otimes \Gamma$ defined in Eq. (18). Any separable ρ_{AB} is mapped by M into a separable operator $\mu_{AB} \geq 0$, as expected. The symmetric map also commutes with a $U_A \otimes U_B$ isomorphism

$$\begin{aligned} M[(U_A \otimes U_B)\rho_{AB}(U_A^\dagger \otimes U_B^\dagger)] \\ = (U_A \otimes U_B)(M\rho_{AB})(U_A^\dagger \otimes U_B^\dagger) \end{aligned} \quad (19)$$

so that the spectrum of $\mu_{AB} = M\rho_{AB}$ is invariant under local transformations on ρ_{AB} . It is also reversible, its inverse map $M^{-1} = \Gamma^{-1} \otimes \Gamma^{-1}$ being given by

$$\begin{aligned} M^{-1}: \mu_{AB} \rightarrow \mathbb{I}_A \otimes \mathbb{I}_B - (d_B - 1)^{-1}(\mu_A \otimes \mathbb{I}_B) \\ - (d_A - 1)^{-1}(\mathbb{I}_A \otimes \mu_B) + \mu_{AB} = \rho_{AB}, \end{aligned} \quad (20)$$

where $\mu_A = \text{Tr}_B[\mu_{AB}] = (d_B - 1)(\mathbb{I}_A - \rho_A)$ and $\mu_B = \text{Tr}_A[\mu_{AB}] = (d_A - 1)(\mathbb{I}_B - \rho_B)$. As expected, this map is trace preserving and self-inverse only in the case where $d_A = d_B = 2$. It corresponds then to a time-reversal operation applied to the *joint* system AB . In this case, M by itself is not useful as far as revealing inseparability is concerned since it is positive, i.e., $M\rho_{AB} \geq 0$. Therefore, all inseparable states of two quantum bits are mapped into positive operators just as are separable states. Still, M plays a role when analyzing the separability of two quantum bits as it is equivalent to the complex conjugation operation in the “magic” basis introduced by Hill and Wootters [9] (see theorem 6). Whether the positivity of M holds in arbitrary dimensions is not known.

Theorem 2. The reduction separability criterion ($\Lambda\rho_{AB} \geq 0$) is *not* a sufficient condition for the separability of ρ_{AB} .

In order to prove that this criterion is not sufficient, we show that it is possible to find an *inseparable* system with $\lambda_{AB} \geq 0$, i.e., such that its inseparability is *not* revealed by Λ . We will construct such an inseparable system by extending an inseparable component with a separable one, “diluting” the inseparability [6]. Consider an inseparable system $A'B'$ with $\lambda_{A'B'} \neq 0$. Let us extend $A'B'$ with a separable system $A''B''$, and apply the reduction criterion to the joint system AB where $A \equiv A'A''$ and $B \equiv B'B''$. Since the joint system is characterized by $\rho_{AB} = \rho_{A'B'} \otimes \rho_{A''B''}$, its associated operator under the map Λ is given by

$$\lambda_{AB} = \Lambda \rho_{AB} = (\mathbb{I}_{A'} \otimes \rho_{B'}) \otimes (\mathbb{I}_{A''} \otimes \rho_{B''}) - \rho_{A'B'} \otimes \rho_{A''B''}. \quad (21)$$

Using the operators $\lambda_{A'B'} = \Lambda \rho_{A'B'} = \mathbb{I}_{A'} \otimes \rho_{B'} - \rho_{A'B'}$ and $\lambda_{A''B''} = \Lambda \rho_{A''B''} = \mathbb{I}_{A''} \otimes \rho_{B''} - \rho_{A''B''}$ corresponding to Λ applied to each component system, we obtain

$$\lambda_{AB} = \lambda_{A'B'} \otimes \lambda_{A''B''} + \lambda_{A'B'} \otimes \rho_{A''B''} + \rho_{A'B'} \otimes \lambda_{A''B''} \quad (22)$$

with $\lambda_{A'B'} \neq 0$ and $\lambda_{A''B''} \geq 0$ (since $A''B''$ is separable). The *dilution* of entanglement comes from the fact that the third term on the right-hand side of Eq. (22) is ≥ 0 . As a consequence, Eq. (22) *cannot* guarantee that $\lambda_{AB} \neq 0$ even though the composite system AB contains an inseparable component as $\lambda_{A'B'} \neq 0$ [i.e., even though the sum of the first two terms on the right-hand side of Eq. (22) is $\neq 0$]. ■

Note that, even when both components are inseparable with $\lambda_{A'B'}, \lambda_{A''B''} \neq 0$, then $\lambda_{AB} \neq 0$ is not necessarily true, so that the inseparability of the joint system AB is not always revealed by Λ . This property contrasts with the situation prevailing when using the conditional amplitude matrix if the conditional amplitude operator of each component admits an eigenvalue > 1 , then so does the corresponding operator for the whole system [6]. Conversely, Eq. (22) implies that if both components have $\lambda_{A'B'} \geq 0$ and $\lambda_{A''B''} \geq 0$, then $\lambda_{AB} \geq 0$.

It is not difficult to find examples of such inseparable states AB whose inseparability is masked (i.e., $\lambda_{AB} \geq 0$) by extending an inseparable component $A'B'$ that satisfies $\lambda_{A'B'} \neq 0$ with a separable one $A''B''$. For example, let $A'B'$ be one of the Bell states, e.g., $\rho_{A'B'} = |\Phi^+\rangle\langle\Phi^+|$ with $|\Phi^+\rangle = 2^{-1/2}(|00\rangle + |11\rangle)$, and let $A''B''$ be a product of two random quantum bits, i.e., $\rho_{A''B''} = (\mathbb{I}_{A''} \otimes \mathbb{I}_{B''})/4$. Since $\rho_{B'} = \mathbb{I}_{B'}/2$, we have $\lambda_{A'B'} = \mathbb{I}_{A'B'}/2 - \rho_{A'B'} \neq 0$, as expected. Using $\lambda_{A''B''} = \rho_{A''B''}$, we see that Eq. (22) yields

$$\lambda_{AB} = (\mathbb{I}_{A'B'} - \rho_{A'B'}) \otimes \rho_{A''B''}, \quad (23)$$

which is obviously a non-negative operator, so that the inseparability of AB is hidden. The example of weakly inseparable states with a positive partial transpose (see Ref. [4]) is treated in Appendix A, to illustrate that $\lambda_{AB} \geq 0$ is not a sufficient condition in general.

Remark 1. The mechanism of dilution of inseparability can be understood by examining the action of the map Γ on product states. Indeed, when applying $\Lambda = \Gamma \otimes I$ on the state $\rho_{AB} = \rho_{A'B'} \otimes \rho_{A''B''}$, Γ acts on the state $\rho_{A'} \otimes \rho_{A''}$ (B and B' are left unchanged by I). Let us consider a density operator of the product form $\rho = \rho' \otimes \rho''$. Since we have $\text{Tr}(\rho) = \text{Tr}(\rho')\text{Tr}(\rho'')$, we see that it is mapped to

$$\begin{aligned} \Gamma(\rho' \otimes \rho'') &= \text{Tr}(\rho')\text{Tr}(\rho'') - \rho' \otimes \rho'' \\ &= [\text{Tr}(\rho') - \rho'] \otimes [\text{Tr}(\rho'') - \rho''] \\ &\quad + \text{Tr}(\rho') \otimes \rho'' + \rho' \otimes \text{Tr}(\rho'') - 2\rho' \otimes \rho'' \\ &= \Gamma\rho' \otimes \Gamma\rho'' + \Gamma\rho' \otimes \rho'' + \rho' \otimes \Gamma\rho'', \end{aligned} \quad (24)$$

which implies the relation

$$\Gamma = \Gamma' \otimes \Gamma'' + \Gamma' \otimes I'' + I' \otimes \Gamma'', \quad (25)$$

where Γ' (or Γ'') stands for the same map but acting on the subspace of ρ' (or ρ'') while Γ acts on the joint space. Using the same notation for Λ (i.e., Λ' acts on the subspace of $A'B'$ while Λ'' acts on the subspace of $A''B''$), the latter equation gives

$$\Lambda = \Gamma \otimes I = \Lambda' \otimes \Lambda'' + \Lambda' \otimes I'' + I' \otimes \Lambda'', \quad (26)$$

which implies Eq. (22). The same reasoning can be applied to the dual map $\tilde{\Lambda} = I \otimes \Gamma$ and the symmetric map $M = \Gamma \otimes \Gamma$. Thus, even if the maps Λ' and Λ'' reveal inseparability by themselves, the combined map, Eq. (26), is not guaranteed to do so because the nonpositivity of $(\Lambda' \otimes \Lambda'')\rho = (\Lambda'\rho') \otimes (\Lambda''\rho'')$ can be masked by one of the last two terms (the one where Λ is applied to the separable component).

Remark 2. It is worth noting that the separability criterion based on the partial transposition [2] does *not* suffer from this dilution of inseparability (even though it is not a sufficient condition in general). Consider, as before, a system AB characterized by $\rho_{AB} = \rho_{A'B'} \otimes \rho_{A''B''}$, where the *inseparable* component $A'B'$ is detected by partial transposition, i.e., $(\rho_{A'B'})^{T_A} \neq 0$. Since $(\rho_{AB})^{T_A} = (\rho_{A'B'})^{T_A} \otimes (\rho_{A''B''})^{T_A}$, we have $\text{Tr}_{A''B''}[(\rho_{AB})^{T_A}] = (\rho_{A'B'})^{T_A} \neq 0$. Since the partial trace of a non-negative operator is a non-negative operator, this implies that $(\rho_{AB})^{T_A} \neq 0$, so that the inseparability of the extended system AB is detected provided that the inseparability of a component of it (here $A'B'$) is detected.

III. SEPARABILITY OF TWO TWO-DIMENSIONAL SYSTEMS

Theorem 3. The map Γ acting on a two-dimensional system corresponds to time reversal, and is therefore equivalent to applying the complex conjugation operator K followed by a rotation \mathcal{R}_y by an angle π about the y axis, that is, $\Gamma = \mathcal{R}_y K$.

Let us write the arbitrary state of a two-dimensional quantum system (a quantum bit) in the Bloch-sphere picture:

$$\rho = \frac{1}{2}(1 + \vec{r} \cdot \vec{\sigma}), \quad (27)$$

where $\vec{\sigma}$ represent the three Pauli matrices and $\vec{r} = \text{Tr}(\rho \vec{\sigma})$ is a *real* vector in the Bloch sphere (of radius 1). The vector \vec{r} describes the statistics of measurements on the system, as, for example, the quantum expectation value of the spin component along an axis defined by the vector \vec{v} is $\text{Tr}[\rho(\vec{v} \cdot \vec{\sigma})] = (\vec{v}, \vec{r})$. Using Eq. (27), it is straightforward to check that

$$\Gamma\rho = 1 - \rho = \frac{1}{2}(1 - \vec{r} \cdot \vec{\sigma}). \quad (28)$$

Thus, Γ performs a *spin flip*, or, equivalently, performs a *parity* transformation on the Bloch vector $\vec{r} \rightarrow -\vec{r}$. This can be viewed as *time reversal*, and therefore can be decomposed into a complex conjugation K followed by a rotation \mathcal{R}_y of an angle π about the y axis, that is, $\Gamma = \mathcal{T} = \mathcal{R}_y K$ [11]. ■

Remark 1. In order to see this explicitly, consider the action of the map $\Lambda=\Gamma\otimes I$ on a product state $|\psi\rangle=|a\rangle\otimes|b\rangle$. Using $\rho_{AB}=P_a\otimes P_b$ with $P_a=|a\rangle\langle a|$ and $P_b=|b\rangle\langle b|$, we have

$$\lambda_{AB}=P_a^\perp\otimes P_b, \quad (29)$$

where $P_a^\perp=\Gamma(|a\rangle\langle a|)=\mathbb{I}_A-|a\rangle\langle a|$ is the projector on the subspace orthogonal to $|a\rangle$. In the case where $d_A=2$, P_a^\perp is a rank-one projector as the total trace is preserved. Then, $P_a^\perp=|a^\perp\rangle\langle a^\perp|$, where $|a^\perp\rangle$ is a state vector orthogonal to $|a\rangle$. (Note that it is impossible to construct a state $|a^\perp\rangle$ that is orthogonal to an *arbitrary* state $|a\rangle$ by applying a *unitary* transformation alone.) It is easy to check that $|a^\perp\rangle$ can be obtained by applying a complex conjugation K on the components of $|a\rangle$ followed by a rotation \mathcal{R}_y of angle π about the y axis. Indeed, any state $|a\rangle=\alpha|0\rangle+\beta|1\rangle$ (with $|\alpha|^2+|\beta|^2=1$) is transformed into $|a^\perp\rangle=-\beta^*|0\rangle+\alpha^*|1\rangle$ by applying the rotation

$$U_y=\exp(-i\pi\sigma_y/2)=-i\sigma_y=\sigma_x\sigma_z=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad (30)$$

(that is, a bit and phase flip) to the state vector $\alpha^*|0\rangle+\beta^*|1\rangle$. The transformed state $|a^\perp\rangle$ is such that $\langle a^\perp|a\rangle=0$ and $|a^\perp\rangle\langle a^\perp|=\mathbb{I}_A-|a\rangle\langle a|$, as expected. Thus, Γ coincides with time reversal for a spin-1/2 system ($d_A=2$) as the latter is equal to complex conjugation K followed by the rotation \mathcal{R}_y , i.e., $T=\mathcal{R}_yK$ [11]. Consequently, Γ is an *anti-unitary* operation on state vectors in a two-dimensional Hilbert space (see Appendix B). (For any two state vectors $|a\rangle$ and $|\tilde{a}\rangle$, we have $\langle\tilde{a}^\perp|a^\perp\rangle=\langle\tilde{a}|a\rangle^*$.)

Corollary. For the Hilbert-Schmidt decomposition of ρ_{AB} , the map $\Lambda=\Gamma\otimes I$ corresponds to a sign flip of the Pauli matrices acting on A while leaving those acting on B unchanged.

Let us consider the Hilbert-Schmidt decomposition of an arbitrary state of two quantum bits (or spin-1/2 particles) [12]:

$$\rho_{AB}=\frac{1}{4}\left(\mathbb{I}_A\otimes\mathbb{I}_B+\vec{r}\cdot\vec{\sigma}_A\otimes\mathbb{I}_B+\mathbb{I}_A\otimes\vec{s}\cdot\vec{\sigma}_B+\sum_{m,n=1}^3t_{n,m}\sigma_A^{(n)}\otimes\sigma_B^{(m)}\right), \quad (31)$$

where $\sigma_A^{(n)}$ and $\sigma_B^{(m)}$ stand for the Pauli matrices (with $n=1,2,3$) in the A and B space, respectively. Equation (31) depends on 15 real parameters, the two three-dimensional vectors \vec{r} and \vec{s} , and the 3×3 real matrix $t_{n,m}$. The vectors \vec{r} and \vec{s} correspond to the reduced state of A and B in the Bloch sphere since we have

$$\rho_A=\text{Tr}_B[\rho_{AB}]=\frac{1}{2}(\mathbb{I}_A+\vec{r}\cdot\vec{\sigma}_A), \quad (32)$$

$$\rho_B=\text{Tr}_A[\rho_{AB}]=\frac{1}{2}(\mathbb{I}_B+\vec{s}\cdot\vec{\sigma}_B). \quad (33)$$

They characterize the reduced systems A and B , that is, the local (marginal) statistics of any observable on A or B . The matrix $t_{n,m}=\text{Tr}[\rho_{AB}(\sigma_A^{(n)}\otimes\sigma_B^{(m)})]$ describes the joint statistics of A and B as it characterizes the correlation between the measured spin components along two axes (defined by the vectors \vec{a} and \vec{b}): $\text{Tr}[\rho(\vec{a}\cdot\vec{\sigma}_A\otimes\vec{b}\cdot\vec{\sigma}_B)]=(\vec{a},\vec{b})$. Using Eqs. (31) and (33), it is checked by straightforward calculation that Λ simply flips the sign of the terms in $\vec{\sigma}_A$:

$$\lambda_{AB}=\frac{1}{4}\left(\mathbb{I}_A\otimes\mathbb{I}_B-\vec{r}\cdot\vec{\sigma}_A\otimes\mathbb{I}_B+\mathbb{I}_A\otimes\vec{s}\cdot\vec{\sigma}_B-\sum_{m,n=1}^3t_{n,m}\sigma_A^{(n)}\otimes\sigma_B^{(m)}\right). \quad (34)$$

This implies that $\Lambda=\Gamma\otimes I$ applied to a $2\times n$ system corresponds simply to “local” time reversal $T\otimes I$, that is, performing time reversal on the subsystem A while leaving the subsystem B unchanged [8].

Remark 2. The dual map $\tilde{\Lambda}=I\otimes\Gamma$ flips the sign of the Pauli matrices acting on B while leaving the sign of those acting on A unchanged. The action of the symmetric map $M=\Gamma\otimes\Gamma$ on the Hilbert-Schmidt decomposition of ρ_{AB} is to flip the sign of the Pauli matrices $\vec{\sigma}_A$ and $\vec{\sigma}_B$. This operation corresponds therefore to time reversal applied to A and B simultaneously, and is equivalent to complex conjugation in the “magic” basis (see theorem 6). It is worth noting that the set of states that remain invariant under the symmetric map M are those with $\vec{r}=\vec{s}=0$, that is, mixtures of generalized Bell states (the latter being defined as the states obtained by applying any local transformation to the four Bell states). These states are called “ T states” by Horodecki *et al.* [12], and are such that the entropy of A and B is maximal, that is $S(\rho_A)=S(\rho_B)=1$. (The only pure states in this set are the fully entangled states of two qubits, i.e., the generalized Bell states.) Thus, in particular, the (generalized) Bell states are left unchanged by the action of M . In contrast, a (separable) product state $\rho_A\otimes\rho_B$ is mapped into the distinct (non-negative) state $\mu_{AB}=(\mathbb{I}_A-\rho_A)\otimes(\mathbb{I}_B-\rho_B)$. Because of this property, μ_{AB} by itself is uninteresting as far as revealing inseparability is concerned, as mentioned earlier.

Theorem 4. A bipartite system of two-dimensional components A and B characterized by an arbitrary joint density operator ρ_{AB} is separable if and only if the operator $\lambda_{AB}=\Lambda\rho_{AB}$ is positive semidefinite.

It is enough to show that Λ is equivalent to a partial transposition up to a completely positive map (in fact, a unitary transformation), since Peres’ separability criterion is known to be *necessary* and *sufficient* in this case [3]. Since we are dealing with Hermitian operators, the map $T\otimes I$, where T is the standard transposition of operators on \mathcal{H}_A , is equivalent to the “partial conjugation” operation $K\otimes I$, where K is the complex conjugation operator acting on states on \mathcal{H}_A . (Note that, although K is well defined, partial conjugation $K\otimes I$ is *only* defined for product state vectors in \mathcal{H}_{AB} [4].) Thus, theorem 3 reads $\Gamma=\mathcal{R}_yT$. We can now use the fact that any positive map Π acting on density operators in a two-dimensional Hilbert space can be written as [3]

$$\Pi = \Pi_1^{\text{CP}} + \Pi_2^{\text{CP}} T, \quad (35)$$

where Π_1^{CP} and Π_2^{CP} are completely positive maps (which therefore do not reveal inseparability). With the identification $\Pi_1^{\text{CP}}=0$ and $\Pi_2^{\text{CP}}=\mathcal{R}_y$, we see that the map Γ can be used rather than the transposition operator T (or K) in order to test the positivity of the operator resulting from applying *any* element of the set of maps $\Pi \otimes I$ on ρ_{AB} (this follows from the reasoning used in Ref. [3]). Thus, using the fact that the complex conjugation operator K is *unitarily* equivalent to Γ , we have shown that $\Lambda \rho_{AB} \geq 0$ results in a necessary *and* sufficient condition for the separability of 2×2 systems. ■

Remark 1. The map Γ applied to a two-dimensional system is unitarily equivalent to the transposition operator T . Since the spectrum of an operator is conserved by a unitary transformation (\mathcal{R}_y), the spectrum of the operator obtained by partial transposition in subspace A , $(T \otimes I)\rho_{AB} = \rho_{AB}^{T_A}$, is the same as the spectrum of $\lambda_{AB} = \Lambda \rho_{AB}$. Therefore, testing Peres' separability condition or the positivity of λ_{AB} is operationally equivalent, and these conditions can be used interchangeably in the case of two quantum bits, as illustrated in Appendix A. Moreover, λ_{AB} and $\rho_{AB}^{T_A}$ have the same spectrum for $2 \times n$ systems, so that the conditions are also equivalent if Γ is applied on the two-dimensional subsystem. As a consequence, the separability condition based on Λ is necessary *and* sufficient for 2×3 systems, while it is only necessary for $2 \times n$ systems with larger n , just as Peres' condition [3]. Numerical evidence suggests that, for systems with $d_A, d_B \geq 2$, the reduction condition is weaker than (or equivalent to) the one based on partial transposition (this has been later proven in Ref. [7]).

Remark 2. It is instructive to illustrate theorem 4 for T states [12], that is, in the case where A and B have a maximal reduced entropy. The T states ($\vec{r} = \vec{s} = 0$) are such that the reduced density operators are given by $\rho_A = \rho_B = \mathbb{I}/2$, so that the reduced entropies are $S(\rho_A) = S(\rho_B) = 1$. These states are thus completely characterized by the matrix $t_{n,m}$. It has been shown in Ref. [12] that any T state can be transformed by a unitary transformation of the product form $U_A \otimes U_B$ into a state for which $t_{n,m}$ is *diagonal*. As far as separability is concerned, we can thus restrict ourselves to the class of all states with diagonal t , since these are representative of the entire set of T states (up to a $U_A \otimes U_B$ isomorphism).

The class of states with diagonal t is a convex subset of the set of T states, and any state belonging to this subset can be characterized by the real vector $\vec{t} = (t_{11}, t_{22}, t_{33})$ made out of the diagonal elements of t . It was proven in Ref. [12] that an operator ρ_{AB} of the form given by Eq. (31) with $\vec{r} = \vec{s} = 0$ and diagonal t corresponds to a state (i.e., a *positive* unit-trace operator) if and only if the vector \vec{t} belongs to a tetrahedron with vertices $\vec{t}_1 = (-1, 1, 1)$, $\vec{t}_2 = (1, -1, 1)$, $\vec{t}_3 = (1, 1, -1)$, and $\vec{t}_4 = (-1, -1, -1)$. In other words, any state of this class can be represented by a point inside this tetrahedron. In this representation, the four Bell states $|\Phi^\pm\rangle = 2^{-1/2}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = 2^{-1/2}(|01\rangle \pm |10\rangle)$ correspond to the vertices of the tetrahedron, that is,

$$\begin{aligned} \vec{t}_1: \quad |\Phi^-\rangle\langle\Phi^-| &= \frac{1}{4}(\mathbb{I}_A \otimes \mathbb{I}_B - \sigma_A^{(x)} \otimes \sigma_B^{(x)} \\ &\quad + \sigma_A^{(y)} \otimes \sigma_B^{(y)} + \sigma_A^{(z)} \otimes \sigma_B^{(z)}), \\ \vec{t}_2: \quad |\Phi^+\rangle\langle\Phi^+| &= \frac{1}{4}(\mathbb{I}_A \otimes \mathbb{I}_B + \sigma_A^{(x)} \otimes \sigma_B^{(x)} \\ &\quad - \sigma_A^{(y)} \otimes \sigma_B^{(y)} + \sigma_A^{(z)} \otimes \sigma_B^{(z)}), \\ \vec{t}_3: \quad |\Psi^+\rangle\langle\Psi^+| &= \frac{1}{4}(\mathbb{I}_A \otimes \mathbb{I}_B + \sigma_A^{(x)} \otimes \sigma_B^{(x)} \\ &\quad + \sigma_A^{(y)} \otimes \sigma_B^{(y)} - \sigma_A^{(z)} \otimes \sigma_B^{(z)}), \\ \vec{t}_4: \quad |\Psi^-\rangle\langle\Psi^-| &= \frac{1}{4}(\mathbb{I}_A \otimes \mathbb{I}_B - \sigma_A^{(x)} \otimes \sigma_B^{(x)} \\ &\quad - \sigma_A^{(y)} \otimes \sigma_B^{(y)} - \sigma_A^{(z)} \otimes \sigma_B^{(z)}). \end{aligned} \quad (36)$$

In Ref. [12], it is also shown that a state ρ_{AB} of this T -diagonal class is *separable* if and only if the vector \vec{t} characterizing ρ_{AB} belongs to an octahedron with vertices $\vec{o}_1^\pm = (\pm 1, 0, 0)$, $\vec{o}_2^\pm = (0, \pm 1, 0)$, and $\vec{o}_3^\pm = (0, 0, \pm 1)$. Let us consider the action of Λ in this representation. As shown earlier, Λ flips the “spin” $\vec{\sigma}_A$. Within the set of T states, this amounts to changing the sign of the $t_{n,m}$ matrix, that is, to flipping the sign of the vector \vec{t} for T -diagonal states. Therefore, the criterion for separability $\lambda_{AB} = \Lambda \rho_{AB} \geq 0$ translates, in this representation, to the condition that the “parity” operation on the vector \vec{t} characterizing a separable state results in a positive operator (i.e., a legitimate state). Hence, $-\vec{t}$ must belong to the tetrahedron. It is easy to see that the set of points of the tetrahedron which are such that their image under parity still belongs to the tetrahedron corresponds exactly to the octahedron defined above. Therefore, no inseparable state exists that satisfies $\Lambda \rho_{AB} \geq 0$, so that Λ provides a necessary *and* sufficient condition for separability within the class of T states, as expected.

Theorem 5. The symmetric map M acting on two two-dimensional systems conserves the spectrum, so that the separability criteria resulting from the map Λ and its dual $\tilde{\Lambda}$ are equivalent. ■

As a consequence of theorem 3, $M = \Gamma \otimes \Gamma$ amounts to performing a complex conjugation K (or transposition) of the joint density operator in \mathcal{H}_{AB} , followed by a tensor product of the rotation \mathcal{R}_y defined by $U_y = \exp(-i\pi\sigma_y/2) = -i\sigma_y$, that is, $U_y \otimes U_y = -\sigma_y \otimes \sigma_y$. Note that, as we are dealing with Hermitian (density) operators, their spectrum is unchanged by K . The same is true for the rotation $U_y \otimes U_y$. Therefore, $\mu_{AB} = M \rho_{AB}$ has the same spectrum as ρ_{AB} when $d_A = d_B = 2$. As Γ is self-inverse ($\Gamma^2 = I$) when $d_A = d_B = 2$, we have the relation $I \otimes \Gamma = (\Gamma \otimes I)(\Gamma \otimes \Gamma)$ or in short $\tilde{\Lambda} = \Lambda M$. This implies that

$$\tilde{\Lambda} \rho_{AB} = \Lambda [(U_y \otimes U_y) \rho_{AB}^* (U_y^\dagger \otimes U_y^\dagger)], \quad (37)$$

which in turn results in

$$\tilde{\lambda}_{AB} = (U_y \otimes U_y) \lambda_{AB}^* (U_y^\dagger \otimes U_y^\dagger) \quad (38)$$

as Λ commutes with $U_y \otimes U_y$ and complex conjugation. Since λ_{AB} is Hermitian (just as ρ_{AB}), the latter expression shows that the spectrum of $\tilde{\lambda}_{AB}$ and λ_{AB} are identical, so that the resulting criteria for separability are equivalent.

Theorem 6. The symmetric map M applied to a bipartite system of two-dimensional components (i.e., global time reversal) is equivalent to complex conjugation in the “magic” basis introduced in Ref. [10] (this was pointed out independently in Ref. [13], which was brought to our attention after completion of this work).

Since $\Gamma = \mathcal{R}_y K$, the symmetric map $M = \Gamma \otimes \Gamma$ applied to the state ρ_{AB} of a bipartite system results in

$$M\rho_{AB} = (U_y \otimes U_y) \rho_{AB}^* (U_y^\dagger \otimes U_y^\dagger), \quad (39)$$

where $U_y \otimes U_y = -\sigma_y \otimes \sigma_y$. Since M is antiunitary and self-inverse ($M^2 = I$), it is a *conjugation* [14]. It can be written as the complex conjugation operator if expressed in a specific basis. Let us assume that V is the unitary operator (in the joint space) that transforms the product states into the states $\{|e_i\rangle\}$ that form this specific basis, that is,

$$\begin{aligned} |e_1\rangle &= V|00\rangle, & |e_2\rangle &= V|01\rangle, \\ |e_3\rangle &= V|10\rangle, & |e_4\rangle &= V|11\rangle. \end{aligned} \quad (40)$$

We would like to show that M is equivalent to rotating the states $|e_i\rangle$ into the product states, taking the complex conjugation of the density matrix (in the product basis), and then rotating the product states back to the $|e_i\rangle$'s:

$$M\rho_{AB} = V(V^\dagger \rho_{AB} V)^* V^\dagger = (VV^T) \rho_{AB}^* (VV^T)^\dagger, \quad (41)$$

where V^T is the transpose of the unitary matrix V . Identifying Eqs. (39) and (41), we obtain

$$VV^T = U_y \otimes U_y = -\sigma_y \otimes \sigma_y = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \quad (42)$$

It is easy to prove that, if V is unitary, then VV^T is unitary and symmetric (but not necessarily Hermitian). In order to find a solution for V that satisfies Eq. (42), we first diagonalize the matrix $\sigma_y \otimes \sigma_y$. Consider the unitary matrix

$$\begin{aligned} W &\equiv \exp\left(-\frac{i\pi}{4}(1-\sigma_x) \otimes (1-\sigma_x)\right) \\ &= (1 \otimes 1 + 1 \otimes \sigma_x + \sigma_x \otimes 1 - \sigma_x \otimes \sigma_x)/2. \end{aligned} \quad (43)$$

It is in fact a *real* orthogonal matrix, so that $W^{-1} = W^\dagger = W^T$. It can easily be shown that W diagonalizes $\sigma_y \otimes \sigma_y$, that is,

$$W(\sigma_y \otimes \sigma_y)W^T = \sigma_z \otimes \sigma_z. \quad (44)$$

It is not the only such matrix, as $\sigma_y \otimes \sigma_y$ is obviously also diagonalized by $\exp[-i(\pi/4)\sigma_x] \otimes \exp[-i(\pi/4)\sigma_x]$. How-

ever, we are looking here for a (real) rotation matrix rather than a general unitary matrix. Note that the matrix W is self-inverse, i.e., $W^2 = 1$, so that it is also symmetric ($W^T = W$). By multiplying Eq. (42) by W on the left and the right, we obtain

$$WV(WV)^T = -\sigma_z \otimes \sigma_z = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad (45)$$

which implies that the product WV can be written as a diagonal matrix D :

$$WV = D \equiv \begin{pmatrix} \pm i & 0 & 0 & 0 \\ 0 & \pm 1 & 0 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 0 & 0 & 0 & \pm i \end{pmatrix}. \quad (46)$$

This yields a (nonunique) solution for the unitary matrix $V = W^T D = WD$ that defines the basis $\{|e_i\rangle\}$. The states $|e_i\rangle$ are thus obtained by applying the rotation matrix W to the product states $\pm i|00\rangle$, $\pm|01\rangle$, $\pm|10\rangle$, and $\pm i|11\rangle$. It is worth noticing at this point that the rotation matrix

$$W = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix} \quad (47)$$

transforms the product states into the four maximally entangled states which are obtained by applying a local transformation $H \otimes 1$ on the four Bell states, i.e.,

$$\begin{aligned} |00\rangle &= (H \otimes 1)|\Phi^+\rangle = (|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2, \\ |01\rangle &= (H \otimes 1)|\Psi^+\rangle = (|00\rangle + |01\rangle - |10\rangle + |11\rangle)/2, \\ |10\rangle &= (H \otimes 1)|\Phi^-\rangle = (|00\rangle - |01\rangle + |10\rangle + |11\rangle)/2, \\ |11\rangle &= (H \otimes 1)|\Psi^-\rangle = (-|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2, \end{aligned} \quad (48)$$

where H is the Hadamard transform. (As a matter of fact, the unitary transformation W corresponds simply to a controlled-NOT gate where the control is in the dual basis $\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$ rather than the standard basis.) Therefore, the unitary transformation $V = WD$ is such that the product states are rotated into the four generalized Bell states with the appropriate phases

$$\begin{aligned} |e_1\rangle &= V|00\rangle = \pm i(H \otimes 1)|\Phi^+\rangle, \\ |e_2\rangle &= V|01\rangle = \pm 1(H \otimes 1)|\Psi^+\rangle, \\ |e_3\rangle &= V|10\rangle = \pm 1(H \otimes 1)|\Phi^-\rangle, \\ |e_4\rangle &= V|11\rangle = \pm i(H \otimes 1)|\Psi^-\rangle. \end{aligned} \quad (49)$$

These states $|e_i\rangle$ are therefore equivalent, up to a local change of basis $H \otimes 1$ and a phase i that are irrelevant here,

to the “magic” states introduced in Ref. [10]. (Any four states obtained from the $|e_i\rangle$ ’s up to an overall phase and a unitary transformation acting locally on each quantum bit are legitimate “magic” states.) This implies that, when expressed in this basis, the symmetric map $M=\Gamma\otimes\Gamma$ reduces the complex conjugation operation that was used in the context of the calculation of the entropy of formation of a pair of quantum bits (see Refs. [9,13]). ■

Theorem 7. A distinct necessary separability condition for the bipartite state ρ_{AB} is that its support can be spanned by a set of product states which are such that the corresponding product operators obtained by applying Γ to the state vector in \mathcal{H}_A span the support of $\lambda_{AB}=\Lambda\rho_{AB}$.

We only consider this condition in the case where $d_A=2$. Let us first show that if ρ_{AB} is a separable state, then λ_{AB} is a separable operator obtained by replacing the states $|a\rangle$ in \mathcal{H}_A by projectors P_a^\perp orthogonal to them. Consider the separable state

$$\rho_{AB}=\sum_i w_i(|a_i\rangle\langle a_i|\otimes|b_i\rangle\langle b_i|), \quad (50)$$

where the $|a_i\rangle\otimes|b_i\rangle$ are pure product states [using the spectral decomposition of $\rho_A^{(i)}$ and $\rho_B^{(i)}$, it is easy to rewrite Eq. (7) into this form]. As a result of theorem 3, we see that ρ_{AB} it is mapped by Λ into the separable operator

$$\lambda_{AB}=\sum_i w_i(P_{a_i}^\perp\otimes|b_i\rangle\langle b_i|). \quad (51)$$

The operator λ_{AB} is a unit-trace operator in the case $d_A=2$ since each component pure state $|a\rangle\otimes|b\rangle$ is mapped into a *pure* product state, $|a^\perp\rangle\otimes|b\rangle$, in which case it simply reads

$$\lambda_{AB}=\sum_i w_i(|a_i^\perp\rangle\langle a_i^\perp|\otimes|b_i\rangle\langle b_i|). \quad (52)$$

Let us show that Eq. (52) results in a simple *necessary* condition for separability (distinct from $\lambda_{AB}\geq 0$), inspired from the condition recently proposed by Horodecki [4]. The central point is to note that if ρ_{AB} is separable, then the ensemble of product states $|a_i\rangle\otimes|b_i\rangle$ span the entire support of ρ_{AB} . (Conversely, any state $|a_i\rangle\otimes|b_i\rangle$ must belong to the support of ρ_{AB} and cannot have a nonvanishing component orthogonal to it.) From Eq. (52), we see that the ensemble of states $|a_i^\perp\rangle\otimes|b_i\rangle$ span the entire support of the corresponding separable state λ_{AB} obtained by applying Λ on ρ_{AB} . Also, any state $|a_i^\perp\rangle\otimes|b_i\rangle$ cannot be outside the support of λ_{AB} . This results in a *necessary* condition for separability which can be stated as follows: if a state ρ_{AB} is separable, then it must be possible to span its support by a set of product states $|a\rangle|b\rangle$ which are such that their image (i.e., the product states obtained by rotating the complex conjugate of state vector $|a\rangle$ in the A space by an angle π about the y axis while leaving the state vector $|b\rangle$ in the B space unchanged) span the support of the mapped state $\lambda_{AB}=\Lambda\rho_{AB}$. ■

IV. CONCLUSION

Given a bipartite system characterized by a density operator ρ_{AB} , we construct a simple separability criterion based on the positive linear map $\Gamma:\rho\rightarrow(\text{Tr }\rho)-\rho$. Any separable state ρ_{AB} is mapped by the tensor product of Γ (acting on A) and the identity I (acting on B) into a positive operator. Therefore, a necessary condition for separability is based on checking the non-negativity of the operator $(\Gamma\otimes I)\rho_{AB}=I_A\otimes\rho_B-\rho_{AB}$. This reduction condition, along with the one based on the dual map $I\otimes\Gamma$, can be shown to be nonsufficient for a system of arbitrary dimension because entanglement dilution can thwart the map’s sensitivity. Since Γ commutes with any unitary transformation, the spectrum of the operator $(\Gamma\otimes I)\rho_{AB}$ is invariant under a local unitary transformation $U_A\otimes U_B$, making this reduction criterion independent of the basis in which A and B are expressed.

In the case of a two-dimensional system, Γ is shown to be the time-reversal operator, which flips the sign of the spin matrices (or, equivalently, reverses the Bloch vector characterizing the state of the quantum bit), so that the map $\Gamma\otimes I$ amounts to changing the arrow of time for subsystem A with respect to subsystem B . Such a relation between time-reversal and Peres’ partial transposition has been pointed out previously by Sanpera *et al.* [8], who showed that the partial transposition operator is unitarily equivalent to “local” time reversal. Thus, our reduction criterion for separability based on $\Gamma\otimes I$ is equivalent to Peres’ criterion [2] for $2\times n$ systems (when applying Γ on the two-dimensional subsystem). As a consequence, it is necessary *and* sufficient for 2×2 and 2×3 systems while it is only necessary for larger systems, just as is Peres’ [3]. For systems with $d_A, d_B > 2$, however, the reduction condition is generally weaker than the one based on partial transposition.

Finally, we consider the symmetric map $(\Gamma\otimes\Gamma)\rho_{AB}=I_A\otimes I_B-\rho_A\otimes I_B-I_A\otimes\rho_B+\rho_{AB}$. The 2×2 states which are left invariant under this map are mixtures of generalized Bell states, which include the maximally entangled pure states as well as the product of two independent (unentangled) random bits. It can be seen that $\Gamma\otimes\Gamma$ is related to quantum nonlocality even though it does not directly reveal inseparability of two quantum bits. Indeed, it reduces to the complex conjugation in the “magic” basis that has been introduced in the context of the entropy of formation of a pair of quantum bits (see Refs. [9,13]). It might therefore be interesting to look for a simple relation between the map Γ (related to the reduction criterion for inseparability) and the entropy of formation.

ACKNOWLEDGMENTS

We acknowledge useful discussions with Michal Horodecki. We are also grateful to Chris Fuchs for communicating to us unpublished results of Ref. [13], especially the connection between the map M and the “magic” basis for two qubits. This work was supported in part by NSF Grant Nos. PHY 94-12818 and PHY 94-20470, and by a grant from DARPA/ARO through the QUIC Program (No. DAAH04-96-1-3086).

APPENDIX A: EXAMPLES

Here we consider several examples illustrating the separability criterion $\lambda_{AB} \geq 0$, and compare it to Peres' criterion [2]. Examples 1–4 deal with states of two quantum bits, and illustrate the fact that the Λ criterion is necessary and sufficient (the spectrum of λ_{AB} is identical to the spectrum of $\rho_{AB}^{T_A}$). Examples 5 and 6 illustrate that the Λ condition is not sufficient for systems in larger dimensions (3×3 and 2×4) whose partial transpose is positive (cf. Ref. [3]). In fact, the Λ condition is equivalent to Peres' condition for $2 \times n$ systems, so that it is also necessary and sufficient for 2×3 systems [3] while it is only necessary for larger n .

Example 1. Consider a Werner state [1] with parameter x ($0 \leq x \leq 1$), that is, a mixture of a fraction x of the singlet state $|\Psi^-\rangle$ and a random fraction $(1-x)$. We shall see that $\lambda_{AB} \geq 0$ is equivalent to Peres' criterion, and is therefore sufficient. Indeed, the joint density matrix

$$\rho_{AB} = x|\Psi^-\rangle\langle\Psi^-| + \frac{(1-x)}{4}(1\otimes 1)$$

$$= \begin{pmatrix} \frac{1-x}{4} & 0 & 0 & 0 \\ 0 & \frac{1+x}{4} & -\frac{x}{2} & 0 \\ 0 & -\frac{x}{2} & \frac{1+x}{4} & 0 \\ 0 & 0 & 0 & \frac{1-x}{4} \end{pmatrix} \quad (\text{A1})$$

is mapped by Λ into the matrix

$$\lambda_{AB} = \begin{pmatrix} \frac{1+x}{4} & 0 & 0 & 0 \\ 0 & \frac{1-x}{4} & \frac{x}{2} & 0 \\ 0 & \frac{x}{2} & \frac{1-x}{4} & 0 \\ 0 & 0 & 0 & \frac{1+x}{4} \end{pmatrix} \quad (\text{A2})$$

which admits three eigenvalues equal to $(1+x)/4$ and a fourth equal to $(1-3x)/4$. The latter becomes negative if $x > 1/3$, so that λ_{AB} is positive semidefinite only if $x \leq 1/3$, which has been proven to be the *exact* threshold for separability (any Werner state with $x \leq 1/3$ is separable as it can be written as a mixture of product states [15]). As expected, the spectrum of λ_{AB} is equal to the spectrum of the partial transpose of ρ_{AB} , so that the Λ condition is sufficient to ensure separability for Werner states.

Example 2. Consider a mixed state that is made out of a fraction x of the entangled state $|\psi\rangle = a|01\rangle + b|10\rangle$, and fractions $(1-x)/2$ of the separable product states $|00\rangle$ and $|11\rangle$ (see Ref. [16]). The joint density matrix is of the form

$$\rho_{AB} = x|\psi\rangle\langle\psi| + \frac{1-x}{2}|00\rangle\langle 00| + \frac{1-x}{2}|11\rangle\langle 11|$$

$$= \begin{pmatrix} \frac{1-x}{2} & 0 & 0 & 0 \\ 0 & x|a|^2 & xab^* & 0 \\ 0 & xa^*b & x|b|^2 & 0 \\ 0 & 0 & 0 & \frac{1-x}{2} \end{pmatrix} \quad (\text{A3})$$

with a and b satisfying $|a|^2 + |b|^2 = 1$. It is mapped by Λ into the matrix

$$\lambda_{AB} = \begin{pmatrix} x|b|^2 & 0 & 0 & 0 \\ 0 & \frac{1-x}{2} & -xab^* & 0 \\ 0 & -xa^*b & \frac{1-x}{2} & 0 \\ 0 & 0 & 0 & x|a|^2 \end{pmatrix}. \quad (\text{A4})$$

The eigenvalues of λ_{AB} are $x|a|^2$, $x|b|^2$, and $(1-x \pm 2x|ab|)/2$. This implies that ρ_{AB} is inseparable if $x > (1+2|ab|)^{-1}$, exactly as predicted by Peres using the partial transpose of ρ_{AB} . Since we are dealing with two qubits, this is the exact limit between separability and inseparability [2,3].

Example 3. In the simpler case where ρ_{AB} is a mixture of a fraction x of the singlet state $|\Psi^-\rangle$ and a fraction $(1-x)$ of the separable product state $|00\rangle$,

$$\rho_{AB} = x|\psi\rangle\langle\psi| + (1-x)|00\rangle\langle 00|$$

$$= \begin{pmatrix} 1-x & 0 & 0 & 0 \\ 0 & x/2 & -x/2 & 0 \\ 0 & -x/2 & x/2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (\text{A5})$$

we obtain

$$\lambda_{AB} = \begin{pmatrix} x/2 & 0 & 0 & 0 \\ 0 & 0 & x/2 & 0 \\ 0 & x/2 & 1-x & 0 \\ 0 & 0 & 0 & x/2 \end{pmatrix}. \quad (\text{A6})$$

The latter matrix admits two eigenvalues equal to $x/2$ and two eigenvalues equal to $[1-x \pm \sqrt{(1-x)^2 + x^2}]/2$, so that its determinant is equal to $-(x/2)^4$. Thus, this state is inseparable whenever $x > 0$, as expected. (It is separable only if it is the pure product state $|00\rangle$.)

Example 4. Consider the class of two-qubit inseparable states described by Horodecki *et al.* [3], a mixture of two entangled states:

$$\rho_{AB} = p|\psi_1\rangle\langle\psi_1| + (1-p)|\psi_2\rangle\langle\psi_2|, \quad (\text{A7})$$

where $|\psi_1\rangle = a|00\rangle + b|11\rangle$ and $|\psi_2\rangle = a|01\rangle + b|10\rangle$, with $a, b > 0$ and satisfying $|a|^2 + |b|^2 = 1$. The joint density matrix

$$\rho_{AB} = \begin{pmatrix} pa^2 & 0 & 0 & pab \\ 0 & (1-p)a^2 & (1-p)ab & 0 \\ 0 & (1-p)ab & (1-p)b^2 & 0 \\ pab & 0 & 0 & pb^2 \end{pmatrix} \quad (\text{A8})$$

is mapped by Λ to

$$\lambda_{AB} = \begin{pmatrix} (1-p)b^2 & 0 & 0 & -pab \\ 0 & pb^2 & (p-1)ab & 0 \\ 0 & (p-1)ab & pa^2 & 0 \\ -pab & 0 & 0 & (1-p)a^2 \end{pmatrix}. \quad (\text{A9})$$

The latter matrix admits two eigenvalues equal to $[p \pm \sqrt{p^2 + 4a^2b^2(1-2p)}]/2$ and two eigenvalues equal to $[1-p \pm \sqrt{(1-p)^2 + 4a^2b^2(2p-1)}]/2$, so that its determinant is equal to $-a^4b^4(1-2p)^2$. This state is therefore inseparable whenever $ab \neq 0$ and $p \neq 1/2$, in perfect agreement with Ref. [3].

Example 5. Consider the 3×3 system in a weakly inseparable state introduced by Horodecki [4],

$$\rho_{AB} = \frac{1}{1+8a} \begin{pmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{pmatrix}, \quad (\text{A10})$$

where a is a parameter ($a \neq 0, 1$). As shown in Ref. [4], the partial transpose of this state is positive, although ρ_{AB} is inseparable, which makes the inseparability of ρ_{AB} undetectable using Peres' criterion. It is simple to check that the Λ -mapped matrix

$$\lambda_{AB} = \frac{1}{1+8a} \begin{pmatrix} \frac{1+3a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & -a & 0 & 0 & 0 & -a \\ 0 & 2a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+3a}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1+3a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & 0 & 0 \\ -a & 0 & 0 & 0 & 2a & 0 & 0 & 0 & -a \\ 0 & 0 & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+3a}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2a & 0 \\ -a & 0 & 0 & 0 & -a & 0 & 0 & 0 & 2a \end{pmatrix} \quad (\text{A11})$$

is positive (with a trace equal to 2), so that Λ cannot reveal the inseparability of ρ_{AB} either. Accordingly, the determinant of λ_{AB} is equal to $6a^7(1-a)(5a+3)/(1+8a)^9$ and thus positive. Note that the dual map also yields a positive operator $\tilde{\lambda}_{AB}$ (of

trace 2), although the eigenvalues of $\tilde{\lambda}_{AB}$ are distinct from those of λ_{AB} , as is its determinant $\text{Det}(\tilde{\lambda}_{AB})=24a^7(1-a^2)/(1+8a)^9$. This example emphasizes that Λ does not result in a sufficient separability condition for 3×3 systems, just as Peres' condition [3].

Example 6. Following Horodecki [4], we consider a 2×4 system in an inseparable state

$$\rho_{AB} = \frac{1}{1+7b} \begin{pmatrix} b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1+b}{2} & 0 & 0 & \frac{\sqrt{1-b^2}}{2} \\ b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & b & 0 & \frac{\sqrt{1-b^2}}{2} & 0 & 0 & \frac{1+b}{2} \end{pmatrix} \quad (\text{A12})$$

that has a positive partial transpose, where b is a parameter ($b\neq 0, 1$). Applying Λ , we see that

$$\lambda_{AB} = \frac{1}{1+7b} \begin{pmatrix} \frac{1+b}{2} & 0 & 0 & \frac{\sqrt{1-b^2}}{2} & 0 & -b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & -b & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & -b \\ \frac{\sqrt{1-b^2}}{2} & 0 & 0 & \frac{1+b}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & b & 0 & 0 & 0 \\ -b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & -b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & -b & 0 & 0 & 0 & 0 & b \end{pmatrix} \quad (\text{A13})$$

has eigenvalues $0, b, 2b$, and $[1+2b \pm \sqrt{(1+2b)^2 - 2b(3+b)}]/2$ so that it is always non-negative. Note that the spectrum of λ_{AB} is the same as the spectrum of the partial transpose ρ_{AB}^T (cf. Ref. [4]), as expected. This confirms that the condition based on $\Lambda=\Gamma\otimes I$ and Peres' separability condition are equivalent for $2\times n$ systems (when Γ is applied to the two-dimensional system and I to the n -dimensional one). In this example, applying the dual map $\tilde{\Lambda}=I\otimes\Gamma$ yields a positive operator which traces to 3.

APPENDIX B: THE ANTIUNITARY MAP Γ

Consider the action of the map $\Gamma:\rho\rightarrow(\text{Tr }\rho)-\rho$ on the density operator ρ characterizing a two-dimensional system (i.e., a quantum bit). Since ρ can be written as a linear combination of the unit matrix and the three Pauli matrices $\vec{\sigma}$ with *real* coefficients, it is sufficient to consider the action of Γ on these (Hermitian) basis matrices. We find that Γ is an *antiunitary* operator that leaves the unit matrix unchanged

and flips the sign of the Pauli matrices $\sigma_{x,y,z}$,

$$\overset{\Gamma}{\text{l}\rightarrow\text{l}}, \quad \overset{\Gamma}{\sigma_x\rightarrow-\sigma_x}, \quad \overset{\Gamma}{\sigma_y\rightarrow-\sigma_y}, \quad \overset{\Gamma}{\sigma_z\rightarrow-\sigma_z}. \quad (\text{B1})$$

The complex conjugation operator K (or equivalently the transposition, as we deal with Hermitian operators) corresponds to an *antiunitary* operator which acts on the four basis matrices as

$$\overset{K}{\text{l}\rightarrow\text{l}}, \quad \overset{K}{\sigma_x\rightarrow\sigma_x}, \quad \overset{K}{\sigma_y\rightarrow-\sigma_y}, \quad \overset{K}{\sigma_z\rightarrow\sigma_z}. \quad (\text{B2})$$

(Remember that it is enough to consider the action of K on the basis matrices as the coefficients are real.) Also, \mathcal{R}_y is a rotation characterized by the unitary matrix $U_y=\exp(-i\pi\sigma_y/2)=-i\sigma_y=\sigma_x\sigma_z$ which maps ρ into $U_y\rho U_y^\dagger=\sigma_y\rho\sigma_y$, so that the basis matrices are transformed according to

$$\begin{array}{cccc} \mathcal{R}_y & \mathcal{R}_y & \mathcal{R}_y & \mathcal{R}_y \\ \mathbb{I} \rightarrow \mathbb{I}, & \sigma_x \rightarrow -\sigma_x, & \sigma_y \rightarrow \sigma_y, & \sigma_z \rightarrow -\sigma_z. \end{array} \quad (\text{B3})$$

It is straightforward to check, using Eqs. (B1), (B2), and (B3), that Γ is the product of K and \mathcal{R}_y . (It is a general property of an antiunitary transformation that it can be written as the product of a unitary transformation and a fixed antiunitary operator such as time reversal.) This can also be verified easily by applying $\mathcal{R}_y K$ to a system in a state given by Eq. (27). We get

$$\begin{aligned} U_y \rho^* U_y^\dagger &= \sigma_y \rho^* \sigma_y \\ &= \frac{1}{2} [1 + \sigma_y (\vec{r} \cdot \vec{\sigma}^*) \sigma_y] \\ &= \frac{1}{2} (1 - \vec{r} \cdot \vec{\sigma}) = \Gamma \rho, \end{aligned} \quad (\text{B4})$$

where we have used the fact that \vec{r} is a *real* vector and that $\sigma_y \vec{\sigma} \sigma_y = -\vec{\sigma}^*$. This generalizes what was shown in Sec. III for pure states, namely that if $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|a^\perp\rangle = U_y(\alpha^*|0\rangle + \beta^*|1\rangle) = -\beta^*|0\rangle + \alpha^*|1\rangle$, then we have

$$|a^\perp\rangle \langle a^\perp| = \Gamma(|a\rangle \langle a|). \quad (\text{B5})$$

-
- [1] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
 - [2] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
 - [3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
 - [4] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
 - [5] N. J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997).
 - [6] N. J. Cerf and C. Adami, Phys. Rev. A **60**, 893 (1999).
 - [7] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
 - [8] A. Sanpera, R. Tarrach, and G. Vidal, Report No. quant-ph/9707041 (unpublished).
 - [9] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).
 - [10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
 - [11] L. I. Schiff *Quantum Mechanics* (McGraw-Hill, New York, 1968).
 - [12] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996).
 - [13] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
 - [14] M. Reed and B. Simon, *Methods of Modern Mathematical Physics* (Academic Press, New York, 1979).
 - [15] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
 - [16] N. Gisin, Phys. Lett. A **210**, 151 (1996).