Reduction criterion of separability and limits for a class of distillation protocols

Michał Horodecki*
Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Paweł Horodecki†
Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-952 Gdańsk, Poland

(Received 12 November 1997)

We analyze the problem of distillation of entanglement of mixed states in higher-dimensional compound systems. Employing the positive maps method [M. Horodecki *et al.*, Phys. Lett. A **223**, 1 (1996)] we introduce and analyze a criterion of separability that relates the *structures* of the total density matrix and its reductions. We show that any state violating the criterion can be distilled by suitable generalization of the two-qubit protocol that distills any inseparable two-qubit state. In particular, this means that any state ϱ of two N-level systems with $\langle\psi_+|\varrho|\psi_+\rangle > 1/N$ can be distilled (ψ_+ is the singlet state generalized to higher dimension). The criterion also singles out all the states that can be distilled by a class of protocols. The proof involves construction of the family of states that are invariant under transformation $\varrho \rightarrow U\otimes U^* \varrho U^\dagger \otimes U^{*\dagger}$, where U is a unitary transformation and the asterisk denotes complex conjugation. The states are related to the depolarizing channel generalized to the nonbinary case. [S1050-2947(99)05904-1]

PACS number(s): 03.67.−a, 03.65.Bz, 42.50.Dv, 89.70.+c

I. INTRODUCTION

Quantum entanglement [1] produces many rather nonintuitive quantum phenomena such as quantum parallelism [2], quantum cryptography [3], quantum dense coding [4,5], quantum teleportation [6,7], and reduction of communication complexity [8]. In practice we usually deal with noisy entanglement, due to the fact that the pure states evolve to the mixed states under uncontrolled interaction with environment. A mixed state is supposed to contain entanglement if it cannot be written in the form [9]

$$\varrho = \sum_i p_i \varrho_A^i \otimes \varrho_B^i \tag{1}$$

(we call such a state entangled or inseparable). To benefit from the entanglement contained in an inseparable mixed state, we must convert it to the active singlet form by means of local quantum operations and classical communication (LQCC) between the parties sharing the pairs of particles in the mixed state [10–13]. Such a process is called purification or distillation of noisy entanglement.

It is clear that the separable states of the form (1) cannot be distilled, since LQCC operations cannot change the separable states into inseparable ones. Then it is natural to ask in this context: Can any inseparable state be distilled? To answer this question, one had to deal with two problems. First, it was necessary to have an operational criterion of separability (inseparability). Various necessary conditions of separability in terms of Bell and entropic inequalities [14–17] were presented. An important step is due to Peres [18], who showed that positivity of partial transpose of a state is a necessary condition for separability. Then it has been proved that the necessary and sufficient condition for separability of mixed state is its positivity under all the maps of the form $I\otimes\Lambda$, where Λ is any positive map [19]. This separability condition reduces for 2×2 and 2×3 systems [20] to positivity of the state under partial transpose.

Clearly, to answer the above question, apart from the characterization of inseparable states it was necessary to investigate protocols of distillation [10–13]. For 2×2 systems, it has been shown [13] that a protocol composed of local filtering [21,22] and recurrence protocol [10] is capable of distilling all inseparable states [23]. It seemed to be obvious that all the inseparable states can be distilled. However, recent results showed that this is not so. Namely, it turned out [24] that the states that do not violate the Peres condition cannot be distilled and there are explicit examples of mixed states the entanglement of which cannot be brought into singlet form. Such a nondistillable entanglement is called bound. Thus the answer to the above-mentioned question is negative.

In this context a basic problem arises: Can all the states violating the Peres condition be distilled? The answer to this question is at present unknown. To solve the problem, one should analyze distillation in higher dimensions. In this paper we perform such investigations.

One of the important tools we employ here is positive maps: we introduce a necessary condition for separability (we call it reduction criterion) based on positive map $\Lambda(A) = I\,\mathrm{Tr}\,A - A$. The condition is equivalent to separability for 2×2 (and 2×3) systems. Moreover, it has the property that any state of $N\times N$ system that violates it can be effectively distilled by suitable generalization of the protocol given in Ref. [13]. The converse also holds: the only states that can be distilled by such protocols necessarily violate the criterion. Thus we obtain limits on the use of the considered class of protocols. One of the essential steps is determining the family of states that is invariant under product unitary transformation of the form $U\otimes U^*$, where the star denotes complex conjugation. These are mixtures of completely chaotic

*Electronic address: michalh@iftia.univ.gda.pl
†Electronic address: pawel@mifgate.pg.gda.pl

©1999 The American Physical Society

states and the maximally entangled one ψ_+. We obtain that for $N\times N$ systems such a $U\otimes U^*$ invariant state can be distilled if and only if $\langle\psi_+|\varrho|\psi_+\rangle>1/N$. The family of states is closely related to the N-dimensional generalization of the generalized depolarizing channel.

This paper is organized as follows. In Sec. II we outline the method of investigation of inseparability by means of positive maps. In Sec. III we present a reduction criterion of separability based on the above-mentioned positive map. In particular, we show that it constitutes the necessary and sufficient condition for separability for 2×2 and 2×3 systems. We also show that it is weaker than the Peres criterion for higher dimensions. In Sec. IV we discuss the criterion in the context of the entropic criteria relating the density matrix of the system to its reductions. In Sec. V we derive the family of states that are invariant under action of unitary $U\otimes U^*$ transformations. We show how the family is related to the N-dimensional depolarizing channel. Subsequently, in Sec. VI, we utilize the results of the previous section to show that any state violating the reduction criterion can be distilled to the singlet form. It is done via generalized XOR operation and $U\otimes U^*$ twirling operation. We also point out that the criterion determines the range of use of a class of distillation protocols. We mean here the protocols consisting of two steps: (i) one-side, single-pair filtering, (ii) the procedure that cannot distill the states with a fully entangled fraction less than $1/N$. In Sec. VII the results are illustrated by means of some examples.

II. POSITIVE MAPS, COMPLETELY POSITIVE MAPS, AND INSEPARABILITY

In quantum mechanics, the state of a physical system is represented by a density matrix, i.e., positive operator of unit trace. Positivity means that the matrix is Hermitian and all its eigenvalues are nonnegative (if an operator σ is positive we write $\sigma\geqslant0$). This assures that diagonal elements of a density matrix written in any basis are nonnegative so that they can be interpreted as probabilities of events. Then, to describe the change of state due to a physical process, we need a (linear) map that preserves positivity of operators,

$$\sigma\geqslant0\Rightarrow\Lambda(\sigma)\geqslant0. \tag{2}$$

Such maps are called *positive* maps. However, it has been recognized [25] that the above condition is *not* sufficient for a given map to describe a physical process. Consider two systems A and B in some joint state ϱ_{AB}. Suppose the systems are spatially separated, so that each one evolves separately and the evolution of the subsystems is given by maps Λ_A and Λ_B. Then the total evolution is described by the map $\Lambda=\Lambda_A\otimes\Lambda_B$. Of course the operator $\varrho=\Lambda(\varrho_{AB})$ describing the state after evolution must still be positive. It leads us to a very strong condition: the tensor multiplication of the maps describing the physical processes must still be a positive map. The maps belonging to the subset of positive maps satisfying this condition are called *completely positive*. It appears that a map Λ belongs to this family if and only if $\Lambda\otimes I_N$ is a positive map for each natural N, where $I_N:M_N\to M_N$ denotes an identity map acting on $N\times N$ matrices (i.e., the matrices with N rows and N columns). This is commonly regarded as the definition of a completely positive (CP) map [25]. For finite-dimensional systems an even weaker condition is sufficient (see Appendix). Finally, one can distinguish an important subfamily of the CP maps that preserves trace, i.e.,

$$\mathrm{Tr}\,\Lambda(\sigma)=\mathrm{Tr}\,\sigma.$$

In contrast with such a general and slightly abstract approach, one can consider the basic processes allowed by the quantum formalism:

(i) $\varrho\to\varrho\otimes\varrho'$ (adding a system in state ϱ'),
(ii) $\varrho\to U\varrho U^\dagger$ (unitary transformation),
(iii) $\varrho_{AB}\to\mathrm{Tr}_B\varrho_{AB}$ (discarding the system—partial trace).

One can argue that any map describing physical processes should be able to be written by means of the above three maps [25]. It appears that comparison of the two approaches leads to a satisfactory result: any trace-preserving CP map can be composed of the above trace-preserving CP maps. Supplementing the three basic processes with the process of selection after measurement, we obtain the family of all CP maps. Thus, the most general physical process the quantum state can undergo is described by a CP map. As a result, the structure of the family of the CP maps has been extensively investigated [26,25] and is at present well known. However, one knows that there exist positive maps that are not CP maps. A familiar example is time-reversal operator, which acts as a transposition of a matrix in a chosen basis,

$$(T\sigma)_{ij}=\sigma_{ji}. \tag{3}$$

To see that it is not CP, hence cannot describe a physical process [27,28], consider a two-spin-$\frac{1}{2}$ system in the singlet state given by

$$\psi_s=\frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle-|\downarrow\rangle|\uparrow\rangle). \tag{4}$$

Suppose that one of the subsystems is subjected to transposition while the other one does not evolve. Then it is easy to see that the resulting operator $A=(I\otimes T)(|\psi_s\rangle\langle\psi_s|)$ is not positive.

Since the positive maps that are not CP cannot describe physical evolution, their structure has not been extensively investigated and remains still obscure. However, recently it has been realized that they can be a powerful tool in the investigation of quantum inseparability of mixed states [19]. To see this, let us discuss in more detail the considerable failing of the positive non-CP maps. The fault is that there *are* states of compound systems (like the singlet state) that are mapped by $I\otimes\Lambda$ onto operators that are not positive. The basic question is, what features of the ‘‘bad’’ states cause the trouble? To answer the question, recall that the singlet state is *entangled*, since it cannot be written as a product of two state vectors describing the subsystems. As we mentioned in the Introduction, the notion of entanglement extends naturally to cover mixed states [see formula (1)]. Now, let us note that there is no trouble with positive non-CP maps as long as we deal with separable states only. Indeed, in this case, if one of the systems is subjected to a positive map, the resulting operator remains positive:

$$(I\otimes\Lambda)\left(\sum_i p_i\varrho_A^i\otimes\varrho_B^i\right)=\sum_i p_i\varrho_A^i\otimes\Lambda(\varrho_B^i)\geqslant 0 \qquad (5)$$

since $\Lambda(\varrho_B^i)\geqslant 0$ due to positivity of Λ. Thus, if a positive map is not CP, this can be recognized only by means of inseparable states. In other words, it is only *inseparability* that forces us to remove some positive maps from the family of maps describing physical processes. This suggests that the positive maps can be extremely useful tool for investigation of inseparability. Indeed, a theorem has been proved [19] stating that *any state is inseparable if and only if there exists a positive map such that* $(I\otimes\Lambda)(\varrho)$ *is not positive*. In particular, if we have a positive map that is not CP, then it automatically provides a necessary condition for separability that can be written as

$$(I\otimes\Lambda)(\varrho)\geqslant 0. \qquad (6)$$

This means that if a state is separable, the above inequality holds.

III. REDUCTION CRITERION OF SEPARABILITY

In this section we will utilize the map (acting on matrices $N\times N$) of the form [29]

$$\Lambda(\sigma)=I\,\mathrm{Tr}\,\sigma-\sigma, \qquad (7)$$

where I is an identity matrix. It is easy to see that if $\sigma\geqslant 0$ then also $I\,\mathrm{Tr}\,\sigma-\sigma\geqslant 0$, hence Λ is a positive map. Writing the condition (6) explicitly for this particular map, we obtain [30]

$$\varrho_A\otimes I-\varrho\geqslant 0, \qquad (8)$$

where $\varrho_A=\mathrm{Tr}_B\varrho$ is a reduction of the state of interest. Thus, to use the criterion, one should find the reduction ϱ_A and check nonnegativity of the eigenvalues of the operator $\varrho_A\otimes I-\varrho$. Of course, one can also consider the dual criterion

$$I\otimes\varrho_B-\varrho\geqslant 0. \qquad (9)$$

Since the two conditions involve reduction of the density matrix, we will refer to their conjunction as the reduction criterion.

Let us now consider briefly the reduction criterion in the context of the Peres partial transpose criterion [18], which can be explicitly written as

$$(I\otimes T)(\varrho)\equiv\varrho^{T_B}\geqslant 0. \qquad (10)$$

Here $\varrho^{T_B}_{m\mu,n\nu}\equiv\langle e_m\otimes f_\mu|\varrho^{T_B}|e_n\otimes f_\nu\rangle=\varrho_{m\nu,n\mu}$ and $\{e_i\otimes f_j\}_{ij}$ is any product basis. It is easy to see that both criteria are equivalent for the 2×2 (and 2×3) case. Indeed, the map (7) is, in this case, of the form $\Lambda(A)=(\sigma_y A\sigma_y)^T$ producing then equivalent criterion. Note that for higher dimensions, the map (7) can be composed of a transpose and a completely positive map (see Appendix). Hence, according to [19], if a given state violates the criterion (8) then it must also violate the Peres criterion [32]. Indeed, suppose that ϱ satisfies the latter. Then we have $\sigma\equiv\tilde{T}\varrho\geqslant 0$, hence also for any CP map Λ_{CP} the operator $\tilde{\Lambda}_{CP}(\tilde{T}(\sigma))$ is positive (here $\tilde{\Lambda}$ denotes the map $I\otimes\Lambda$). Consequently, if a positive, but not CP, map Λ can be written as $\Lambda=\Lambda_{CP}T$ (or equivalently $\Lambda=T\Lambda_{CP}$, see Appendix) and a state satisfies the condition (10), then it also satisfies the condition $\tilde{\Lambda}\varrho\geqslant 0$ constituted by Λ. Thus we see that the reduction criterion is not stronger than the Peres criterion.

On the other hand, there exist states that satisfy the reduction criterion but violate the Peres criterion. These are the Werner states [9] W_N of $N\times N$ system, given by

$$W_N=(N^3-N)^{-1}\{(N-\phi)I+(N\phi-1)V\}, \qquad (11)$$

where $-1\leqslant\phi\leqslant 1$ and V is defined as $V\psi\otimes\tilde{\psi}=\tilde{\psi}\otimes\psi$. The states are inseparable for $\phi<0$. For a 2×2 system the Werner states take a simple form [33],

$$W_2=(1-\alpha)\frac{I}{4}+\alpha|\psi_s\rangle\langle\psi_s|, \quad -\tfrac{1}{3}\leqslant\alpha\leqslant 1, \qquad (12)$$

being mixtures of the maximally chaotic state and the singlet state for $\alpha\geqslant 0$. It can be seen that for $N\geqslant 3$ inseparable Werner states violate the partial transpose criterion while satisfying the reduction one. Indeed, they have maximally mixed reductions and the norm (maximal eigenvalue) is less than $1/N$, hence the inequality (8) cannot be violated (explicitly, the reduction criterion for Werner states is written as $2-N\leqslant\phi\leqslant N$, which is satisfied for $N\geqslant 3$).

The family of Werner states has an interesting property, namely, they are the only states invariant under any transformation of the form

$$\varrho\rightarrow U\otimes U\varrho U^\dagger\otimes U^\dagger, \qquad (13)$$

where U is a unitary transformation. As we will see, our criterion will lead in a natural way to distinguishing another family of states that are invariant under any transformation of the form

$$\varrho\rightarrow U\otimes U^*\varrho U^\dagger\otimes U^{*\dagger}, \qquad (14)$$

where the asterisk denotes complex conjugation of matrix elements of U (we will call such states $U\otimes U^*$ invariant). The two families are identical (up to a local unitary transformation) for the two-qubit case, but become distinct for higher dimensions.

To summarize, in higher dimensions the reduction criterion is weaker than the Peres criterion [34]. The advantage of the reduction criterion is that, as will be shown, all the states violating it *can* be distilled. The latter result is compatible with [13], where it is shown that the two-qubit states that violate the Peres criterion can be distilled.

Finally, there is a question of whether one could obtain a stronger criterion by applying the present one to the state of the form $\varrho\otimes\cdots\otimes\varrho$ rather than to the state ϱ of single pair (we will call it collective application of the criterion). Here the big tensor product divides the full system into the systems of single pairs, in contrast to the small one, which divides the system into Alice and Bob systems. Consider now the Peres condition (10) and apply it collectively. One can check that [18]

$$\tilde{T}(\varrho_1\otimes\varrho_2)=\tilde{T}(\varrho_1)\otimes\tilde{T}(\varrho_2). \tag{15}$$

Hence, if the state $\varrho\otimes\varrho$ violates the criterion, then so does ϱ, so that the collective application of the Peres criterion does not produce a stronger one. Recently, Rains proved [35] that in the case of the reduction criterion, too, if the state $\varrho_1\otimes\varrho_2$ of two pairs violates it, then the state of each pair separately also does. Indeed, denoting the partial traces of states ϱ_1 and ϱ_2 over the systems B by τ_1 and τ_2, respectively, one obtains

$$\tilde{\Lambda}(\varrho_1\otimes\varrho_2)=(I\otimes\tau_1)\otimes(I\otimes\tau_2)-\varrho_1\otimes\varrho_2, \tag{16}$$

hence

$$\begin{aligned}\tilde{\Lambda}(\varrho_1)\otimes\tilde{\Lambda}(\varrho_2)&=(I\otimes\tau_1-\varrho_1)\otimes(I\otimes\tau_2-\varrho_2)\\&=\tilde{\Lambda}(\varrho_1\otimes\varrho_2)+2\varrho_1\otimes\varrho_2\\&\quad-\varrho_1\otimes(I\otimes\tau_2)-(I\otimes\tau_1)\otimes\varrho_2.\end{aligned} \tag{17}$$

This can be rewritten as

$$\tilde{\Lambda}(\varrho_1\otimes\varrho_2)=\tilde{\Lambda}(\varrho_1)\otimes\tilde{\Lambda}(\varrho_2)+\varrho_1\otimes\tilde{\Lambda}(\varrho_1)+\tilde{\Lambda}(\varrho_2)\otimes\varrho_2. \tag{18}$$

Hence one obtains the desired result, i.e.,

$$[\tilde{\Lambda}(\varrho_1)\geqslant 0 \ \text{ and } \ \tilde{\Lambda}(\varrho_2)\geqslant 0]\Rightarrow\tilde{\Lambda}(\varrho_1\otimes\varrho_2)\geqslant 0. \tag{19}$$

IV. REDUCTION CRITERION AND ENTROPIC CRITERIA

It is interesting to discuss the reduction criterion in the context of entropic criteria, which also exploit the relation between the total system and its subsystems. The first necessary condition of separability of this type was constructed by means of von Neumann entropies of the system and subsystems [15]. The entropic criteria were then generalized by using the quantum Renýi entropies S_α [16]. They are given by the following inequalities for conditional entropies [16,17]:

$$S_\alpha(A|B)\geqslant 0, \quad S_\alpha(B|A)\geqslant 0 \tag{20}$$

with

$$S_\alpha(A|B)=S_\alpha(\varrho)-S_\alpha(\varrho_B), \quad S_\alpha(B|A)=S_\alpha(\varrho)-S_\alpha(\varrho_A), \tag{21}$$

where

$$S_\alpha=\frac{1}{1-\alpha}\ln\mathrm{Tr}\ \varrho^\alpha \ \text{ for } \ 1<\alpha<\infty, \tag{22}$$

S_1 is the von Neumann entropy and $S_\infty=-\ln\|\varrho\|$. It has been shown [15,16,19] that the above inequalities are satisfied by separable states for $\alpha=1$, 2, and ∞.

The crucial difference is that these are *scalar* conditions, while the reduction criterion relates the *structure* of the density matrix to its reductions rather than scalar functions. This suggests that the entropic inequalities should be weaker than the reduction criterion. In fact, it is the case for $\alpha=1$ (see [31]) and $\alpha=\infty$ (see below). Of course, even weak conditions are not useless. For instance, the von Neumann conditional entropy has been recently used for definition of quantum coherent information—a very important characteristic of quantum channels [36]. If, however, one is interested in characterization of separable (inseparable) states, the structural criteria are much more convenient. Let us now show that the reduction criterion is stronger than the ∞-entropy inequality. The latter criterion says, in fact, that for a separable state the largest eigenvalue of the density matrix of the total system cannot exceed the largest eigenvalue of any of the reduced density matrices:

$$\|\varrho\|\equiv\lambda_{\max}(\varrho)\leqslant\lambda_{\max}(\varrho_X)\equiv\|\varrho_X\|, \quad X=A,B. \tag{23}$$

It is seen that the above inequalities are implied by the conditions (8),(9). Indeed, suppose that (8) is satisfied, i.e., $\varrho\leqslant\varrho_A\otimes I$. Note that if $0\leqslant\sigma_1\leqslant\sigma_2$ then we have also $0\leqslant\|\sigma_1\|\leqslant\|\sigma_2\|$. Consequently, since ϱ is positive and $\|\varrho_A\|=\|\varrho_A\otimes\square\|$, we immediately obtain that $\|\varrho\|\leqslant\|\varrho_A\otimes I\|=\|\varrho_A\|$. Similarly, (9) implies $\|\varrho\|\leqslant\|\varrho_B\|$.

For the states with maximally disordered subsystems the reduction criterion is equivalent to the ∞-entropy inequality. Indeed, in this case the smallest eigenvalue of the operator $\varrho_A\otimes I-\varrho$ is equal to $\lambda=(1/N)-\|\varrho\|=\|\varrho_A\|-\|\varrho\|$, hence both criteria are satisfied or violated simultaneously. Finally, the reduction criterion is *essentially* stronger than the ∞-entropy inequalities, as the latter are not sufficient for separability for two-qubit systems [19] while the reduction criterion is, as shown in the preceding section.

V. $U\otimes U^*$-INVARIANT STATES

In this section, applying the method used by Werner [9] we derive the family of $U\otimes U^*$ invariant states. For this purpose let us consider a Hermitian operator A, which we want to be $U\otimes U^*$ invariant. Let us write its matrix elements in a product basis

$$\langle mn|A|pq\rangle\equiv\langle e_m\otimes e_n|A|e_p\otimes e_q\rangle. \tag{24}$$

Imposing on A the condition of $U\otimes U^*$ invariance with unitary operations U converting some $|m_0\rangle$ into $-|m_0\rangle$ and leaving the other basis elements unchanged, we obtain that the only nonzero elements are of type $\langle mn|A|mn\rangle$, $\langle mn|A|nm\rangle$, and $\langle mm|A|nn\rangle$. Now, taking into account another set of unitary transformations, each of the latter multiplying some single basis element by imaginary unit i and leaving the remaining elements unchanged, we obtain immediately that all $\langle mn|A|nm\rangle, m\neq n$ elements must vanish. Then, considering all two-element permutations of basis vectors we obtain that the set of nonvanishing matrix elements can be divided into three groups: $\langle mn|A|mn\rangle, m\neq n$, $\langle mm|A|nn\rangle, m\neq n$, and $\langle mm|A|mm\rangle$ with all elements in each group being equal. Thus, any $U\otimes U^*$ invariant Hermitian operator can be written as $A=bB+cC+dD$, where $B=\Sigma_{m\neq n}|mn\rangle\langle mn|, C=\Sigma_{m\neq n}|mm\rangle\langle nn|, D=\Sigma_m|mm\rangle\langle mm|$. Obviously, hermiticity of A implies that parameters b,c,d should be real. One can introduce real unitary transformation of type

$$U_1\otimes U_1=(\tilde{U}_2\oplus I_{N-2})\otimes(\tilde{U}_2\oplus I_{N-2}) \tag{25}$$

with

$$\tilde{U}_2=\begin{bmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{bmatrix}, \tag{26}$$

where $\tilde{U}_2$ acts on some two-dimensional subspace H_1 of the Hilbert space H of a subsystem and I_{N-2} is a projection onto an orthogonal complement of H_1. It can be easily shown that the operator D is not invariant under $U_1\otimes U_1$, and hence is not $U\otimes U^*$ invariant. Thus parameter d appears to be linearly dependent on b and c. Demanding, in addition, $\mathrm{Tr}(A)=1$, we obtain that the set of Hermitian $U\otimes U^*$ invariant operators with unit trace are described by one real linear parameter. On the other hand, it can be checked immediately that the family

$$\varrho_\alpha=(1-\alpha)\frac{I}{N^2}+\alpha P_+ \tag{27}$$

fulfills the above criteria. Here $P_+=|\psi_+\rangle\langle\psi_+|$ with

$$\psi_+=\frac{1}{\sqrt{N}}\sum_{i=1}^{N}|i\rangle\otimes|i\rangle \tag{28}$$

is the generalized singlet state. Indeed, the identity operator is obviously $U\otimes U^*$ invariant and for P_+ we obtain

$$U\otimes U^* P_+ U^\dagger\otimes U^{*\dagger}=I\otimes U^*U^T P_+ I\otimes(U^*U^T)^\dagger=P_+, \tag{29}$$

where the property [37] $A\otimes I\psi_+=I\otimes A^T\psi_+$ was used. Imposing now the positivity condition (we are interested in states), we obtain the family

$$\varrho_\alpha=(1-\alpha)\frac{I}{N^2}+\alpha P_+, \quad \text{with } \frac{-1}{N^2-1}\leqslant\alpha\leqslant 1. \tag{30}$$

Note that ϱ_α can be viewed as a generalization of the two-qubit Werner-Popescu state (12) being a mixture of singlet and maximally chaotic states. The family can be parametrized by fidelity $F=\mathrm{Tr}\,\varrho_\alpha P_+$ as follows:

$$\varrho_{\alpha(F)}\equiv\varrho_F=\frac{N^2}{N^2-1}\left[(1-F)\frac{I}{N^2}+\left(F-\frac{1}{N^2}\right)P_+\right],$$
$$0\leqslant F\leqslant 1. \tag{31}$$

The above states are inseparable for $F>1/N$, since they violate the condition (8). Since F is a $U\otimes U^*$ invariant parameter, we obtain that for $F\leqslant 1/N$ [respectively, $\alpha\leqslant 1/(N+1)$] the states can be reproduced by $U\otimes U^*$ twirling, i.e., a random $U\otimes U^*$ operation represented by the integral

$$\int U\otimes U^*\sigma U^\dagger\otimes U^{*\dagger}dU, \tag{32}$$

performed on the proper *product* pure state σ (here dU denotes uniform probability distribution on unitary group $U(N)$ proportional to the Haar measure). This can be the state $\sigma=P_\phi\otimes P_{\phi'}$ corresponding to the vectors $\phi=|1\rangle,\phi'=a|1\rangle+b|2\rangle$ with $F=(|\langle\phi|\phi'\rangle|^2)/N$. Thus the states (31) [respectively, (30)] are inseparable *if and only if* $F>1/N$, respectively $[\alpha>1/(N+1)]$.

The family presented defines the N-dimensional *α-depolarizing channel*, which completely randomizes the state of N-level input systems with probability α while it leaves it undisturbed with probability $1-\alpha$. Such a channel, in the case $N=2$, has recently been extensively investigated [12,38]. As will be shown, the corresponding family of states (30) resulting from sending half of the state P_+ through the (N,α)-depolarizing channel can be distilled by means of LQCC operations if and only if $F>1/N$, respectively $[\alpha>1/(N+1)]$. Then by using the results relating quantum capacities and distillable entanglement [12], we obtain that the considered channel supplemented by a two-way classical channel [12] has nonzero quantum capacity for this range of α. This reproduces the known result $F>\frac{1}{2}(\alpha>\frac{1}{3})$ for $N=2$ [12].

VI. DISTILLATION PROTOCOL

Now our goal is to distill the states that violate the condition (8). The first stage (filtering) [21,22] will be almost identical to that of the protocol given in [13]. For this purpose rewrite the condition (8) in the form

$$\langle\psi|\varrho_A\otimes I-\varrho|\psi\rangle\geqslant 0 \quad \text{for any} \quad \psi\in C^N\otimes C^N, \quad ||\psi||=1, \tag{33}$$

or

$$\mathrm{Tr}\,\varrho P_\psi\leqslant\mathrm{Tr}\;\varrho_A\varrho_A^\psi, \tag{34}$$

where $P_\psi=|\psi\rangle\langle\psi|$ and ϱ_A^ψ is reduced density matrix of P_ψ. Note that if we take P_ψ to be maximally entangled states and maximize the left-hand side of Eq. (34) over them, we will obtain the condition for fully entangled fraction [10,12] generalized to higher dimensions,

$$f(\varrho)\equiv\max_\Psi\mathrm{Tr}(\varrho P_\Psi), \tag{35}$$

where the maximum is taken over all maximally entangled Ψ's. Namely, we then have

$$f(\varrho)\leqslant\frac{1}{N} \tag{36}$$

for any separable ϱ. Suppose now that a state ϱ *violates* the condition (34) for a certain vector $|\psi\rangle$,

$$|\psi\rangle=\sum_{m,n}a_{mn}|m\rangle\otimes|n\rangle. \tag{37}$$

Now, any such vector can be produced from the singlet state ψ_+ given by Eq. (28) in the following way:

$$|\psi\rangle=A\otimes I|\psi_+\rangle, \tag{38}$$

where $\langle m|A|n\rangle=\sqrt{N}a_{mn}$. It can be checked that $AA^\dagger=N\varrho_A^\psi$. Then, the new state

$$\varrho'=\frac{A^\dagger\otimes I\varrho A\otimes I}{\mathrm{Tr}(\varrho AA^\dagger\otimes I)} \tag{39}$$

resulting from filtering ϱ by means of one-side action $A^\dagger \otimes I \varrho A \otimes I$ satisfies the inequality

$$\operatorname{Tr} \varrho' P_+ > \frac{1}{N}. \tag{40}$$

Now, the problem is how to distill states with the property (40). For this purpose we need to generalize the protocol [10] used for the two-qubit case. The first thing we need is the generalized twirling procedure, which would leave the state P_+ unchanged. This, however, cannot be the application of the random bilateral unitary transformation of the form $U \otimes U$ since there is no $U \otimes U$ invariant pure state in higher dimensions [this can be seen directly from the form of the Werner states (11)]. As we have shown in Sec. V, we obtain a suitable generalization by applying at random transformations $U \otimes U^*$, where the asterisk denotes complex conjugation in any chosen basis (e.g., in the basis $|i\rangle$). From the results of the preceding section it follows that for any ϱ if $\operatorname{Tr} \varrho P_+ = F$ then

$$\int U \otimes U^* \varrho U^\dagger \otimes U^{*\dagger} dU$$
$$= \varrho_\alpha \equiv (1-\alpha)\frac{I}{N} + \alpha P_+ \quad \text{with} \quad \alpha = \frac{N^2 F - 1}{N^2 - 1},$$
$$0 \leqslant F \leqslant 1, \tag{41}$$

i.e., after twirling we obtain state ϱ_α with the same fidelity F as the initial state. As was shown in the preceding section, the states ϱ_α are inseparable if and only if $F > 1/N$.

Now, to distill the states considered we need to generalize the quantum XOR gate [2]. The N-dimensional counterpart of the latter we choose to be

$$U_{XOR^N} |k\rangle |l\rangle = |k\rangle |l \oplus k\rangle, \tag{42}$$

where $k \oplus l = (k + l) \bmod N$. The $|k\rangle$ and $|l\rangle$ states describe the source and target systems, respectively. Now the protocol is analogous to that in Ref. [10]. (1) Two input pairs are twirled, i.e., each of them is subjected to random bilateral rotation of type $U \otimes U^*$. (2) The pairs are subjected to the transformation $U_{XOR} N \otimes U_{XOR} N$. (3) The target pair is measured in the basis $|i\rangle \otimes |j\rangle$. (4) If the outcomes are equal, the source pair is kept, otherwise it is discarded.

If the outcomes are identical, then by twirling the resulting source pair we obtain it in state $\varrho_{\alpha'}$ where α' satisfies the equation

$$\alpha'(\alpha) = \alpha \frac{[N(N+1)-2]\alpha + 2}{(N+1)[1+(N-1)\alpha^2]}. \tag{43}$$

The above function is increasing and continuous in total range $\alpha \in [1/(N+1), 1]$. Hence, as in Ref. [10], the fidelity F increases if the initial fidelity was greater than $1/N$. Then to obtain a nonzero asymptotic yield of distilled pure entanglement, one has to follow the above protocol to obtain some high-fidelity F and then project locally the resulting state onto two-dimensional spaces. For high enough F the resulting states on the 2×2 system can be distilled by, e.g., hashing protocol ([12]) (if needed, the obtained 2×2 singlets can be changed into $N \times N$ singlets; this will be considered in more detail elsewhere).

To summarize, given a large number of pairs of particles in a state that violates the condition (8) [or (9)], one first needs to apply the filtering procedure given by operator A, and then subject the pairs that passed the filter to the recurrence protocol described above. Note that operator A, if it is to describe the process of filtering (or a part of generalized measurement), should be properly normalized, so that $\|A\| \leqslant 1$.

Thus we have shown that any state violating the reduction criterion can be distilled. Suppose, conversely, that a state can be distilled by a protocol consisting of two steps: (i) one-side, single-pair filtering and (ii) a protocol that distills a state if and only if $F > 1/N$. Then after the filtering step the new state must satisfy inequality (40). Hence, the initial state must violate the inequality (33) for a vector $\psi = I \otimes A \psi_+$, where A described the filter. So we obtain that if a state can be distilled by means of the kind of protocols considered, it violates the reduction criterion.

Note that the present results allow for simple, independent proof of the fact [39] that the tensor product of K pairs of two spin-$\frac{1}{2}$ Bell diagonal states $\otimes_K \varrho_B$, each with fidelity $F \leqslant \frac{1}{2}$, cannot be transformed into a state of $N \times N$ system with $F' > 1/N$ by means of separable superoperators [40,39], which are defined as $\Lambda(\varrho) = \Sigma_i A_i \otimes B_i \varrho A_i^\dagger \otimes B_i^\dagger$. Indeed, if a two-spin-$\frac{1}{2}$ Bell diagonal state ϱ_B has $F \leqslant \frac{1}{2}$, then it is separable state [12,17]. On the other hand, any state of $N \times N$ system, say σ_N, with $F > 1/N$ is inseparable since it can be $U \otimes U^*$ twirled to the state (31) with $F > 1/N$, which we have shown to be inseparable. But *no* separable state (in particular $\otimes_K \varrho_B$ constructed from separable states ϱ_B) can be transformed by separable operations into the inseparable state σ_N.

VII. EXAMPLES

In this section we will illustrate the reduction criterion and the first stage of our distillation protocol. For this purpose, consider the following unitary embedding of the Hilbert space C^N into $C^N \otimes C^N$ [41]

$$|i\rangle \rightarrow |i\rangle \otimes |i\rangle. \tag{44}$$

By means of this transformation we can ascribe to any state ϱ^N on C^N a state ϱ_e^N acting on $C^N \otimes C^N$. For example, if $N = 3$ and ϱ^N is given by

$$\varrho^N = \begin{bmatrix} \varrho_{11} & \varrho_{12} & \varrho_{13} \\ \varrho_{21} & \varrho_{22} & \varrho_{23} \\ \varrho_{31} & \varrho_{32} & \varrho_{33} \end{bmatrix} \tag{45}$$

then

$$\varrho_e^N=\begin{bmatrix} \varrho_{11} & 0 & 0 & 0 & \varrho_{12} & 0 & 0 & 0 & \varrho_{13}\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ \varrho_{21} & 0 & 0 & 0 & \varrho_{22} & 0 & 0 & 0 & \varrho_{23}\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ \varrho_{31} & 0 & 0 & 0 & \varrho_{32} & 0 & 0 & 0 & \varrho_{33} \end{bmatrix} \quad (46)$$

The reductions of ϱ_e^N are both equal to the state ϱ^N with the off-diagonal set equal to 0. That the state ϱ_e^N is inseparable if and only if ϱ^N is not diagonal can be viewed in different ways. First, the state ϱ_e^N with some off-diagonal elements different from zero violates the ∞-entropy inequality as $\|\varrho_e^N\|=\|\varrho^N\|>\max_j\{\varrho_{jj}\}=\|\varrho_{e,X}^N\|$, where $X=A$ or B (of course if ϱ^N is diagonal then ϱ_e^N is trivially separable). On the other hand, we can apply the Peres criterion [18]. However, the two criteria do *not* say whether and how the state can be *distilled*. Then let us apply the reduction criterion. Here (e.g., for $N=3$) we have

$$\varrho_{e,A}^N\otimes I-\varrho_e^N=\begin{bmatrix} 0 & 0 & 0 & 0 & -\varrho_{12} & 0 & 0 & 0 & -\varrho_{13}\\ 0 & \varrho_{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \varrho_{11} & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & \varrho_{22} & 0 & 0 & 0 & 0 & 0\\ -\varrho_{21} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\varrho_{23}\\ 0 & 0 & 0 & 0 & 0 & \varrho_{22} & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \varrho_{33} & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \varrho_{33} & 0\\ -\varrho_{31} & 0 & 0 & 0 & -\varrho_{32} & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (47)$$

Hence, if only the state ϱ_e^N is inseparable, it violates the criterion. Then we can distill the state calculating the eigenvector corresponding to the suitable negative eigenvalue, subjecting the state to the appropriate filter and performing then the recurrence protocol. However, it can be checked that for $N=3$ this state already has fidelity greater than $\frac{1}{3}$; hence it can be distilled without the filtering step.

Consider now the second, more explicit, example. Let P_+^3 denote the singlet state (28) with $N=3$ and let $P_{ij}=|i\rangle\langle i|\otimes|j\rangle\langle j|$. The state of interest is

$$\sigma=pP_+^3+(1-p)P_{12}, \quad p\leqslant\tfrac{1}{3}. \quad (48)$$

It can be proved that fully entangled fraction f of this state is not greater than $\frac{1}{3}$. For this purpose, consider the overlap of the $U_A\otimes U_B$ transformation of the state P_+ with an arbitrary pure state P_Φ, $\Phi=\Sigma_{i,j=1}^N a_{ij}|i\rangle|j\rangle$. We obtain that

$$\mathrm{Tr}(P_\Phi U_A\otimes U_B P_+ U_A^\dagger\otimes U_B^\dagger)=\mathrm{Tr}(P_\Phi I\otimes U_B U_A^\dagger P_+ U_A U_B^\dagger)=|\mathrm{Tr}(A_\Phi U_B U_A^\dagger)|^2, \quad (49)$$

where, as in Sec. VI, the matrix elements of A_Φ are $\{A_\Phi\}_{ij}=\sqrt{N}a_{ij}$. Straightforward computation analogous to the one performed in Ref. [42] leads us to the following formula for a fully entangled fraction of pure state Φ:

$$f(P_\Phi)=[\mathrm{Tr}(\sqrt{(A_\Phi A_\Phi^\dagger)})]^2=\frac{1}{N}\left(\sum_{i=1}^N c_i\right)^2, \quad (50)$$

where c_i are Schmidt decomposition (hence positive) coefficients of the state Φ. From the above formula it follows that in our case the fully entangled fraction of the product pure state cannot be greater than $\frac{1}{3}$. Since we assumed that the probability p is also not greater than $\frac{1}{3}$, we obtain immediately that the fully entangled fraction of the state satisfies $f(\sigma)\leqslant\frac{1}{3}$. Now we can apply the prescription given in Sec. V. According to Eq. (48) we have the matrix $\sigma_A\otimes I-\sigma$ of the form

$$\sigma_A \otimes I - \sigma = \begin{bmatrix} 1-p & 0 & 0 & 0 & -\frac{p}{3} & 0 & 0 & 0 & -\frac{p}{3} \\ 0 & \frac{p}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1+\frac{2}{3}p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{p}{3} & 0 & 0 & 0 & 0 & 0 \\ -\frac{p}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{p}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{p}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{p}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{p}{3} & 0 \\ -\frac{p}{3} & 0 & 0 & 0 & -\frac{p}{3} & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{51}$$

This matrix has negative eigenvalue $\lambda = \frac{1}{2}(1-\frac{4}{3}p - \sqrt{1-\frac{4}{3}p+\frac{4}{3}p^2})$ with the corresponding eigenvector $|\psi\rangle$,

$$|\psi\rangle = \frac{1}{\sqrt{1+2y^2}}(|1\rangle|1\rangle + y|2\rangle|2\rangle + y|3\rangle|3\rangle),$$

$$y = \frac{1}{4p}(3-10p+3\sqrt{1-\tfrac{4}{3}p+\tfrac{4}{3}p^2}). \tag{52}$$

According to Sec. V, in order to distill some entanglement from the state, we can apply the local filter

$$A = \sqrt{\frac{3}{1+2y^2}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & y \end{bmatrix}. \tag{53}$$

Then we obtain the new state

$$\sigma' = \frac{1+2y^2}{3-2p+2py^2}\left(pP_+ + \frac{3(1-p)}{1+2y^2}P_{12} \right)$$
$$\equiv p'P_+ + (1-p')P_{12}. \tag{54}$$

From the previous results, we know that the new state must have fidelity greater than $\frac{1}{3}$. To see it in this particular case it suffices only to show that $p'/(1-p') > \frac{1}{2}$. This inequality can be transformed to the form

$$3-14p+22p^2+(3-10p)\sqrt{1-\tfrac{4}{3}p+\tfrac{4}{3}p^2} > 0. \tag{55}$$

Using the fact that $p \leqslant \frac{1}{3}$, the last term in this formula is not less than $\frac{1}{3}$. This leads to an inequality that can be checked directly. Thus in the process of filtering, the input state with a fidelity of less than $\frac{1}{3}$ has been transformed into the state with F strictly greater than $\frac{1}{3}$. Then the protocol based on generalized XOR operations described in Sec. V can be applied. Note that the result of the procedure is independent of the choice of normalization of the filter. Thus we can multiply the matrix by a constant to obtain $||A|| = 1$. Then, since for $p \leqslant \frac{1}{3}$ we have $y \geqslant 1$, the optimal filter is given by

$$A = \begin{bmatrix} \frac{1}{y} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{56}$$

VIII. DISCUSSION AND CONCLUSION

We have introduced a separability criterion (reduction criterion) relating the *structures* of the total state of the system to its reductions. To obtain the criterion, we employed the connection between positive maps and inseparability. Subsequently, we have shown that any state violating the reduction criterion is distillable. Now, in further investigation of the problem of whether any state violating the Peres condition can be distilled, it suffices to restrict oneself to the states that satisfy the criterion. Moreover, we have determined a limit for use of a class of protocols i.e., those consisting of two steps: one-side, single-pair filtering and any procedure that can only distill the states with a fully entangled fraction greater than $1/N$.

It is worth noting that to prove that any state violating the reduction criterion can be distilled, the main task was to distill inseparable $U\otimes U^*$ invariant states. In a similar way, it can be shown that to be able to distill all the states violating the partial transpose criterion one needs only to provide a protocol of distillation of the inseparable $U\otimes U$ invariant states (Werner states). This, combined with filtering, will produce the desired result. So the problem of whether or not the Peres criterion puts the borderline between bound (non-distillable) and free (ditstillable) entanglement is equivalent to the problem of whether or not all inseparable Werner states can be distilled. Up until now, we have known how to distill only some of the Werner states (this can be achieved by using the Popescu result [43]); however, the rest cannot be distilled by known methods.

The present criterion may be exploited together with two-side filtering and it cannot be ruled out that it might allow us to distill states that do not violate it at the beginning. Then it is interesting to characterize the class of states that initially do not violate the criterion, but do if subjected to a one-side filtering. It is remarkable that all the states violating the criterion, or violating it after local transformations, are nonlocal. This follows from consideration of the distillation process in the context of the sequential hidden variable model [43,44].

The reduction criterion divides the set of inseparable states into two classes of states: those that violate it and those that satisfy it. It seems that the former possess properties analogous to the inseparable two-qubit states. In particular, there is a hope that the methods that have been successfully applied to the two-qubit states (or one-qubit quantum channels), such as weight enumerator techniques [45,39], will also work for the states violating the reduction criterion (or corresponding noisy channels). Then the latter states could be called two-qubit-like states. In contrast, the inseparable states satisfying the criterion are supposed to exhibit features that never occur in the two-qubit case. To deal with these states, completely new methods must be worked out. An example of such states is Werner states, for which no direct generalization of two-qubit methods leads to distillation.

Finally, note that both positive maps applied so far in investigations of separability have some physical sense. The transpose means changing the direction of time [27]. The present positive map if applied to a part of a compound system indicates a nonzero content of pure entanglement in the state of the system. Then we believe that further investigation of inseparability by means of positive maps could allow us not only to characterize the set of separable states, but also to reveal a possible physical meaning of maps that are positive but not completely positive.

ACKNOWLEDGMENTS

We are indebted to A. Kossakowski and A. Uhlmann for a discussion on positive maps, R. Horodecki for many helpful comments, and E. Rains for allowing us to incorporate his proof concerning collective application of the reduction criterion and for helpful comments. We are also grateful to N. J. Cerf and R. M. Gingrich for information on their numerical results, which contributed to eliminating an error that appeared in an earlier version of this paper. P.H. acknowledges the Elsag-Bailey–I.S.I. Foundation Research Meeting on Quantum Computation. The work was supported by the Polish Committee for Scientific Research under Contract No. 2 P03B 024 12, and by the Foundation for Polish Science.

APPENDIX

Here we will prove that the positive map Λ given by Eq. (7) is decomposable; i.e., it can be written in the form [28]

$$\Lambda=\Lambda_1^{CP}+T\Lambda_2^{CP}, \tag{A1}$$

where Λ_i^{CP} are CP maps and T is the transpose. In fact, we will see that the map is trivially decomposable, i.e., it is of the form $\Lambda=T\Lambda^{CP}$. To prove the above we need the lemma establishing one-to-one correspondence between CP maps $\Lambda:M_N\rightarrow M_N$ and positive matrices (operators) belonging to tensor product $M_N\otimes M_N$ (this is analogous to the fact that positive maps are equivalent to the matrices in $M_N\otimes M_N$, which are positive in product vectors [46,19]).

Lemma. A linear map $\Lambda:M_N\rightarrow M_N$ is completely positive if and only if the operator $D\in M_N\otimes M_N$ given by

$$D=(I\otimes\Lambda)P_+ \tag{A2}$$

is positive [here P_+ is given by Eq. (28)].

Proof. If Λ is CP, then, by the very definition of the CP map, the operator D is positive. Conversely, suppose that the operator D is positive. Then it can be written by means of its spectral decomposition

$$D=\sum_i \lambda_i|\psi_i\rangle\langle\psi_i| \tag{A3}$$

with nonnegative eigenvalues λ_i. Taking V_i such that $I\otimes V_i|\psi_+\rangle=|\psi_i\rangle$ (see Sec. VI), we obtain

$$D=\sum_i \lambda_i I\otimes V_i P_+ I\otimes V_i^\dagger. \tag{A4}$$

Comparing this formula with Eq. (A2) and noting that Λ is uniquely determined by this equation, we obtain that it is given by

$$\Lambda(\sigma)=\sum_i W_i\sigma W_i^\dagger, \tag{A5}$$

where $W_i=\sqrt{\lambda_i}V_i$. However, this is the general form of completely positive maps [26]. This ends the proof of the lemma.

Remark. The lemma also holds for $\Lambda:M_N\rightarrow M_K$ with $N=K$. Then the P_+ belongs to $M_N\otimes M_N$ and the operator D belongs to $M_N\otimes M_K$.

Consider now the map of interest given by $\Lambda(\sigma)=I\,\mathrm{Tr}\,\sigma-\sigma$. The corresponding operator D [by Eq. (8)] is given by

$$D=(P_+)_A\otimes I-P_+, \tag{A6}$$

where $(P_+)_A$ is the reduction of the state P_+ so that $(P_+)_A=(1/N)I$. Consider now the partial transpose of B. It can be checked that D^{T_B} is of the form

$$D^{T_B}=\frac{1}{N}(I\otimes I-V), \tag{A7}$$

where V is the operator [9] defined by $V\psi\otimes\phi=\phi\otimes\psi$ for any vectors $\phi,\psi\in C^N\otimes C^N$. As $V^2=I\otimes I$ we obtain that V has eigenvalues ±1 so that $I\otimes I-V$ is a positive operator. Thus we see that D^{T_B} is a positive operator. However, we have $D^{T_B}=(I\otimes T\Lambda)P_+$. Then by the lemma the map $\Gamma=T\Lambda$ is CP. Consequently, we obtain

$$\Lambda=T\Gamma, \tag{A8}$$

which ends the proof. Of course, Λ can be also written as $\Lambda=\Gamma' T$ with completely positive Γ'. Indeed, as Γ is CP, then it is of the form $\Gamma(\sigma)=\Sigma_i V_i\sigma V_i^\dagger$. Hence

$$\begin{aligned}T(\Gamma(\sigma))&=\sum_i (V_i\sigma V_i^\dagger)^T=\sum_i (V_i^T)^\dagger\sigma^T V_i^T=\sum_i \tilde{V}_i\sigma^T\tilde{V}_i^\dagger\\ &\equiv\Gamma'(T(\sigma))\end{aligned} \tag{A9}$$

with $\tilde{V}_i=(V_i^T)^\dagger$. Thus Γ' is completely positive.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935); E. Schrödinger, Naturwissenschaften **23**, 807 (1935); J. S. Bell, Physics (N.Y.) **1**, 195 (1964).

[2] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989); P. Shor, SIAM J. Comput. **26**, 1484 (1997).

[3] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[5] K. Mattle, H. Weinfurter, P. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[6] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[7] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Elbl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997); D. Boschi, S. Brance, F. de Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[8] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

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

[10] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[11] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

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

[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).

[14] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).

[15] R. Horodecki and P. Horodecki, Phys. Lett. A **194**, 147 (1994).

[16] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **210**, 377 (1996).

[17] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996).

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

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

[20] Throughout this paper the $N\times M$ system means the system described by the Hilbert space $C^N\otimes C^M$ so that, e.g., a 2×2 system corresponds to the two-spin-$\frac{1}{2}$ or, in general, two two-level (two-qubit) one.

[21] N. Gisin, Phys. Lett. A **210**, 151 (1996).

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

[23] This result can be immediately generalized to cover the 2×3 case.

[24] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998); P. Horodecki, Phys. Lett. A **232**, 333 (1997).

[25] G. Lindblad, Commun. Math. Phys. **40**, 147 (1975); W. F. Stinespring, Proc. Am. Math. Soc. **26**, 211 (1955).

[26] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Wiley, New York, 1991).

[27] P. Busch and J. Lahti, Found. Phys. **20**, 1429 (1990); A. Sanpera, R. Tarrach, and G. Vidal, e-print quant-ph/9707041.

[28] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).

[29] A. Kossakowski (private communication).

[30] After completion of the first version of this manuscript, we received information that this condition was independently derived and discussed in Ref. [31].

[31] N. J. Cerf, C. Adami, and R. M. Gingrich, e-print quant-ph/9710001.

[32] This is in agreement with the numerical evidence obtained by N. Cerf and R. Gingrich (private communication).

[33] S. Popescu, Phys. Rev. Lett. **72**, 797 (1994).

[34] Quite recently, B. Terhal (e-print quant-ph/9810091) introduced a new positive map, which has a structure similar to our map but produces a criterion *independent* of the Peres one. Such criteria allow us to explore the region of bound entanglement [24].

[35] E. Rains (private communication).

[36] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).

[37] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[38] P. W. Shor and J. A. Smolin, e-print quant-ph/9604006; D. DiVincenzo, P. W. Shor, and J. A. Smolin, Phys. Rev. A **57**, 830 (1998).

[39] E. M. Rains, e-print quant-ph/9707002.

[40] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[41] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **44**, 535 (1991).

[42] R. Horodecki, M. Horodecki, and P. Horodecki, Phys. Lett. A **222**, 21 (1996).

[43] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).

[44] N. D. Mermin (unpublished); S. Popescu, in *The Dilemma of Einstein, Podolsky and Rosen—60 Years After*, edited by A. Mann and M. Revzen (IOP, Bristol, 1996); S. Teufel, K. Brendl, D. Dürr, S. Goldstein, and N. Zanghí, Phys. Rev. A **56**, 1217 (1997); M. Żukowski, R. Horodecki, M. Horodecki, and P. Horodecki, *ibid.* **58**, 1694 (1998).

[45] P. Shor and R. Laflamme, Phys. Rev. Lett. **78**, 1600 (1997); E. Rains, e-print quant-ph/9611001; IEEE Trans. Inf. Theory (to be published); *ibid.* **44**, 1388 (1998) (also available as e-print quant-ph/9612015).

[46] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).