Characterization of separable states and entanglement witnesses

M. Lewenstein,[1] B. Kraus,[2] P. Horodecki,[3] and J. I. Cirac[2]
[1]*Institute for Theoretical Physics, University of Hannover, Hannover, Germany*
[2]*Institute for Theoretical Physics, University of Innsbruck, A-6020 Innsbruck, Austria*
[3]*Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-952 Gdańsk, Poland*
(Received 25 May 2000; published 20 March 2001)

We provide a canonical form of mixed states in bipartite quantum systems in terms of a convex combination of a separable state and a so-called edge state. We construct entanglement witnesses for all edge states, which allows us to introduce a canonical form of nondecomposable entanglement witnesses and the corresponding positive maps. We also present a nontrivial necessary condition for entanglement witnesses and positive maps to be extremal.

DOI: 10.1103/PhysRevA.63.044304 PACS number(s): 03.67.Hk, 03.65.Ta, 03.65.Ca

One of the most fundamental open problems of quantum mechanics is the characterization and classification of mixed entangled states of multipartite systems, i.e., states that exhibit quantum correlations [1]. This problem is of enormous importance for applications in quantum information processing [2–5]. A density operator $\rho \geqslant 0$ acting on a finite Hilbert space $H = H_A \otimes H_B$ describing the state of two quantum systems A and B is called entangled [6] (or not separable) if it *cannot* be written as a convex combination of product states, i.e., as

$$\rho = \sum_k p_k |e_k, f_k\rangle\langle e_k, f_k|, \tag{1}$$

where $p_k \geqslant 0$, and $|e_k, f_k\rangle \equiv |e_k\rangle_A \otimes |f_k\rangle_B$ are product vectors. Conversely, ρ is separable (or not entangled) if it can be written in the form (1).

For low-dimensional systems (in $H = \mathbb{C}^2 \otimes \mathbb{C}^2$ and $H = \mathbb{C}^2 \otimes \mathbb{C}^3$), there exists an operationally simple necessary and sufficient condition for separability, the so-called Peres-Horodecki criterion [7,8]. It indicates that a state ρ is separable if and only if (iff) its partial transpose is positive, where the partial transpose means the transpose with respect to one of the subsystems [9]. However, in higher dimensions this is only a necessary condition; that is, there exist entangled states whose partial transpose is positive (PPTES's) [10–12]. Thus, the separability problem reduces to finding whether a density operator with positive partial transpose is separable or not [1].

There exists a complete characterization of separable states based on entanglement witnesses (EW's) and positive maps (PM's) [8]. Briefly speaking, a state ρ is entangled iff there exists a Hermitian operator W (an EW) such that $\mathrm{Tr}(W\sigma) \geqslant 0$ for all separable σ, but $\mathrm{Tr}(W\rho) < 0$. The latter condition offers the possibility of experimental detection of entanglement via the measurement of W—an observable that ''witnesses'' the quantum correlations in ρ [13]. Starting from EW's one can define PM's [14] that also detect entanglement. An example of a PM is transposition T [15,16], whose tensor extension $I \otimes T$ detects all non-PPT states. Unfortunately, the characterization of EW's and PM's is not known, and therefore the most challenging open questions are how to construct EW's in general, and finding the minimal set of them that allows detection of all entangled states. First steps toward answering these questions were accomplished in Ref. [13]. In Ref. [17] we extended these results, and presented a way of creating and optimizing entanglement witnesses starting from the so-called edge states. The methods that we used to prove most of our results were based on the technique of ''subtracting projectors on product vectors'' [18,19].

In this Brief Report we use the methods and results presented in Ref. [17] to present a canonical form for a nondecomposable EW (ND-EW) and the corresponding PM. We also provide a characterization of separable states using a special class of EW's that are related not necessarily to edge states, but to certain subspaces of H. Finally, we present a nontrivial necessary condition for ND-EW's and PM's to be extremal. In order to make this paper self-contained, we will review some of the results already presented in our previous paper [17]. We refer the reader to that reference for the technical details concerning those results.

We will denote by $K(\rho)$, $R(\rho)$, and $r(\rho)$ the kernel, range, and rank of ρ, respectively. Let us start by defining the edge states. An ''edge'' state δ is a PPTES such that, for all product vectors $|e,f\rangle$ and $\epsilon > 0$, $\delta - \epsilon |e,f\rangle\, \langle e,f|$ is not positive or does not have a PPT. Obviously, the ''edge'' states lie on the boundary between PPTES's and not-PPT states. In order to characterize them we use the following criterion [10,19].

Criterion. A PPTES δ is an ''edge'' state iff there exists no $|e,f\rangle \in R(\delta)$ such that $|e,f^*\rangle \in R(\delta^{T_B})$ [20].

Note that the edge states violate the range criterion of separability in an extreme manner [10,19]. They are of special importance since they are responsible for the entanglement contained in PPTES's. In order to see that we generalize the method of the best separable approximation [18] to the case of PPT states.

Proposition 1. Every PPTES ρ is a convex combination

$$\rho = (1-p)\rho_{\mathrm{sep}} + p\,\delta, \tag{2}$$

of some separable state ρ_{sep} and an edge state δ.

Note that in the decomposition (2) the weight p can be chosen to be minimal [i.e., there exists no decomposition of type (2) with a smaller p].

The decomposition (2) can be obtained using the method of subtracting projectors onto product states $|e,f\rangle \in R(\rho)$ such that $|e,f^*\rangle \in R(\rho^{T_B})$. One can show [18] that $\rho' \propto \rho - \lambda|e,f\rangle\langle e,f|$ is still a PPTES if $\lambda = \min\{1/(\langle e,f|\rho^{-1}|e,f\rangle), 1/[\langle e,f^*|(\rho^{T_B})^{-1}|e,f^*\rangle]\}$. Moreover, such an operation diminishes the rank of either ρ or ρ^{T_B}, or both. The construction of the optimal decomposition is a hard task, but construction of a decomposition with nonminimal p can be obtained in a finite number of steps. This provides us with a simple method to construct edge states in arbitrary dimensions, and a separability check [19].

It is natural to ask how to detect PPTES's, in view of the decomposition (2). As mentioned above, one approach is to use EW's. There exists a class of EW (called decomposable [17]) that have the form $W = P + Q^{T_B}$, where P and Q are positive operators. Such witnesses can detect only non-PPT entangled states [21]. The EW's that cannot be written as $W = P + Q^{T_B}$ are called nondecomposable EW's. An EW is nondecomposable iff it detects a PPTES [17]. In particular, every ND-EW detects an edge state since one can immediately see from Eq. (2) that if $\mathrm{Tr}(W\rho) < 0$ then $\mathrm{Tr}(W\delta) < 0$. Despite their importance, it is not known how to characterize the class of ND-EW's. It is thus an important task to study the EW's of the edge states.

One of the important results of this report is that for any edge state one can explicitly construct a ND-EW that detects it. To show that, we generalize the method of [13], which is restricted to PPTES's constructed out of unextendible product bases [11] which, in particular, do not exist for $(2\times N)$-dimensional systems. Let δ be an edge state, C an arbitrary positive operator such that $\mathrm{Tr}(\delta C) > 0$, and P and Q positive operators whose ranges satisfy $R(P) \subseteq K(\delta)$, $R(Q) \subseteq K(\delta^{T_B})$. We define

$$W_\delta \equiv P + Q^{T_B} \tag{3}$$

and

$$\epsilon \equiv \inf_{|e,f\rangle} \langle e,f|W_\delta|e,f\rangle, \quad c \equiv \sup_{|e,f\rangle} \langle e,f|C|e,f\rangle. \tag{4}$$

Note that the properties of δ ensure that $\epsilon > 0$. We then have the following lemma (Lemma 6 of Ref. [17]).

Lemma 1. Given an edge state δ, then

$$W_1 = W_\delta - \frac{\epsilon}{c} C \tag{5}$$

is a ND-EW that detects δ.

The simplest choice of P, Q, and C consists of taking the projections onto $K(\delta)$ and $K(\delta^{T_B})$ and the identity operator, respectively [23]. As we will see below, this choice provides us with a canonical form for ND-EW's. In order to show that, let us first introduce some additional notations.

Let $\mathcal{S} \subset \mathcal{P}$ denote the convex set (cone) of separable (PPT) states. Let $\mathcal{P}^\perp \subset \mathcal{S}^\perp$ be the convex sets (dual cones) of ND-EW's (EW's). All those sets are closed.

Definition. An EW (decomposable EW) W is *tangent* to $\mathcal{S}$ (to $\mathcal{P}$) if there exists a state $\rho \in \mathcal{S}$ ($\rho \in \mathcal{P}$) such that $\mathrm{Tr}(W\rho) = 0$. Furthermore, we say that W is tangent to $\mathcal{S}$ ($\mathcal{P}$) at $\rho \in \mathcal{S}$ ($\mathcal{P}$) if $\mathrm{Tr}(W\rho) = 0$.

Observation 1. The state ρ is separable iff, for all EW's tangent to $\mathcal{S}$, $\mathrm{Tr}(W\rho) \geq 0$.

Proof. For (only if) the proof is trivial. For (if), let ρ be an entangled state, and let W be an EW that detects ρ, i.e., $\mathrm{Tr}(W\rho) < 0$. We define $\epsilon \geq 0$ as in Eq. (4). If $\epsilon = 0$ then W is tangent to $\mathcal{S}$. If $\epsilon > 0$ then $W' = W - \epsilon \mathbb{1}$ is still an EW that detects the entanglement of ρ and it is tangent to $\mathcal{S}$.

Observation 2. If a decomposable EW W is tangent to $\mathcal{P}$ at ρ, then for any decomposition (2) W must also be tangent to $\mathcal{P}$ at the edge state δ.

We can now prove the following proposition.

Proposition 2. If an EW W that does not detect any PPTES's is tangent to $\mathcal{P}$ at some edge state δ, then it is of the form

$$W = P + Q^{T_B}, \tag{6}$$

where $P, Q \geq 0$ such that $R(P) \subseteq K(\delta)$, $R(Q) \subseteq K(\delta^{T_B})$.

Proof. As mentioned before, an EW W that does not detect any PPTES's must be decomposable; that is, $W = P + Q^{T_B}$. From the PPT property of δ and the positivity of P, Q we have that the ranges $R(\delta)$ and $R(P)$ [$R(\delta^{T_B})$ and $R(Q)$] must be orthogonal.

We are now in the position to prove one of the main results of this paper, regarding our canonical form of ND-EW's.

Proposition 3. Any ND-EW W has the form

$$W = P + Q^{T_B} - \epsilon \mathbb{1}, \quad 0 < \epsilon \leq \inf_{|e,f\rangle} \langle e,f|P + Q^{T_B}|e,f\rangle, \tag{7}$$

where P and Q fulfill the conditions of Proposition 2 for some edge state δ [24].

Proof. Consider $W(\lambda) = W + \lambda \mathbb{1}$. Obviously, for some $\lambda > 0$, say λ_0, $W(\lambda_0)$ becomes decomposable (or positive). Note that, for any $\lambda < \lambda_0$, $W(\lambda)$ is nondecomposable and therefore it detects some PPTES ρ. Using continuity we conclude that $W(\lambda_0)$ is tangent to $\mathcal{P}$. From Observation 2 there exists an edge state δ to which $W(\lambda_0)$ is tangent. From Proposition 2 we obtain that $W(\lambda_0) = P + Q^{T_B}$, where P and Q satisfy the needed conditions, and consequently $W = P + Q^{T_B} - \epsilon \mathbb{1}$ with $\epsilon = \lambda_0$. Since W is an EW, ϵ must not be greater than $\inf_{|e,f\rangle} \langle e,f|P + Q^{T_B}|e,f\rangle$.

Proposition 3′. If the assumptions of Proposition 3 hold then W is of the form (7) with $R(P)$ and $R(Q)$ orthogonal to some Hilbert subspaces $\mathcal{H}^a$ and $\mathcal{H}^b$, respectively, where (i) there exists no $|e,f\rangle \in \mathcal{H}^a$ such that $|e,f^*\rangle \in \mathcal{H}^b$; (ii) $R[\mathrm{Tr}_B(P_{\mathcal{H}^a})] = R[\mathrm{Tr}_B(P_{\mathcal{H}^b})]$, $R[\mathrm{Tr}_A(P_{\mathcal{H}^a})] = R[\mathrm{Tr}_A(P_{\mathcal{H}^b})^*]$, where P_X stands for the projector onto the subspace X; (iii) $\dim \mathcal{H}^x > \max\{r[\mathrm{Tr}_A(P_{\mathcal{H}^x})], r[\mathrm{Tr}_B(P_{\mathcal{H}^x})]\}$, $x = a,b$.

Proof. The point (i) is clear; (ii) and (iii) follow from simple analysis of the ranges of the partial reductions of δ as well as the properties of the range of PPT states [22,19].

Remark 1. The formulation presented permits us to release ourselves from dealing with edge states in the canonical decomposition (7). Instead, we may consider only the pairs of ''strange'' subspaces $H^{a,b}$ of the Hilbert space.

Remark 2. It is worth recalling that all EW's are in one-to-one correspondence to PM's [14]. In particular, any ND-EW leads to a so-called nondecomposable positive map (ND-PM), i.e., a map that cannot be written as a convex sum of a completely positive map and some other completely positive map followed by transposition. The characterization of ND-PM's is one of the most challenging open problems in mathematical physics. Proposition 3 ($3'$) thus provides us with a canonical form for ND-PM's. As we mentioned, a PM Λ (transforming operators acting on $\mathcal{H}_C$ to those acting on $\mathcal{H}_B$) provides a separability test that is stronger than its EW counterpart W_Λ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$. The correspondence between such a PM and EW is given by the following relation: if $|\Psi\rangle = \Sigma_{k=1}^{d_A} |k\rangle_A \otimes |k\rangle_C$ then $W_\Lambda = \mathbb{1}_A \otimes \Lambda(|\Psi\rangle\langle\Psi|)$.

As mentioned above, when studying separability we just have to deal with ND-EW's. In order to reduce the set of ND-EW's and ND-PM's, let us introduce the following definitions. Given two ND-EW'sW_1 and W_2, then we say that W_2 is ND finer than W_1 if all the PPTES's detected by W_1 are also detected by W_2. We say that W is a nondecomposable optimal EW (ND-OEW) if there exists no ND-EW that is ND finer than W. Thus it is obvious that the ND-EW's we are interested in are the ND-OEW's. Let us call an operator $D = P + Q^T$, with $P, Q \geqslant 0$ and T denoting the partial transposition with respect to A or B, decomposable. Furthermore let us define the set of product vectors on which the expectation value of W vanishes, i.e., $p_W = \{|e,f\rangle \in H$, such that $\langle e,f|W|e,f\rangle = 0\}$. This set plays an important role in the optimization, which can be seen in the following results concerning the characterization of ND-OEW's.

Proposition 4 (Theorem 1b of Ref. [17]). A ND-EW W is ND optimal iff for all decomposable operators D and $\epsilon > 0$ the operator $W' = W - \epsilon D$ is not an EW.

Corollary. If both p_W as well as p_{W^T} span the whole Hilbert space $H_A \otimes H_B$, then W is a ND-OEW.

Remark 3. The necessary and sufficient conditions for a ND-EW to be ND optimal are presented in Ref. [17]. Loosely speaking a ND-EW is ND optimal iff either both p_W and p_{W^T} span the whole Hilbert space, or there exist some nonproduct vectors $|\Psi\rangle$ related to p_W (or p_{W^T}) such that both p_W (p_{W^T}) jointly with the set of $|\Psi\rangle$ and p_{W^T} (p_W) span the whole $H_A \otimes H_B$. In our numerical studies, however, we have not encountered the latter possibility; it is thus likely that the converse of the Corollary is true.

Our results allow us now to design a finite-step algorithm to ND-optimize a given EWW, by subtracting decomposable operators.

(I) Take a decomposable operator $D = P + Q^T$ such that $P p_W = 0$ and $Q p_{W^T} = 0$ and check if

$$\lambda_0 \equiv \inf_{|e\rangle \in H_A} [D_e^{-1/2} W_e D_e^{-1/2}]_{\min} > 0. \tag{8}$$

Here $W_e = \langle e|W|e\rangle$, $D_e = \langle e|D|e\rangle$, where $|e\rangle \in H_A$, whereas $[X]_{\min}$ is the minimal eigenvalue of X.

(II) If λ_0 is positive construct the new ND finer EW $W' = W - \lambda_0 D$.

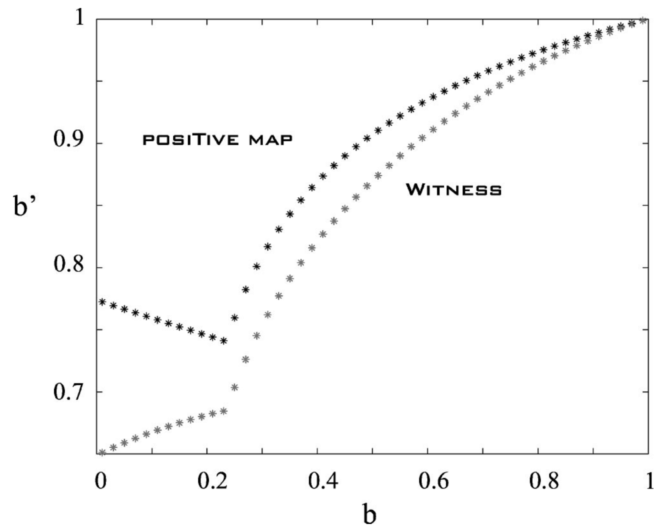

FIG. 1. Values of b' for which if $\overline{b} \leqslant b' \overline{\rho_{\tilde{b}}}$ is detected by the optimal witness and the positive map obtained from $\tilde{\rho}_b$.

(III) Iterate the procedure (I) and (II) as long as there is no $D = P + Q^T$ with $P p_W = 0$ and $Q p_{W^T} = 0$.

After each step the set of p_W, p_{W^T} (or both of them) increases at least by one element. This new element will not be in $K(P)$ [or in $K(Q)$, or in both], which automatically implies that it will be linearly independent of either the elements of p_W, p_{W^T} or both. So, after a finite number of steps p_W and p_{W^T} will span the whole Hilbert space, which ensures that the final ND-EW is ND optimal. In principle, it may happen that $\lambda_0 = 0$ at some step, before p_W and p_{W^T} span the whole H. Our numerical simulations suggest, however, that among all possible D's one can always find one with $\lambda_0 > 0$.

We have applied the methods of finding and optimizing EW's to a family $\rho_b (b \in [0,1])$ of PPTES's in the (2×4)-dimensional system from Ref. [10]. For $b = 0,1$ those states are separable, whereas for $0 < b < 1$ the ρ_b's are edge states, which can be checked directly as shown in Ref. [10]. We have applied the following procedure. By virtue of some symmetries of ρ_b, one can perform a local change of basis after which the transformed state $\tilde{\rho}_b$ fulfills $\tilde{\rho}_b^{T_B} = \tilde{\rho}_b$. This step allowed us to construct the ND-EW $W_1 = P + P^{T_B} - \lambda_0 \mathbb{1}$, where P is the projector on $K(\tilde{\rho}_b)$, which already detects the edge state. Following the procedure above we subtracted decomposable operators. In addition we chose them to be invariant under partial transposition with respect to system B. Note that then $W = W^{T_B}$ at any step and therefore we only had to make sure that p_W spanned the whole Hilbert space, which automatically ensured that the final ND-EW was ND optimal. In Fig. 1 we show how many members of the whole family of $\rho_{b'}$'s are detected by the ND-OEW obtained from ρ_b. We plot here also the efficiency of the corresponding ND-PM. Here the improvement of efficiency is less spectacular, but still significant.

It must be stressed that both the EW's and the PM's constructed in a 2×4 system are examples for a quantum system with a one-qubit subsystem. We have also provided examples of the set p_W that spans the whole Hilbert space. This set allows us to construct very peculiar separable states of full rank that lie on the boundary of $\mathcal{S}$. Note also that, in general, the parameter λ_0 in the optimization procedure has to be found numerically. In Ref. [17] we were able to formulate an analytic method that allows one to detect the whole family of ρ_b's.

As we remember, the key problem is to find the minimal set of EW's detecting a PPTES. Obviously, this minimal set will consist of ND-OEW's. A related problem is to find a set of extremal points of $\mathcal{P}^{\perp}$. Note that a nonoptimal ND-EW is a convex sum of an optimal one and a decomposable operator (Proposition 4), so it cannot be an extremal point. Note that Proposition 3 ($3'$) combined with the optimality property provides the necessary form of extremal points of EW's as well as PM's. We have thus the following proposition.

Proposition 5. The set of extremal points of the set of EW's, $\mathcal{S}^{\perp}$, is contained in the set $\mathcal{A}$ of all optimal EW's of the form (7) plus projectors and transposed projectors.

Proposition 5'. The set of extremal points of the cone of ND-EW's, $\mathcal{P}^{\perp}$, is contained in the set $\mathcal{B}$ of all optimal ND-EW's of the form (7).

Remark 4. Moreover, applying the isomorphism [14] to the members of $\mathcal{A}$ ($\mathcal{B}$) we obtain the set $\mathcal{A}'$ ($\mathcal{B}'$) of PM's (ND-PM's) containing the set of all extreme PM's. The above theorems thus provide the first nontrivial necessary condition for EW's and PM's to be extremal. In particular, following Proposition $3'$ we can obtain a weaker condition by considering optimal EW's of the form (7) without involving the notion of the edge states, but only pairs of ''strange'' subspaces $\mathcal{H}^a$ and $\mathcal{H}^b$.

This work was supported by the DFG (SFB 407 and Schwerpunkt ''Quanteninformationsverarbeitung''), the DAAD, the ÖFW (SFB ''Control and Measurement of Coherent Quantum Systems''), the ESF PESC Program on Quantum Information, the TMR network Grant No. ERB-FMRX-CT96-0087, the IST Program EQUIP, and the Institute for Quantum Information GmbH.

[1] M. Horodecki, P. Horodecki, and R. Horodecki, in *Quantum Information—Basic Concepts and Experiments*, edited by G. Alber and M. Weiner (Springer, Berlin, in press).

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

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

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

[5] For a review, see A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996); A. Steane, Rep. Prog. Phys. **61**, 117 (1998).

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

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

[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 8 (1996).

[9] Given an operator X and an orthonormal basis $\{|k\rangle\}_{k=1}^{N} \in H_B$, one defines the partial transpose of X with respect to B in that basis as follows: $X^{T_B} = \Sigma_{k,k'=1}^{N} |k'\rangle_B\langle k|X|k'\rangle_B\langle k|$. One can analogously define the partial transpose of X with respect to A in a given basis X^{T_A}. Partial transposition satisfies the useful property $\mathrm{tr}(X^{T_B}Y) = \mathrm{tr}(XY^{T_B})$. We say that a positive operator has a positive partial transposition if $\rho^{T_B} \geqslant 0$. Note that this property is basis independent.

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

[11] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).

[12] Such states provide examples of the so-called bound entangled states; see M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[13] B. M. Terhal, Lin. Algebr. Appl. **323**, 61 (2000); see also Phys. Lett. A **271**, 319 (2000).

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

[15] E. Störmer, Acta Math. **110**, 233 (1963).

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

[17] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

[18] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998); A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).

[19] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000); P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac, *ibid.* **62**, 032310 (2000).

[20] According to this criterion, if ρ is separable then there must exist a set of product vectors $\{|e_k, f_k\rangle\}$ that spans the range $R(\rho)$ such that the set of partial complex-conjugated product states $\{|e_k, f_k^*\rangle\}$ spans the range of ρ^{T_B}; see [10].

[21] Optimal decomposable EW's can be shown to have the form of the partial transpose of a positive operator whose range does not contain any product vector; see [17].

[22] P. Horodecki, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, e-print quant-ph/9910122.

[23] This choice applied to the entangled states of Ref. [11] reproduces the witnesses constructed in Ref. [13].

[24] Note that we could replace the identity operator in Eq. (7) by other decomposable operators.