Separability, entanglement, and full families of commuting normal matrices

Jan Samsonowicz,[1,*] Marek Kuś,[2,†] and Maciej Lewenstein[3,‡]
[1]*Faculty of Mathematics and Information Science, Warsaw University of Technology, Pl. Politechniki 1, 00-61 Warszawa, Poland*
[2]*Center for Theoretical Physics, PAS, Aleja. Lotników 32/46, 02-668 Warszawa, Poland*
[3]*Institut de Ciències Fotòniques, ICREA and ICFO, Parc Mediterani de la Tecnologia, Castelldefels, 08860 Spain*
(Received 4 May 2007; published 15 August 2007)

We reduce the question of whether a given quantum mixed state is separable or entangled to the problem of existence of a certain full family of commuting normal matrices whose matrix elements are partially determined by components of the pure states constituting a decomposition of the considered mixture. The method reproduces many known entanglement and/or separability criteria, and provides yet another geometrical characterization of mixed separable states.

DOI: 10.1103/PhysRevA.76.022314 PACS number(s): 03.67.Mn, 03.65.Ud

I. INTRODUCTION

A. Entanglement and separability problem

Entanglement is the most important quantum phenomenon, responsible for genuine, distinct, and unique properties of the quantum world, and the possibilities this world offers for future technological applications, such as quantum engineering and quantum information [1]. Despite enormous efforts, many fundamental questions concerning entanglement remain open (for excellent recent reviews, see [2,3] for some general geometric settings of the problem). In a seminal paper in 1989 Werner [4] gave the definition of a separable (i.e., nonentangled) state: a state of a bipartite system is separable if and only if it is a mixture of pure product states. The simple question as to whether a given state is separable or not is known as the *separability problem*. Only in very rare instances do we know operational sufficient and necessary criteria (SNCs) that allow us to solve this problem.

(a) For 2×2 (two-qubit) and 2×3 (qubit-qutrit) systems, the SNCs are given by the positive definiteness of the partial transform [5]; this is the famous positive partial transform (PPT) criterion, introduced by Peres as necessary for separability in Ref [6].

(b) For three-qubit symmetric ("bosonic") states, the PPT criterion also represents the SNCs [7].

(c) For continuous-variable 1×1 (one mode per party) Gaussian states, the PPT criterion (formulated at the level of correlation matrices) is a SNC [8,9].

(d) For continuous-variable $m\times n$ (all bipartite) Gaussian states, there exists an operational SNC based on recursion for correlation matrices [10].

(e) For continuous-variable tripartite $1\times 1\times 1$ Gaussian states, there exists an operational SNC based on "iteration" of the PPT condition for correlation matrices [11].

In general, we have to rely on either only necessary criteria, or only sufficient ones, or numerical approaches. Although there exist very efficient numerical procedures that employ optimization methods of semidefinite programming [12], the complexity of the problem grows with the dimensionality of the underlying Hilbert spaces: in fact it has been proven that the problem belongs to the complexity *NP* class [13].

B. Reformulations of the separability problem

The market for only necessary or only sufficient criteria is growing constantly, and it is impossible to review it in a non-review-style paper (for this reason, we recommend to the readers the review [2]). There are also many attempts to reformulate the problem of separability in different mathematical terms. A paradigmatic example for such an approach is the formulation of the separability problem in terms of positive maps due to Horodecki *et al.* [5]. A state is entangled if and only if there exists a positive map acting on, say, Alice, such that, when applied to the state in question, it produces a nonpositive definite operator. A similar approach deals with entanglement witnesses, i.e., observables that have positive averages on all separable states, but a negative average on some entangled state: A state is entangled if and only if there exists a witness operator that detects it, i.e., has a negative average. Obviously, neither of these approaches is operational, but nevertheless they are extremely useful, since they allow the generation of many necessary separability (sufficient entanglement) criteria via explicit construction of positive maps [14] and witnesses [15], and methods of their (local) measurements (see [16]).

We have recently presented another example of the reformulation of the separability problem employing harmonic analysis on compact groups [17]. In this approach, quantum mechanical states are replaced by noncommutative characteristic functions defined on the considered group, and the separability problem reduces to the question of whether a characteristic function defined on a product group of two groups can be represented as a mixture of products of characteristic functions on each of the individual groups. The present paper is in a sense similar to Ref. [17]: we present yet another reformulation of the separability problem, and reduce it to the apparently unrelated question of the existence of a *full* (in a sense specified below) *family of commuting normal matrices*, whose matrix elements are partially determined by components of the pure states that constitute a decomposition of the considered mixed state.

*J.Samsonowicz@alpha.mini.pw.edu.pl
†Marek.Kus@cft.edu.pl
‡Maciej.Lewenstein@icfo.es

C. Decompositions of mixed states

A given genuine (not pure) mixed state ρ has an infinite number of decompositions in terms of projectors onto pure states. This fact was already recognized by Schrödinger in 1935 [18], and elaborated thoroughly from a more modern point of view by Hughston *et al.* [19]. Any decomposition of a density matrix of rank r into K projectors can be described in terms of a rectangular $K\times r$ matrix, whose r columns are orthonormal. Such objects are known in geometry to form a so-called $V_{K,r}=U(K)/U(K-r)$ Stiefel manifold [20]. The separability problem might also be formulated as a problem of statistical mechanics of a fictitious system on the Stiefel manifold, characterized by a positive definite Hamiltonian (cost function) that vanishes for separable states [21]. Here, we follow another avenue: we consider all decompositions of ρ into K terms for sufficiently large K. Such decompositions are related via unitary transformations $U(K)$. The matrix elements of the density matrix, on the other hand, form a Gram matrix of scalar products of certain vectors from this K-dimensional space. Section II of the paper is thus devoted to the study of such Gram decompositions. It provides complementary results to those of Ref. [19].

D. Plan of the paper

As stated above, Sec. II is devoted to the Gram decompositions, and its main result is Theorem 1, which describes how the two different Gram decompositions are connected. We present a reformulation of the separability problem in Sec. III, in Theorem 2. Here, an example of so-called Werner matrices [4] is elaborated in detail. Section IV contains the main result of this paper: a SNC (unfortunately not operational) for separability in terms of the existence of what we call a full family of commuting normal matrices (FFCNM) (Theorem 3). We specify this result for the particularly simple case of $2\times N$ systems, where the separability SNC requires existence of a single normal matrix, whose matrix elements are partially known. Here, we use the general properties of the density matrices in $2\times N$ systems (as presented in Appendix B) and formulate elegant theorems for the existence of normal extensions of partially known matrices, based on earlier and some additional results for 2×2, and 2×3 systems. We discuss also application of our criterion to PPT entangled states of rank 5 in 2×4 systems. We relate these results to the theory of generalized concurrence [22].

II. GRAM DECOMPOSITIONS OF DENSITY MATRICES

A. Decompositions of density matrices

Physical states of composite quantum systems are represented by density matrices, i.e., Hermitian, positive definite linear operators of trace 1, acting in the Hilbert space $\mathcal{H}=\mathcal{H}_A\otimes\mathcal{H}_B\otimes\cdots$, which is a tensor product of Hilbert spaces corresponding to subsystems $A,B,\ldots$ of the considered system. In the following, we shall be concerned with states of bipartite systems in a finite-dimensional Hilbert space, i.e., a space described by positive definite Hermitian density matrices $\rho=\rho^\dagger\geq 0$ with $\mathrm{Tr}\,\rho=1$, acting on the Hilbert space of the composite system $\mathcal{H}=\mathcal{H}_A\otimes\mathcal{H}_B$. Without losing generality, we will assume that $\dim\mathcal{H}_A=M\geq 2$ and $\dim\mathcal{H}_B=N\geq M$, i.e., $\mathcal{H}=\mathbb{C}^M\otimes\mathbb{C}^N=\mathbb{C}^{M\times N}$. In the following, we shall use the notation $r(\rho)$ for the rank of the matrix ρ (which for a Hermitian matrix equals the number of its nonvanishing eigenvalues).

Performing the spectral decomposition of ρ, we have

$$\rho=\sum_{l=1}^{r}\lambda_l|\psi_l\rangle\langle\psi_l|, \tag{1}$$

where λ_l are (positive) eigenvalues of ρ, $|\psi_l\rangle$ its eigenvectors, and $r=r(\rho)$ its rank. Defining $|\Psi_l\rangle=\sqrt{\lambda_l}|\psi_l\rangle$, we thus decompose the nonnegative definite Hermitian matrix ρ as a sum of rank-1 operators,

$$\rho=\sum_{l=1}^{r}|\Psi_l\rangle\langle\Psi_l|. \tag{2}$$

The decomposition of (2) into the sum of rank-1 operators is nonunique. Indeed, the vectors

$$|\Phi_n\rangle=\sum_{l=1}^{r}W_{nl}|\Psi_l\rangle,\quad n=1,\ldots,K\geq r, \tag{3}$$

lead to another one,

$$\rho=\sum_{n=1}^{K}|\Phi_n\rangle\langle\Phi_n|, \tag{4}$$

involving $K\geq r$ components, provided that the rectangular $K\times r$ matrix W satisfies $W^\dagger W=I$, where I is the $r\times r$ identity matrix, i.e., W belongs to the $V_{K,r}$ manifold. In fact, all possible decompositions (4) of ρ into a sum of rank-1 operators can be obtained from the spectral decomposition of ρ (2) in such a way [18,19].

B. Gram decompositions

Let $\{|E_\nu\rangle\}_{\nu=1,\ldots,M\times N}$ be a basis in $\mathbb{C}^{M\times N}$. Starting from the spectral decomposition (2), we obtain for the matrix elements of ρ

$$\rho_{\mu\nu}=\langle E_\mu|\rho|E_\nu\rangle=\sum_{l=1}^{r}\langle E_\mu|\Psi_l\rangle\langle\Psi_l|E_\nu\rangle=\sum_{l=1}^{r}\bar{w}_\mu^l w_\nu^l=\langle w_\mu,w_\nu\rangle, \tag{5}$$

$$w_\nu:=\begin{bmatrix}w_\nu^1\\ w_\nu^2\\ \cdot\\ \cdot\\ \cdot\\ w_\nu^r\end{bmatrix}\in\mathbb{C}^r,\quad w_\nu^l:=\langle\Psi_l|E_\nu\rangle, \tag{6}$$

where $\langle\cdot,\cdot\rangle$ is the standard Hermitian scalar product in $\mathbb{C}^K$. It means that a Hermitian positive definite matrix is the Gram matrix (i.e., the matrix of scalar products) of the vectors w_ν defined above. We will call a set of vectors $\{w_\nu\}$ satisfying

(5) a Gram system for ρ, and we will say that it provides a Gram decomposition of ρ. If we do not insist that the vectors w_ν are elements of $\mathbb{C}^r$, we can construct other Gram decompositions of ρ, so in this sense the Gram decomposition is nonunique. Indeed, defining

$$w'_\nu = Vw_\nu, \tag{7}$$

where $w'_\mu \in \mathbb{C}^K$, with $K \geq r$ and $V \in \mathbb{M}_{K\times r}$, a rectangular matrix satisfying $V^\dagger V = I$, we have $\rho_{\mu\nu} = \langle w'_\mu, w'_\nu \rangle$. It is easy to prove that all Gram decompositions of the matrix ρ are obtained by the transformation (7) from the spectral one (2) and (6). In particular, two Gram systems calculated from two decompositions (2) and (4) are connected by the relation (7) with $V = \bar{W}$ [cf. (3)]. In the following, we will also use the fact that, if two sets of vectors w'_ν and w''_ν, $\nu = 1, \ldots, r$, $w'_\nu \in \mathbb{C}^K$, $w''_\nu \in \mathbb{C}^K$ are Gram systems for the same positive-definite matrix ρ, i.e., $\langle w'_\mu, w'_\nu \rangle = \langle w''_\mu, w''_\nu \rangle$, then there exists a unitary U acting in $\mathbb{C}^K$ such that $w''_\nu = Uw'_\nu$ for $\nu = 1, \ldots, r$.

C. Gram decomposition in bipartite systems

Let us now take advantage of the fact that ρ acts on a tensor product space, i.e., we chose the basis $\{|E_\nu\rangle\}_{\nu=1,\ldots,M\times N}$ in the form of product states $|E_\nu\rangle = |e_m\rangle \otimes |f_n\rangle =: |e_m \otimes f_n\rangle$, $m = 1, \ldots, M$, $n = 1, \ldots, N$, and repeat the calculation of (5),

$$\rho_{ij,mn} = \langle e_i \otimes f_j | \rho | e_m \otimes f_n \rangle = \sum_{l=1}^{r} \langle e_i \otimes f_j | \Psi_l \rangle \langle \Psi_l | e_m \otimes f_n \rangle$$

$$= \sum_{l=1}^{r} \bar{w}^l_{ij} w^l_{mn} = \langle w_{ij}, w_{mn} \rangle, \tag{8}$$

where now w_{mn}, $m = 1, \ldots, M$, $n = 1, \ldots, N$, are vectors in $\mathbb{C}^r$, with components

$$w^l_{mn} = \langle \Psi_l | e_m \otimes f_n \rangle. \tag{9}$$

If we assume that ρ is of maximal rank $r = MN$ (which for $M \geq 3$ we take for granted in the following), then w_{mn} are linearly independent. In particular, for any fixed $\tilde{m} \in \{1, \ldots, M\}$, $(\tilde{n} \in \{1, \ldots, N\})$ the vectors $w_{\tilde{m}n}$, $n = 1, \ldots, N$ $(w_{m\tilde{n}}$, $m = 1, \ldots, M)$ form a set of N (M) linearly independent vectors in $\mathbb{C}^K$, respectively. In the special case $M = 2$, the first of the latter statements can also be assumed to hold, provided ρ is (nontrivially) supported in the $2 \times N$ space. If this statement were not true, the density matrix ρ would have a product vector in its kernel. In such a situation, either ρ is entangled and not a PPT, or, if it is a PPT, then it can be represented as a mixture of a separable part and a density matrix supported in $[2 \times (N-1)]$-dimensional space (for proofs and details, see Ref. [24]).

D. Relations between various Gram decompositions

Let $\{v_n\}_{n=1,\ldots,N}$ form an arbitrary set of linearly independent vectors in $\mathbb{C}^K$ (in particular, in the light of the above remark, we can choose $v_n = w_{1n}$). We can always find a family of linear maps $F_m : \mathbb{C}^K \to \mathbb{C}^K$, $m = 1, \ldots, M$, such that

$$w_{mn} = F_m v_n. \tag{10}$$

Note that such F_m's are uniquely defined only on the N-dimensional subspace of $\mathbb{C}^K$ spanned by $\{v_n\}_{n=1,\ldots,N}$. If we apply the same procedure to the decomposition (4), we will arrive at

$$w'_{mn} = F'_m v'_n, \tag{11}$$

with v'_n, $n = 1, \ldots, N$, some linearly independent vectors in $\mathbb{C}^K$ and appropriate F'_m.

The vectors w_{mn} and w'_{mn} are connected by (7), i.e.,

$$F'_m v'_n = w'_{mn} = Vw_{mn} = VF_m v_n. \tag{12}$$

Since both sets $\{v_n\}$ and $\{v'_n\}$, $n = 1, \ldots, N$, are linearly independent in, respectively, $\mathbb{C}^r$ and $\mathbb{C}^K$, there exists a $K \times r$ matrix $\tilde{V}$ of maximal rank, such that $v'_n = \tilde{V} v_n$ for $n = 1, \ldots, N$. Consequently,

$$V^\dagger F'_m \tilde{V} v_n = V^\dagger V F_m v_n = F_m v_n, \tag{13}$$

where we used $V^\dagger V = I$. We have thus shown the following.

Theorem 1. For the two decompositions of the Gram vectors of the form (10) and (11) stemming from two decompositions of ρ into rank-1 operators of the form (2) and (4), there exist two $K \times r$ matrices $\tilde{V}$ and V, the former of rank r and the latter satisfying $V^\dagger V = I$, such that on the space spanned by (arbitrarily chosen) N linearly independent vectors $v_n \in \mathbb{C}^r$, the equality

$$V^\dagger F'_m \tilde{V} = F_m \tag{14}$$

holds.

Obviously $\tilde{V}$ depends on the choice of $\{v_n\}$. ■

III. SEPARABILITY PROBLEM

A. Gram decompositions for separable states

Our goal is to characterize Gram decompositions for density matrices of bipartite separable quantum systems. Recall that separable states defined on $\mathcal{H}_A \otimes \mathcal{H}_B$ systems are characterized as follows.

Definition 1. A state ρ is separable if and only if

$$\rho = \sum_{i=1}^{k} p_i \rho_i^A \otimes \rho_i^B, \tag{15}$$

where $\Sigma_i p_i = 1$, $p_i \geq 0$, whereas ρ_i^A and ρ_i^B are states on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

The above expression means that ρ can be written as a convex combination of product states.

To achieve the goal, observe that, by performing a decomposition of the type (2) for all matrices ρ_i^A and ρ_i^B in (15) and taking into account the positivity of the coefficients p_i, we obtain that a state ρ is separable if and only if it can be decomposed in the form of K rank-1 operators proportional to projections on simple tensors:

$$\rho = \sum_{k=1}^{K} |\varphi_k\rangle\langle\varphi_k| \otimes |\psi_k\rangle\langle\psi_k| = \sum_{k=1}^{K} |\varphi_k \otimes \psi_k\rangle\langle\varphi_k \otimes \psi_k|, \tag{16}$$

where $|\varphi_k\rangle \in \mathcal{H}_A$, $|\psi_k\rangle \in \mathcal{H}_B$.

Calculating matrix elements of ρ in the local bases $\{|e_i\rangle\}_{i=1,\ldots,M}$ and $\{|f_i\rangle\}_{i=1,\ldots,N}$ in $\mathcal{H}_A = \mathbb{C}^M$ and $\mathcal{H}_B = \mathbb{C}^N$, respectively, we obtain

$$\rho_{ij,mn} = \langle e_i \otimes f_j|\rho|e_m \otimes f_n\rangle = \sum_{l=1}^{K} \langle e_i|\varphi_l\rangle\langle f_j|\psi_l\rangle\langle\varphi_l|e_m\rangle\langle\psi_l|f_n\rangle$$

$$= \sum_{l=1}^{K} \bar{w}'^{l}_{ij} w'^{l}_{mn} = \langle w'_{ij}, w'_{mn}\rangle, \tag{17}$$

where now

$$w'_{mn} = \begin{bmatrix} w'^{1}_{mn} \\ w'^{2}_{mn} \\ \vdots \\ w'^{K}_{mn} \end{bmatrix} = \begin{bmatrix} \varphi_1^m \psi_1^n \\ \varphi_2^m \psi_2^n \\ \vdots \\ \varphi_K^m \psi_K^n \end{bmatrix} = \begin{bmatrix} \varphi_1^m & & & \\ & \varphi_2^m & & \\ & & \ddots & \\ & & & \varphi_K^m \end{bmatrix} \begin{bmatrix} \psi_1^n \\ \psi_2^n \\ \vdots \\ \psi_K^n \end{bmatrix}$$

$$= D_m v'_n, \tag{18}$$

$$\phi_l^m := \langle\varphi_l|e_m\rangle, \quad \psi_l^n := \langle\psi_l|f_n\rangle. \tag{19}$$

B. Reformulation of the separability problem

From (18) it is thus clear that, for a separable state ρ on $\mathbb{C}^M \otimes \mathbb{C}^N$ which can be decomposed into the sum of K rank-1 product operators (16), there exist $D_m \in \mathbb{M}_{K\times K}$, $m=1,\ldots,M$, D_m diagonal, and $v'_n \in \mathbb{C}^K$, $n=1,\ldots,N$, such that

$$\rho_{ij,mn} = \langle D_i v'_j, D_m v'_n\rangle. \tag{20}$$

Equation (20) is also a sufficient condition for separability, i.e., if there exist $v'_n \in \mathbb{C}^K$, $n=1,\ldots,N$, and diagonal $D_m \in \mathbb{M}_{K\times K}$, $m=1,\ldots,M$, such that (20) is satisfied, then ρ can be decomposed into rank-1 separable states (16) with

$$|\varphi_l\rangle = \sum_{m=1}^{M} \overline{(D_m)_{ll}}|e_m\rangle, \tag{21}$$

$$|\psi_l\rangle = \sum_{n=1}^{N} \overline{(v_n)_l}|f_n\rangle, \tag{22}$$

i.e., ρ is separable.

Indeed, define

$$\tilde{\rho} = \sum_{l=1}^{K} |\varphi_l \otimes \psi_l\rangle\langle\varphi_l \otimes \psi_l|, \tag{23}$$

with φ_l and ψ_l defined by (21) and (22). Then $\tilde{\rho}$ is separable, and an elementary calculation shows that $\tilde{\rho}_{ij,mn} = \rho_{ij,mn}$, and thus $\rho = \tilde{\rho}$.

Summarizing, we can formulate thus the following theorem.

Theorem 2. A state ρ is separable if and only if there exists a Gram decomposition of ρ,

$$\rho_{ij,mn} = \langle w_{ij}, w_{mn}\rangle,$$

$w_{ij} \in \mathbb{C}^K$, for some K, such that

$$w_{ij} = D_i v_j,$$

with N vectors $\{v_1,\ldots,v_N\} \in \mathbb{C}^K$ and M diagonal matrices $D_1,\ldots,D_M$ acting as operators on $\mathbb{C}^K$ ■.

Observe that we can assume that all diagonal matrices D_i are nonsingular. Indeed, from (18) their diagonal elements are equal to the projections of the vectors $|\phi_l\rangle$, which constitute (a part of) the decomposition, onto the basis vectors $|e_m\rangle$. If any number of them vanish, we can always adjust the basis slightly to make them take nonzero values.

Invoking now Theorem 1 we obtain a corollary.

Corollary 1. A state ρ of the full rank $r=MN$ is separable if and only if, for some $K \geq MN$, there exist $K\times r$ matrices $\tilde{V}$ and V of which $\tilde{V}$ is of maximal rank and $V^\dagger V = I$, and diagonal $K\times K$ matrices $D_1,\ldots,D_M$, such that

$$V^\dagger D_m \tilde{V} = F_m$$

holds on the space spanned by v_n, $n=1,\ldots,M$, where $w_{mn} = F_m v_n$ is a Gram system (9) for ρ calculated from its spectral decomposition (2) ■.

Before proceeding, let us make a remark. Observe, namely, that in terms of the Gram decomposition (20) of a separable ρ, the operation of partial transposition in $\mathcal{H}_B$,

$$\rho = \sum_{i=1}^{k} p_i \rho_i^A \otimes \rho_i^B \mapsto \rho^{T_B} = \sum_{i=1}^{k} p_i \rho_i^A \otimes (\rho_i^B)^T, \tag{24}$$

i.e., $\rho_{ij,mn} \mapsto \rho_{in,mj}$, corresponds to the complex conjugation of the frame $\{v_1,\ldots,v_N\}$, i.e.,

$$\{v_1,\ldots,v_N\} \to \{\overline{v_1},\ldots,\overline{v_N}\}, \tag{25}$$

whereas a similar operation performed in $\mathcal{H}_A$,

$$\rho = \sum_{i=1}^{k} p_i \rho_i^A \otimes \rho_i^B \mapsto \rho^{T_A} = \sum_{i=1}^{k} p_i (\rho_i^A)^T \otimes \rho_i^B, \tag{26}$$

i.e., $\rho_{ij,mn} \mapsto \rho_{mj,in}$, consists in

$$\{D_1,\ldots,D_M\} \to \{\overline{D_1},\ldots,\overline{D_M}\}. \tag{27}$$

Indeed,

$$\rho^{T_B}_{ij,mn} = \rho_{in,mj} = \langle D_i v_n, D_m v_j\rangle = \langle v_n, \overline{D_i} D_m v_j\rangle = \overline{\langle \overline{D_i} D_m v_j, v_n\rangle}$$
$$= \langle D_i \overline{D_m v_j}, \overline{v_n}\rangle = \langle \overline{D_m} D_i v_j, \overline{v_n}\rangle = \langle D_i \overline{v_j}, D_m \overline{v_n}\rangle,$$

$$\rho^{T_A}_{ij,mn} = \rho_{mj,in} = \langle D_m v_j, D_i v_n\rangle = \langle v_j, \overline{D_m} D_i v_n\rangle = \langle v_j, D_i \overline{D_m} v_n\rangle$$
$$= \langle \overline{D_i} v_j, \overline{D_m} v_n\rangle,$$

where we used the fact that diagonal matrices commute and their Hermitian conjugation reduces to the complex one.

In Appendix A we discuss in detail the results of this section applied to an example of two-qubit states, the so-called Werner states.

IV. SEPARABILITY AND FULL FAMILIES OF COMMUTING NORMAL MATRICES

A. *K* separability and FFCNM

In forthcoming presentations, we will present applications of Corollary 1 to characterization of the bipartite entanglement for arbitrary systems. In the present paper, we would like to concentrate on the separability of systems with $M=2$, but before that we would like to use our results from the previous sections to formulate a SNC for separability. Let us assume that the investigated state ρ is K separable, i.e., there exists a decomposition into exactly K rank-1 product operators (16), and ρ can be cast in the form (20). Since we assumed that ρ is of maximal rank $r=NM$, we have necessarily $K \geq MN$. From the previous considerations, we now see that the Gram vectors calculated with the help of this decomposition have the form $w'_{mn}=D_m v'_n$.

For an arbitrary decomposition of ρ into exactly K states given by (4) (where $|\Phi_l\rangle$ need not be product states), we obtain another Gram system $w''^{l}_{mn}=\langle \Phi_l | e_m \otimes f_n \rangle \in \mathbb{C}^K$.

The vectors w'_{mn} and w''_{mn}, forming two Gram systems for the same matrix ρ, are connected via a unitary transformation

$$w''_{mn} = U w'_{mn} = U D_m v'_n. \tag{28}$$

Taking the above equality for two pairs of indices (m,n) and (k,n) we obtain

$$M_{mk} w''_{kn} = w''_{mn}, \tag{29}$$

where

$$M_{mk} = U D_m (D_k)^{-1} U^\dagger. \tag{30}$$

Remember that without losing generality we can assume nonsingularity of all matrices D_n. Consequently, M_{km} are also nonsingular.

B. SNC for separability and FFCNM

The matrices M_{nm} are normal, $[M_{km}, M_{km}^\dagger]=0$, and mutually commuting, $[M_{km}, M_{lm'}]=0$. Both observations can be easily proved using the facts that all matrices D_m are diagonal and U is unitary. The above reasoning is summarized in the form of the following theorem.

Theorem 3. A necessary and sufficient condition for K separability of ρ is the existence, for an arbitrary decomposition (4), of a full family of $M(M-1)/2$ normal, commuting, $K \times K$ matrices M_{km} satisfying (29), where w'_{mn} are appropriate Gram vectors for the decomposition (29).

Necessity of the condition follows from the above remarks, and to prove the sufficiency let us assume that (29) is satisfied for some family of normal, commuting matrices M_{km}. It is a standard fact from linear algebra [23] that all matrices in such a family can be simultaneously diagonalized by a single unitary transformation,

$$U^\dagger M_{km} U = D_{km}. \tag{31}$$

According to the previous remarks, we assume that M_{km} and, consequently, D_{km} are nonsingular. Now, from (29) and (31)

$$D_{km} U^\dagger w''_{mn} = U^\dagger M_{km} U U^\dagger w''_{mn} = U^\dagger M_{km} w''_{mn} = U^\dagger w''_{kn}, \tag{32}$$

and, defining $v_n := U^\dagger w''_{1n}$, $w_{kn} := U^\dagger w''_{kn}$, we obtain

$$w_{kn} = (D_{1k})^{-1} v_n. \tag{33}$$

The vectors w_{kn} are Gram vectors for ρ as they are obtained by a single unitary transformation from the vectors w''_{kn} constituting some Gram decomposition of ρ. Equation (32) reveals their structure in a form sufficient for the separability of ρ according to Theorem 2.

V. SEPARABILITY IN $2 \times N$ SYSTEMS AND NORMAL EXTENSIONS

Theorem 3 simplifies significantly for $2 \times N$ systems, because the FFCNM consists of a single matrix, which has to satisfy

$$\hat{M} w''_{0n} = w''_{1n}. \tag{34}$$

In the following we will use 0,1 instead of 1,2 for numbering the components on the qubit side, which is more in accord with the custom of denoting the basis states by $|0\rangle$ and $|1\rangle$. From here we do not need to assume the nonsingularity of ρ—see the remarks preceding the formula (10).

In this section we study the consequences of (34). On one hand, we use the present formulation to obtain particularly simple proofs of known separability criteria. On the other hand, we use known separability criteria to obtain nontrivial statements concerning the existence of normal extensions of matrices whose matrix elements are only partially known.

A. Canonical forms and PPT condition

Let us consider ρ in the canonical form [24] (see also Appendix B)

$$\rho = \begin{bmatrix} A & B \\ B^\dagger & I \end{bmatrix}, \tag{35}$$

where the positivity of ρ implies $A = BB^\dagger + \Lambda\Lambda^\dagger$, where Λ is some $N \times p$ matrix, with $p \geq r(\Lambda\Lambda^\dagger)$. Obviously, $p=1$ necessarily when $r(\Lambda\Lambda^\dagger)=1$; also, one can always take the minimal $p=r(\Lambda\Lambda^\dagger)=1$. We represent $\Lambda\Lambda^\dagger = \Sigma_{n=1}^{p} |\Lambda_n\rangle\langle\Lambda_n|$.

Similar considerations concern the partially transposed matrix, which reads

$$\rho^{T_A} = \begin{bmatrix} A & B^\dagger \\ B & I \end{bmatrix}. \tag{36}$$

We consider here only the nontrivial case of states with the positive partial transpose—states which are not PPT are not separable. The positivity of ρ^{T_A} requires now that $A = B^\dagger B + \hat{\Lambda}^\dagger \tilde{\Lambda}$, where $\tilde{\Lambda}$ is now a $\tilde{p} \times N$ matrix, with $\tilde{p} \geq r(\hat{\Lambda}^\dagger \tilde{\Lambda})$, and having analogous properties as p introduced above. We represent $\hat{\Lambda}^\dagger \tilde{\Lambda} = \Sigma'_{n=1} \tilde{p} |\hat{\Lambda}_n\rangle\langle\hat{\Lambda}_n|$. The PPT condition can thus be stated as $A - B^\dagger B \geq 0$. More precisely, it must hold that

$$A = BB^\dagger + \Lambda\Lambda^\dagger = B^\dagger B + \tilde{\Lambda}^\dagger\tilde{\Lambda}, \tag{37}$$

which implies that given Λ, $\tilde{\Lambda}$ are not independent, and are related by the above constraint.

Let us now discuss several examples to show how this entanglement SNC works.

Rank-N matrices. The results of Ref. [24] indicate that rank-N PPT states are N separable. The matrix $\hat{M}=B$ then, and $[B,B^\dagger]=0$.

The case $\rho=\rho^{T_A}$. From Ref. [24] we gather also that, when $\rho=\rho^{T_A}$, then ρ is $2N$ separable. In this case $B=B^\dagger$, $\Lambda=\hat{\Lambda}^\dagger$, and the matrix M can be written as

$$\hat{M} = \begin{bmatrix} B & \Lambda \\ \Lambda^\dagger & s \end{bmatrix}. \tag{38}$$

with $N\times N$ matrix S to be determined. Obviously, taking s Hermitian provides the desired normal extension of $\hat{M}$.

The case of 2×2 *and* 2×3 *systems*. In the two-qubit or qubit-qutrit case, every separable matrix is K separable, where $K=\max(r(\rho),r(\rho^{T_A}))$. In particular, for the full rank $r(\rho)=4$ $[r(\rho)=6]$, $K=4$ [26] or $K=6$ (as shown in Appendix B), respectively. We have then the following corollary.

Corollary 2. For $N=2,3$, an arbitrary $N\times N$ matrix B, and an arbitrary $p\times N$ matrix Λ constrained by (37), the matrix

$$\hat{M} = \begin{bmatrix} B & \Lambda \\ \tilde{\Lambda} & s \end{bmatrix} \tag{39}$$

has a normal extension, i.e., there exist a $p\times p$ matrix s and an $N\times p$ matrix $\tilde{\Lambda}$ constrained by (37) such that $\hat{M}$ is normal. This holds in particular for minimal $p=\min\{0, r(\rho)-N\}$.

B. Edge PPT entangled states for $N=4$

Perhaps the most interesting are applications for PPT entangled states, and in particular for the so-called edge states [24], i.e., PPT states that cannot be represented as a mixture of a PPT state and a separable states (no separable part can be subtracted). Such states are extreme examples of states to which the range criterion of Horodecki [27] applies. For $N=4$, such states may have rank 5 or 6 (and similarly their partial transpose). From the analysis of Appendix B we infer that, if ρ is a separable state of rank 5 such that its partial transpose has rank 5 (6), then it is 5 separable (6 separable). In the case $r(\rho)=r(\rho^{T_A})=5$, both Λ and $\tilde{\Lambda}$ have rank 1; we denote Λ by $|\Lambda\rangle$, and $\tilde{\Lambda}^\dagger$ by $|\tilde{\Lambda}\rangle$. We get then a further corollary.

Corollary 3. A PPT state ρ such that it and its partial transpose have rank 5 is separable, if and only if there exists a complex number s such that the matrix

$$\hat{M} = \begin{bmatrix} B & |\Lambda\rangle \\ \langle\tilde{\Lambda}| & s \end{bmatrix} \tag{40}$$

is normal, which, assuming that (37) holds, requires that

$$(B-s)|\tilde{\Lambda}\rangle = (B^\dagger - s^*)|\Lambda\rangle.$$

This condition is equivalent to the range criterion. For the particular example ρ_{97} of the 2×4 state analyzed in the seminal 1997 paper [27], it is very easy to analyze, as we show in Appendix C.

This analysis may be extended to the rank-5 states, with the partial transpose of rank 6, for which Eq. (37) becomes

$$BB^\dagger + |\Lambda\rangle\langle\Lambda^\dagger| = B^\dagger B + |\tilde{\Lambda}_1^\dagger\rangle\langle\tilde{\Lambda}_1| + |\tilde{\Lambda}_2^\dagger\rangle\langle\tilde{\Lambda}_2|. \tag{41}$$

We have in this case the following corollary.

Corollary 4. A PPT state ρ of rank 5, such that its partial transpose has rank 6, is separable, if and only if there exist complex numbers α and β, such that $|\alpha|^2+|\beta|^2=1$, and a 2×2 matrix s such that the matrix

$$\hat{M} = \begin{bmatrix} B & \alpha|\Lambda\rangle & \beta|\Lambda\rangle \\ \langle\tilde{\Lambda}_1| & s_{11} & s_{12} \\ \langle\tilde{\Lambda}_2| & s_{21} & s_{22} \end{bmatrix} \tag{42}$$

is normal, which, assuming that (41) holds, requires that

$$(B-s_{11})|\tilde{\Lambda}_1\rangle - s_{21}|\tilde{\Lambda}_2\rangle = (\alpha B^\dagger - \alpha s_{11}^* - \beta s_{12}^*)|\tilde{\Lambda}\rangle,$$

$$(B-s_{22})|\tilde{\Lambda}_2\rangle - s_{12}|\tilde{\Lambda}_1\rangle = (\beta B^\dagger - \alpha s_{21}^* - \beta s_{22}^*)|\tilde{\Lambda}\rangle.$$

Before we end this section, we would like to stress that obviously the above discussion of the normal extension of $\hat{M}$ applies also to $M\times N$ systems, if we focus on a single relation of the type (29), such as, say,

$$\hat{M}_{10}w''_{0n} = w''_{1n}. \tag{43}$$

The analysis pertains then to the study of separability on a particular $2\times N$ subspace of the full Hilbert space. In this sense, it is somewhat similar to the theory of generalized concurrences of Ref. [22].

VI. SUMMARY

We have presented an approach to the separability problem by reformulating it in terms of the existence of separable Gram decompositions of density matrices in auxiliary space. The existence of such Gram decompositions is equivalent to the existence of a full family of commuting normal matrices that relate components of Gram vectors. We have presented many examples and applications of this method, mainly to $2\times N$ systems. Several known separability criteria can be, on one hand, reproduced with this method in a particularly simple way, and, on the other, used to derive nontrivial statements about the existence of the FFCNM.

ACKNOWLEDGMENTS

We thank I. Cirac, F. Hulpke, Ph. Hyllus, J. Korbicz, B. Kraus, and A. Sanpera for helpful discussions. We acknowledge support of ESF PESC "QUDEDIS," EU IP "SCALA," the Spanish MEC (Grant No. FIS2005-04627 and Consolider Ingenio 2010 "QOIT"), and Polish Grant No. PBZ-Min-008/P03/03.

APPENDIX A: WERNER MATRICES FOR TWO QUBITS

As an example illustrating the results of Sec. III let us consider a one-parameter family of states for $N=M=2$,

$$\rho = \frac{1}{4}\begin{bmatrix} 1+p & 0 & 0 & 2p \\ 0 & 1-p & 0 & 0 \\ 0 & 0 & 1-p & 0 \\ 2p & 0 & 0 & 1+p \end{bmatrix}, \tag{A1}$$

the so-called Werner states [4]. The parameter p takes values from the interval $[0,1]$. One finds easily the spectral decomposition $\rho=\Sigma_{l=1}^{r}|\Psi_l\rangle\langle\Psi_l|$ with

$$|\Psi_1\rangle = \begin{bmatrix} 0 \\ \sqrt{\frac{1-p}{8}} \\ -\sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, \quad |\Psi_2\rangle = \begin{bmatrix} \sqrt{\frac{1-p}{8}} \\ 0 \\ 0 \\ -\sqrt{\frac{1-p}{8}} \end{bmatrix}, \quad |\Psi_3\rangle = \begin{bmatrix} 0 \\ \sqrt{\frac{1-p}{8}} \\ \sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, \quad |\Psi_4\rangle = \begin{bmatrix} \sqrt{\frac{1+3p}{8}} \\ 0 \\ 0 \\ \sqrt{\frac{1+3p}{8}} \end{bmatrix}, \tag{A2}$$

and calculates the Gram vectors (9)

$$w_{11} = \begin{bmatrix} 0 \\ \sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1+3p}{8}} \end{bmatrix}, \quad w_{12} = \begin{bmatrix} \sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, \quad w_{21} = \begin{bmatrix} -\sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, \quad w_{22} = \begin{bmatrix} 0 \\ -\sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1+3p}{8}} \end{bmatrix}. \tag{A3}$$

We chose $v_1=w_{11}$ and $v_2=w_{22}$ which allows us to take

$$F_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad F_2 = \begin{bmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\frac{1-p}{1+3p}} \\ 0 & 0 & \sqrt{\frac{1+3p}{1-p}} & 0 \end{bmatrix}. \tag{A4}$$

Only when $p \leq 1/3$ is the state ρ separable. For these values of p, one finds an explicit Gram decomposition (20) of ρ with

$$D_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$D_2 = \begin{bmatrix} \frac{(1-i)(\sqrt{1-3p}+\sqrt{p+1})}{\sqrt{2}(\sqrt{1-p}+\sqrt{3p+1})} & 0 & 0 & 0 \\ 0 & -\frac{(1+i)(\sqrt{p+1}-\sqrt{1-3p})}{\sqrt{2}(\sqrt{1-p}-\sqrt{3p+1})} & 0 & 0 \\ 0 & 0 & -\frac{(1-i)(\sqrt{1-3p}+\sqrt{p+1})}{\sqrt{2}(\sqrt{1-p}+\sqrt{3p+1})} & 0 \\ 0 & 0 & 0 & \frac{(1+i)(\sqrt{p+1}-\sqrt{1-3p})}{\sqrt{2}(\sqrt{1-p}-\sqrt{3p+1})} \end{bmatrix},$$

and

$$v_1' = \begin{bmatrix} \frac{(\sqrt{1-p}+\sqrt{3p+1})}{4\sqrt{2}} e^{\pi i/2} \\ \frac{(\sqrt{1-p}-\sqrt{3p+1})}{4\sqrt{2}} e^{\pi i/2} \\ \frac{(\sqrt{1-p}+\sqrt{3p+1})}{4\sqrt{2}} e^{-\pi i/2} \\ \frac{(\sqrt{1-p}-\sqrt{3p+1})}{4\sqrt{2}} e^{-\pi i/2} \end{bmatrix}, \quad v_2' = \begin{bmatrix} \frac{(\sqrt{p+1}-\sqrt{1-3p})}{4\sqrt{2}} e^{3\pi i/4} \\ \frac{(\sqrt{1-3p}+\sqrt{p+1})}{4\sqrt{2}} e^{-3\pi i/4} \\ \frac{(\sqrt{p+1}-\sqrt{1-3p})}{4\sqrt{2}} e^{3\pi i/4} \\ \frac{(\sqrt{1-3p}+\sqrt{p+1})}{4\sqrt{2}} e^{-3\pi i/4} \end{bmatrix}.$$

For the particular choice of F_1, F_2, v_1, and v_2, the matrices $\tilde{V}$ and V (cf. Corollary 1) are given as

$$\tilde{V} = V = \begin{bmatrix} \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} & \frac{\sqrt{1-3p}-i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} \\ \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} & \frac{-\sqrt{1-3p}+i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} \\ \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} & \frac{\sqrt{1-3p}-i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} \\ \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} & \frac{-\sqrt{1-3p}+i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} \end{bmatrix}, \tag{A5}$$

for which one easily checks that $V^\dagger D_m \tilde{V} = F_m$ on $\mathrm{span}(v_1, v_2)$.

APPENDIX B: SHORT GUIDE TO $2\times N$ SYSTEMS

From Theorem 3 it is clear that investigations of separability can be simplified if we know *a priori* the order of separability K of the given state (i.e., we know that it is K separable). We do not have any general tool for determining exactly the order of separability for arbitrary separable states before finding their actual decomposition into pure products (and even if we find one, to establish the order of separability we still have to prove that the decomposition found involves the minimal number of components). Here we present some exact results concerning orders of separability in the case of $2\times N$ systems for low values of N.

1. Canonical forms

Let ρ be an arbitrary density matrix of a bipartite $2\times N$ system,

$$\rho = \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix}, \tag{B1}$$

where A, B, and C are $N\times N$ matrices; A and C are Hermitian due to Hermiticity of ρ. Positive definiteness of ρ implies $A \geq 0$, $C \geq 0$, and $A - BC^{-1}B^\dagger \geq 0$. The matrix C is nonsingular since ρ, by assumption, is of maximal rank. By an invertible transformation

$$\rho \mapsto (I \otimes C^{-1/2})\rho(I \otimes C^{-1/2}) \tag{B2}$$

we bring ρ to the *canonical form* [24]

$$\rho = \begin{bmatrix} A & B \\ B^\dagger & I \end{bmatrix}. \tag{B3}$$

For simplicity of notation, we kept the same symbols A and B to denote the appropriate blocks of ρ, despite the fact that the original blocks defined in (B1) are altered by the transformation (B2). Such a transformation changes, in principle, the trace of ρ, but since the normalization of the trace does not influence separability properties we will set this point aside. The positivity conditions of ρ reduce now to

$$A = BB^\dagger + \Lambda\Lambda^\dagger, \tag{B4}$$

where Λ is some $p\times N$ matrix.

A necessary criterion of separability is the non-negative definiteness of the partially transposed matrix, which for the case of a $2\times N$ system ($2N$) is defined as

$$\rho^{T_A} = \begin{bmatrix} A & B^\dagger \\ B & I \end{bmatrix}. \tag{B5}$$

From now on we will assume thus that both ρ and ρ^{T_A} are positive definite (otherwise ρ is not separable). Positive definiteness of the partial transpose of (B3) demands that

$$A = B^\dagger B + \tilde{\Lambda}^\dagger \tilde{\Lambda}, \tag{B6}$$

for some $\tilde{\Lambda}$.

2. Decompositions of ρ

For our purposes, it important to consider particular decompositions of ρ for $K=N+p$, and construct the "known" part of the matrix $\hat{M}$ that satisfies Eq. (29). From the canonical form and Eq. (B4), with $\Lambda=(|\Lambda_1\rangle,\ldots,|\Lambda_p\rangle)$, it is easy to see that $\rho=\Sigma_{k=1}^{N+p}|\Phi_k\rangle\langle\Phi_k|$, with

$$|\Phi_k\rangle = |0\rangle\otimes|k\rangle + |1\rangle\otimes B|k\rangle, \tag{B7}$$

for $k=1, \ldots, N$, and

$$|\Phi_k\rangle = |1\rangle\otimes|\Lambda_{k-N}\rangle, \tag{B8}$$

for $k=N+1,\ldots,N+p$. From this particular form we read the components of the vectors w''_{0n}, w''_{1n}:

$$(w''_{0n})^k = \delta_{kn} \tag{B9}$$

for $k=1,\ldots,N$, and zero otherwise. Similarly,

$$(w''_{1n})^k = B_{nk} \tag{B10}$$

for $k=1,\ldots,N$, and

$$(w''_{1n})^k = \langle n|\Lambda_{k-N}\rangle \tag{B11}$$

for $k=N+1,\ldots,N+p$. Obviously, for the particularly simple form of w''_{0n}, Eq. (29) determines only the first N columns of the matrix $\hat{M}^T$, which are

$$\hat{M}^T = \begin{bmatrix} B^T & ? \\ \Lambda^\dagger & ? \end{bmatrix}, \tag{B12}$$

where the other entries are at this moment not known. Transposing and using the PPT constraint (37), we indeed obtain that

$$\hat{M} = \begin{bmatrix} B & \Lambda \\ \tilde{\Lambda} & S \end{bmatrix}, \tag{B13}$$

where, for given B and Λ, the matrix $\tilde{\Lambda}$ is constrained only by the condition (37), and S is completely arbitrary. This form of $\hat{M}$ is intensively used by us in the section on separability in $2\times N$ systems.

3. Edge states

For the purpose of this paper, we remind the reader of the basic concepts associated with the edge states. First, we recall [24,25,28] that, if $|e,f\rangle$ (or any vector, in fact) is in the range of ρ, then we can write

$$\rho = \rho' + \lambda|e,f\rangle\langle e,f|,$$

where $\rho'\geq 0$ provided $\lambda\leq 1/\langle e,f|\rho^{-1}|e,f\rangle$. When the equality holds, the rank of ρ' is smaller than the rank of ρ by 1.

From this observation we have the following corollary.

Corollary 5. A PPT state ρ is an edge state if there exists no product vector $|e,f\rangle$ in its range, such that $|e^*,f\rangle$ is in the range of ρ^{T_A}.

Subtracting projectors on product vectors as in Refs. [24,28]. allows us to determine the minimal number of projectors on product states necessary to decompose a separable state. We recall some particular cases for the reader.

The case 2×2. In this case, $K=\max(r(\rho),r(\rho^{T_A}))$. This result stems from [26]. In the following we shall use the notation (p,q) for the case of $r(\rho)=p$, $r(\rho^{T_A})=q$. Let us consider the case of full ranks (4,4). First we show that we can find the product vector for which $\lambda=1/\langle e,f|\rho^{-1}|e,f\rangle = 1/\langle e^*,f|(\rho^{T_A})^{-1}|e^*,f\rangle$, so that subtracting the projector on this vector reduces the ranks to (3,3). With this aim we suppose that $\rho=\Sigma_{k=1}^{K}|e_k,f_k\rangle\langle e_k,f_k|$ is separable, and that, for all $|e,f\rangle$, $\langle e,f|\rho^{-1}|e,f\rangle<\langle e^*,f|(\rho^{T_A})^{-1}|e^*,f\rangle$ holds. Inserting into this inequality $|e_k,f_k\rangle$ and summing over k, we get a contradiction, $\mathrm{Tr}(I)=4<4=\mathrm{Tr}(I)$. In the same manner, we prove that the opposite inequality cannot be satisfied by all product vectors. Thus, either all product vectors satisfy the equality, or there are at least two product vectors for which the inequality takes opposite signs. But then, from the Darboux property and the fact the set of all product states is connected, we gather that there exists a product vector for which the equality holds. In the next step, we reduce one rank to 2; this, however, implies that so does the other rank, since from the general theory of Ref. [24]. it follows that a rank-N PPT matrix in $2\times N$ systems is N separable.

The case 2×3. This problem was partially addressed in the thesis of Vidal [29]. The proof here is different. We start with the full ranks and, using the same argument as above, we reduce the ranks to (5,5). The argument may then be repeated but with a certain care. Now we suppose that $\rho=\Sigma_{k=1}^{K}|e_k,f_k\rangle\langle e_k,f_k|$ is separable, and that for all $|e,f\rangle$ in its range, and such that $|e^*,f\rangle$ is in the range of ρ^{T_A}, it holds that $\langle e,f|\rho^{-1}|e,f\rangle<\langle e^*,f|(\rho^{T_A})^{-1}|e^*,f\rangle$. Again, inserting into this inequality $|e_k,f_k\rangle$ and summing over k, we get a contradiction, $\mathrm{Tr}(I_{R(\rho)})=5<5=\mathrm{Tr}(I_{R(\rho^{T_A})})$, where $I_R(\rho)$ denotes identity on the range. We may again evoke the Darboux property, but to this end we need to prove that the set of product vectors in question is connected. Let Ψ be a vector from the kernel of ρ and Φ from the kernel of ρ^{T_A}. The product vectors we look for have to satisfy $\langle\Psi|e,f\rangle=0$, $\langle\Phi|e,f\rangle=0$. These equations can be regarded as two linear equations for a three-component vector $|f\rangle$, parametrized by the vector $|e\rangle=|0\rangle+\alpha|1\rangle$, which we have parametrized by the complex number α in some basis. Obviously, $|f\rangle$ is a unique function of α, and by scanning α over the complex plane we can reach any of these vectors in a continuous way. The Darboux theorem says then that there exists a product vector for which equality holds, $\langle e,f|\rho^{-1}|e,f\rangle=\langle e^*,f|(\rho^{T_A})^{-1}|e^*,f\rangle$, and we can

reduce the ranks to (4,4). The next step is as above: reduction of one of the ranks to 3, implying the same reduction for the other. The reason for this is that all rank-3 states in 2×3 systems are 3 separable.

The case 2×4. It is also possible to determine what is the minimal number of terms in the separable decomposition for states of low ranks. In this paper, we consider two cases: (5,5) and (5,6). In the (5,5) case there are three vectors $|\Psi_i\rangle$ in the kernel of ρ, and another three vectors $|\Phi_i\rangle$ in the kernel of ρ^{T_A}. We look for $|e_k,f_k\rangle$ such that $\langle\Psi_i|e,f\rangle=0$, $\langle\Phi_i|e^*,f\rangle=0$ for all $i=1,2,3$. These can be regarded as six linear equations for a four-component vector $|f\rangle$. They have solutions provided three 4×4 determinants (constructed from the first three and one of the last three equations) vanish. These determinants constitute three polynomials of third order in α and first order in α^*. Eliminating α^* from them, we obtain that two polynomials of sixth order in α must vanish. Subtracting them with appropriate coefficients, we conclude that a polynomial of fifth order in α must vanish, i.e., there are at most five product vectors having the desired properties. This implies that, if ρ is separable, then it is 5 separable.

A similar analysis can be done for the case of the state ρ with ranks (5,6). We end up then with one polynomial of sixth order in α, i.e., we have at most six solutions, so, if ρ is separable, then it is 6 separable. Note that the states with ranks (5,6) are either separable, or entangled edge states, or mixtures of rank-(5,5) edge states with a single projector on a product vector from the range of ρ.

Unfortunately, only upper bounds on the number of product states in a decomposition of separable states are known for ρ's of higher ranks. In particular, the Caratheodory theorem (for proof, see [27]) gives a general bound equal to the square of the dimension of the Hilbert space, i.e., in the present case $(2\times4)^2=64$, implying that every separable state is 64 separable.

For the states with ranks (5,7), it can be shown that there exists in the range of ρ a product vector $(|0\rangle+\alpha|1\rangle)|f\rangle$ such that $(|0\rangle+\alpha^*|1\rangle)|f\rangle$ is in the range of ρ^{T_A}. It is easy to see that the condition that these product vectors are orthogonal to the corresponding kernels of ρ and ρ^{T_A} leads to four linear equations for four components of $|f\rangle$. The solutions of such equations exist if the determinant of the corresponding matrix vanishes. This matrix has three rows linear in α and one row linear in α^*, so that the determinant equation has the form

$$W_3(\alpha)+\alpha^*V_3(\alpha)=0, \tag{B14}$$

where $W_3(\cdot)$ and $V_3(\cdot)$ are polynomials of third order. Let us replace $\alpha\to rs$, $\alpha^*\to r/s$ with $r>0$ and s complex, and treat Eq. (B14) as an equation for $s(r)$ (i.e., treat s as parametrically dependent on r),

$$sW_3(rs)+rV_3(rs)=0.$$

We will show that this equation has at least one root $\alpha=rs$ with $|s|=1$, i.e., with $\alpha^*=r/s$. With this aim, we consider the asymptotic behavior at $r\to\infty$. It is easy to show that the above equation has three roots $s_i=O(1/r)\to0$, $i=1,2,3$, and one root $s_4=O(r)\to\infty$. Analogously, for $r\to0$, it is easy to show that the equation has three roots $\tilde{s}_i=O(1/r)\to\infty$, $i=1,2,3$, and one root $\tilde{s}_4=O(r)\to0$. All that implies that, when we continuously change r from 0 to ∞, one of the three "large" roots must become "small." From continuity (i.e., again from the Darboux property) we get that, for some $r=r_0$, the $|s(r_0)|=1$. Unfortunately, we cannot say much more about the total number of such roots. Solving Eq. (B14) with respect to α^*, complex conjugating the result, and stacking it back into Eq. (B14), we obtain an equation for α^* of tenth order, which indicates that there are not more than ten roots of Eq. (B14).

APPENDIX C: HORODECKI'S 2×4 EDGE STATE

In this appendix we show how our method work for the famous state ρ_{97} introduced by Horodecki in the seminal paper [27]. In our notation, this state has

$$B=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&1&0\\0&0&0&0\end{bmatrix} \tag{C1}$$

and

$$|\Lambda\rangle=\begin{bmatrix}\sqrt{(1-b)/2b}\\0\\0\\\sqrt{(1+b)/2b}\end{bmatrix},\quad |\tilde{\Lambda}\rangle=\begin{bmatrix}\sqrt{(1+b)/2b}\\0\\0\\\sqrt{(1-b)/2b}\end{bmatrix}. \tag{C2}$$

This state has rank 5 (like its partial transpose) and is an example of an edge state [24]. As pointed out in Ref. [27], there exists a unitary matrix K, such that $K^2=I$, $KBK=B^\dagger$, and $K|\Lambda\rangle=|\tilde{\Lambda}\rangle$. The condition of existence of the normal extension from Sec. VI reads then $(B-s)|\tilde{\Lambda}\rangle=K(B-s^*)|\tilde{\Lambda}\rangle$, i.e.,

$$\begin{bmatrix}-s\sqrt{(1+b)/2b}\\0\\\sqrt{(1-b)/2b}\\-s\sqrt{(1-b)/2b}\end{bmatrix}=\begin{bmatrix}-s^*\sqrt{(1-b)/2b}\\\sqrt{(1-b)/2b}\\0\\-s^*\sqrt{(1+b)/2b}\end{bmatrix}, \tag{C3}$$

which has only the two solutions $s=0$, $b=1$, and the limiting case $b=0$, with an arbitrary real $s=s^*$. These are exactly the two instances in which the Horodecki state is separable.

[1] See, for instance, *Lectures on Quantum Information*, edited by D. Bruß and G. Leuchs (Wiley-VCH, Berlin, 2007).
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, e-print arXiv:quant-ph/0702225, Rev. Mod. Phys. (to be published).
[3] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States* (Cambridge University Press, Cambridge, U.K., 2006).
[4] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[6] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[7] K. Eckert, J. Schliemann, D. Bruss, and M. Lewenstein, Ann. Phys. (N.Y.) **299**, 88 (2002).
[8] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[9] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[10] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001).
[11] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. A **64**, 052303 (2001).
[12] For a general description of the method, see A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); for a specific formulation of the semidefinite approach for $2\times N$ systems, see H. J. Woerdeman, Phys. Rev. A **67**, 010303(R) (2003).
[13] L. Gurvits, J. Comput. Syst. Sci. **69**, 448 (2004).
[14] See, for instance, B. M. Terhal, Linear Algebr. Appl. **323**, 61 (2001); M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, Phys. Rev. A **63**, 044304 (2001); H.-P. Breuer, Phys. Rev. Lett. **97**, 080501 (2006).
[15] See, for instance, B. M. Terhal, Theor. Comput. Sci. **287**, 313 (2002); M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
[16] See, for instance, P. Horodecki and A. Ekert, Phys. Rev. Lett. **89**, 127902 (2002); O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002); M. Bourennane, M. Eibl, Ch. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, Ph. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
[17] J. K. Korbicz and M. Lewenstein, Phys. Rev. A **74**, 022318 (2006).
[18] E. Schrödinger, Naturwiss. **23**, 807 (1935).
[19] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
[20] M. Spivak, *A Comprehensive Introduction to Differential Geometry* (Publish or Perish, Wilmington, 1979), Vol. 5.
[21] J. Korbicz, Ph.D. thesis, Universität Hannover, 2006.
[22] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **92**, 167902 (2004).
[23] R. A. Horn and Ch. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, U.K., 1990).
[24] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).
[25] T. Wellens and M. Kuś, Phys. Rev. A **64**, 052302 (2001); S. Karnas and M. Lewenstein, J. Phys. A **34**, 6919 (2001).
[26] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).
[27] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[28] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
[29] G. Vidal, Ph.D. thesis, Universidad Barcelona, 1999.