Variational characterizations of separability and entanglement of formation

Koenraad Audenaert,* Frank Verstraete,† and Bart De Moor‡
Department of Electrical Engineering (ESAT), Research Group SISTA, Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
(Received 20 February 2001; published 10 October 2001)

In this paper we develop a mathematical framework for the characterization of separability and entanglement of formation (EOF) of general bipartite states. These characterizations are variational in nature, meaning that separability and EOF are given in terms of a function that is to be minimized over the manifold of unitary matrices. A major benefit of such a characterization is that it directly leads to a numerical procedure for calculating EOF. We present an efficient minimization algorithm and apply it to the bound entangled 3×3 Horodecki states; we show that their EOF is very low and that their distance to the set of separable states is also very small. Within the same variational framework we rephrase the results by Wootters [W. Wootters, Phys. Rev. Lett. **80**, 2245 (1998)] on EOF for 2×2 states and also present some progress in generalizing these results to higher-dimensional systems.

DOI: 10.1103/PhysRevA.64.052304 PACS number(s): 03.67.−a, 89.70.+c, 03.65.Ta

I. INTRODUCTION

The problem of finding necessary and sufficient conditions under which a quantum state of a composite system is separable has received considerable attention in the last few years. The prototype example of a nonseparable state is a pair of two-level particles in a singlet state, a so-called EPR pair, named after Einstein, Podolsky, and Rosen, who used this sort of a state to show that quantum mechanics exhibits strong nonlocal correlations, which seem to violate the relativity principle.

A pure state of a composite system is separable iff it can be written as the direct product of the subsystem states: $|\Psi_{AB}\rangle=|\Psi_A\rangle\otimes|\Psi_B\rangle$. A nonseparable pure state or *entangled* state cannot be decomposed in this way, e.g., the singlet state $(|\uparrow\rangle|\downarrow\rangle-|\downarrow\rangle|\uparrow\rangle)/\sqrt{2}$ consists of a superposition of separable states but is itself not separable.

Nowadays, the importance of entangled states goes beyond a mere fundamental interest, since EPR pairs are the basic resources of quantum techniques such as quantum cryptography, quantum teleportation, and quantum error correction. A mixed state is separable iff its density matrix can be written as a convex linear combination of pure product states; for a bipartite system this reads

$$\rho=\sum_{k=1}^{K} w_k|u^k\rangle\langle u^k|\otimes|v^k\rangle\langle v^k|, \tag{1}$$

where w_k are positive weights summing to 1. The separability problem consists of finding a criterion for checking whether such a decomposition is possible for a given state.

Despite the simple formulation of this problem, a complete solution to this date has not been found. An important achievement was the discovery by Peres of a necessary condition for separability [1]. He noted that the *partial transposition* of a separable state still has non-negative eigenvalues, just as the original state. Thus, if the partial transposition of state ρ is not a state (i.e., does not have non-negative eigenvalues summing to 1), then ρ is not separable (i.e., it is an entangled state). The importance of this criterion was soon realized when Horodecki *et al.* proved [2] that it is also a sufficient criterion for 2×2 and 2×3 systems. For an introduction to recent results on this subject, see, e.g., [3] and [4].

If a state is entangled, one could ask for a measure of the amount of entanglement. For pure states, a measure generally agreed upon is the von Neumann subsystem entropy: the entropy of the partial trace of the state projector. For mixed states, the situation is much more difficult. Not only is there no single measure of entanglement that is suited for every purpose, but calculating the values of the different proposed measures and proving statements about them is exceedingly difficult. Among the proposed measures are the entanglement of formation [5], the entanglement of distillation [5], and relative entropy of entanglement [6].

In this paper, we focus on separability, on entanglement of formation (EOF), and on the related concept of concurrence. All these subjects are related, because states are separable if and only if their EOF is zero. A closed-form expression exists for the EOF of 2×2 systems in terms of their concurrence [7]. A closed-form expression also exists for isotropic states of general systems [8].

The purpose of this paper is to give variational characterizations of separability and EOF for general (i.e., any dimensions) bipartite states. Such a characterization is of the form $Q(\rho)=\min_T f(\rho,T)$, that is, the state property under study can be found as the minimal value of some specific function over the manifold of unitary matrices T. In Sec. II it will be shown how this can be done. The language of Sec. II is matrix analysis, not only because this allows to state the results in a most succinct way but also because it gives clues towards generalizations.

The greatest benefit of a variational characterization is that it directly yields a method for actually calculating the state property Q, albeit in a numerical fashion, using a mini-

*Email address: koen.audenaert@esat.kuleuven.ac.be
†Email address: frank.verstraete@esat.kuleuven.ac.be
‡Email address: bart.demoor@esat.kuleuven.ac.be

mization procedure. In Sec. III we describe the procedure that we have used, and some interesting results we have obtained with it.

II. VARIATIONAL CHARACTERIZATIONS

It is well known that mixed states can be realized by an ensemble of pure states in an infinite number of ways. The determination of the separability of a state and the determination of its entanglement of formation have in common that a particular realization of a state has to be found such that some property holds for all pure states in that realization. In order to find this optimal realization, it is of considerable interest to have a mathematically elegant way of ''generating'' all possible realizations of a state. In Sec. II A we will recollect a result by Hughston, Jozsa, and Wootters that any realization of a state is related to the eigenvalue decomposition of the state via some right-unitary matrix.

The required property for separability is that all pure states in the realization must be product states. In Sec. II B we give a number of useful mathematical expressions for this property. This then leads to a variational characterization of separability, the topic of Sec. II C. For calculating the EOF of the state, the property of the optimal realization is that the so-called average entanglement of the realization is minimal. This property and an ensuing variational characterization of EOF will be discussed in Sec. II D.

In this way, searching all possible realizations for some property amounts to passing through all right-unitary matrices and test the property in question. However, this would be a very impractical way to determine separability or EOF if there would not be some bound on the dimension of these matrices, or, which is the same thing, on the number of pure states in the optimal realization. Luckily, such a bound exists. In the case of separability, Horodecki proved [11] that $(N_1N_2)^2$ pure states (or less) suffice, where N_1 and N_2 are the dimensions of the subsystem Hilbert spaces. Uhlmann [12] proved that a similar bound holds for the determination of EOF: the number of pure states in the optimal realization need not be larger than the square of the rank of the state.

In Sec. II E we discuss the so-called concurrence of a state, a quantity that is closely related to the EOF. We give an alternative proof of an important result on the concurrence of 2×2 states by Wootters [7]. One of the virtues of this alternative proof is that it yields an additional result on the exact amount of pure states in the optimal realization. We then report some progress in generalizing the concurrence concept to higher-dimensional bipartite states.

In Appendix A, finally, a method is described for reducing the set of unitary matrices that has to be examined in the case of separability testing. Under some circumstances, this method directly yields an optimal realization without any need for searching. We have not yet investigated whether this method is applicable to the EOF case.

A. Relation between different realizations of a state

Consider a rank-R state ρ in an $(N_1\times N_2)$-dimensional Hilbert space, realized by an ensemble $\{w_k,|\psi^k\rangle\}_{k=1}^K$, where the w_k are the mixing weights of the K pure state vectors $|\psi^k\rangle$. The number K is called the *cardinality* of the ensemble. Necessarily, K cannot be smaller than the rank R. Since there generally are an infinite number of ensembles realizing a particular mixed state, we are free to choose K larger than R if this suits our purposes. It will turn out that in the general case, we will even be forced to take $K>R$. Specifically, Lockhart proved in [13] that, except in the bipartite case where one of the particles is a qubit or the Hilbert-space dimension is 9, the set of separable states for which $K=R$ is a set of measure zero. Moreover, for $N\times N$ systems, the set of separable states for which the cardinality K is greater than $(R^{1.5})/4$ is an open dense set.

Now, $\rho=\Sigma_{k=1}^K w_k|\psi^k\rangle\langle\psi^k|$ or $\rho=\Psi W\Psi^\dagger$, where W is a $K\times K$ diagonal matrix with $W_{kk}=w_k$ and the columns of Ψ are the K vectors ψ^k. This decomposition of ρ is reminiscent of the eigenvalue decomposition of ρ: $\rho=\Phi M\Phi^\dagger$, where M is an $R\times R$ diagonal matrix whose diagonal elements are the eigenvalues of ρ and the columns of Φ are the R eigenvectors. Since ρ is Hermitian, Φ is a unitary matrix.

It can now easily be proven that these two decompositions must be related by an $R\times K$ right-unitary matrix T; this has been proven first by Hughston, Jozsa, and Wootters [9].

Lemma 1. For a general state ρ, with eigenvalue decomposition $\rho=\Phi M\Phi^\dagger$, there is a matrix Ψ and a non-negative diagonal matrix W such that $\rho=\Psi W\Psi^\dagger$ iff there is an $R\times K$ matrix T such that

$$\Psi W^{1/2}=\Phi M^{1/2}T,$$

with

$$TT^\dagger=\mathbb{1}_R. \tag{2}$$

Right-unitarity of the matrix T means that the R row vectors of T form an orthonormal set in $\mathbb{C}^K$. Stated in matrix-algebraic terms, the proof becomes very simple.

Proof. First of all, it is obvious that $\Phi M\Phi^\dagger=\Psi W\Psi^\dagger$ follows directly from Eq. (2). Conversely, denote $X=\Psi W^{1/2}$ and consider the singular-value decomposition of X: $X=U\Sigma V$, where U is a unitary $R\times R$ matrix, V a right-unitary $R\times K$ matrix, and Σ a diagonal $R\times R$ matrix with non-negative diagonal elements. From $\Phi M\Phi^\dagger=\Psi W\Psi^\dagger$ we get $\Phi M\Phi^\dagger=U\Sigma^2U^\dagger$. Since both M and Σ are positive semidefinite, it follows that $\Sigma=U^\dagger\Phi M^{1/2}\Phi^\dagger U$ so that $X=\Phi M^{1/2}\Phi^\dagger UV$. This is precisely Eq. (2), with $T=\Phi^\dagger UV$. □

Remark. It is noteworthy that the elements of W and M are related to each other independently of Φ and Ψ,

$$w_k=(T^\dagger MT)_{kk}.$$

This follows from the observations that Φ is unitary and that the columns of Ψ have norm 1.

B. Characterization of product states

A state of an $N_1\times N_2$ system is separable iff there exists a realizing ensemble consisting solely of product vectors $\psi=\psi^1\otimes\psi^2$ with $\psi^1\in\mathcal{H}_1$ and $\psi^2\in\mathcal{H}_2$ (in this paper we use

superscripts for enumerating vectors and subscripts for denoting vector components). Product vectors can be characterized easily by rearranging their components in matrix form. For an N_1N_2 vector x, let $\tilde{x}$ be an $N_1\times N_2$ matrix such that $x=\Sigma_{i,j}\tilde{x}_{ij}e^i\otimes e^j$. For product vectors this gives

$$\psi^k=\alpha^k\otimes\beta^k\rightarrow\tilde{\psi}^k=\alpha^k(\beta^k)^T.$$

Obviously, product vectors are characterized by the condition that the rank of $\tilde{\psi}$ is 1. A necessary and sufficient condition for this is that all 2×2 minors of $\tilde{\psi}$ must be zero, or, more succinctly, that the *second compound matrix* of $\tilde{\psi}$ must be zero: $C_2(\tilde{\psi})=0$ ([10], 0.8.1). The second compound matrix of an $N_1\times N_2$ matrix is an $[N_1(N_1-1)/2]\times[N_2(N_2-1)/2]$ matrix with elements

$$C_2(A)_{(ii'),(jj')}=A_{ij}A_{i'j'}-A_{ij'}A_{i'j},\quad i<i',\quad j<j'.$$

The elements of C_2 are all possible 2×2 minors of A. The second compound matrix has a lot of useful properties such as $C_2(AB)=C_2(A)C_2(B)$, $C_2(\mathbb{1}_n)=\mathbb{1}_{n(n-1)/2}$, and $C_2(A^{-1})=[C_2(A)]^{-1}$ ([10], 0.8.1).

For practical applications it is sometimes better to consider a $(N_1-1)\times(N_2-1)$ submatrix of C_2, the one containing the elements $C_2(A)_{(i,i+1),(j,j+1)}$ only. It is easily seen that the vanishing of this submatrix is already sufficient for A being of rank 1.

From the expression for the second compound matrix, which is quadratic in A, it will prove useful to construct a bilinear function of two $N_1\times N_2$ matrices, denoted $\mathcal{C}(A,B)$,

$$\mathcal{C}(A,B)_{(ii'),(jj')}=A_{ij}B_{i'j'}-A_{ij'}B_{i'j},\quad i<i',\quad j<j'.$$

Obviously, $\mathcal{C}(A,A)=C_2(A)$, so that $\mathcal{C}(A,A)=0$ if and only if A has rank 1. More specifically, we can apply this to the state vectors ψ^k: ψ^k is a product vector if $\mathcal{C}(\tilde{\psi}^k,\tilde{\psi}^k)=0$.

In the following, we will only use a symmetrized version of $\mathcal{C}$, which we will denote by

$$C(\psi^k,\psi^l)=\mathcal{C}(\tilde{\psi}^k,\tilde{\psi}^l)+\mathcal{C}(\tilde{\psi}^l,\tilde{\psi}^k).$$

Since this is a bilinear function in the elements of Ψ, we can express this in matrix notation

$$C(\psi^k,\psi^l)_{(\alpha)}=(\Psi^TS^{(\alpha)}\Psi)_{kl},$$

where the notation (α) is a shorthand for the index tuple (i,i',j,j'). The matrices $S^{(\alpha)}$, which we call *indicator matrices*, are defined as

$$S^{(\alpha)}_{(ij),(i'j')}=S^{(\alpha)}_{(i'j'),(ij)}=1,$$

$$S^{(\alpha)}_{(ij'),(i'j)}=S^{(\alpha)}_{(i'j),(ij')}=-1,$$

all other elements being zero. Note that all S have rank equal to 4. For the case of 2×2 systems, there is only one indicator matrix and it is equal to

$$S=\sigma_y\otimes\sigma_y=\begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&-1&0&0\\1&0&0&0\end{pmatrix},$$

(Ref. [7]).

C. Condition for separability

We can now formulate a general necessary and sufficient condition for the separability of a mixed state. As mentioned before, the state $\rho=\Phi M\Phi^\dagger$ is separable iff there exists a decomposition $\rho=\Psi W\Psi^\dagger$ with $\Psi W^{1/2}=\Phi M^{1/2}T$, such that all ψ^k are product states, or $C(\psi^k,\psi^l)=0$, for all $k=l$.

Now

$$C(\psi^k,\psi^l)=C(\sqrt{w_k}\psi^k,\sqrt{w_l}\psi^l)/\sqrt{w_kw_l}$$
$$=\sum_{p,q=1}^{R}\frac{T_{pk}T_{ql}}{\sqrt{w_kw_l}}C(\sqrt{m_p}\phi^p,\sqrt{m_q}\phi^q),\qquad(3)$$

where we have exploited the bilinearity of the form C. Given the eigenvalue decomposition of ρ, the entity $C(\sqrt{m_p}\phi^p,\sqrt{m_q}\phi^q)$ can be calculated in a straightforward way. Let us organize its components into a set of matrices $A^{(\alpha)}\in M_R$,

$$A^{(\alpha)}_{pq}=C(\sqrt{m_p}\phi^p,\sqrt{m_q}\phi^q)_\alpha=\sqrt{M}\Phi^TS^{(\alpha)}\Phi\sqrt{M};\qquad(4)$$

this means that the pq entry of the (α)th A matrix equals the α entry of the matrix $C(\sqrt{m_p}\phi^p,\sqrt{m_q}\phi^q)$. Using this notation, Eq. (3) can be written concisely as

$$C(\psi^k,\psi^l)_\alpha=(T^TA^{(\alpha)}T)_{lk}/\sqrt{w_kw_l}.$$

The state is therefore separable iff we can find an $R\times K$ matrix T, with $K\geqslant R$, such that

$$TT^\dagger=\mathbb{1}_R,$$

$$C_2(\tilde{\psi}^k)_\alpha=(T^TA^{(\alpha)}T)_{kk}=0\quad\forall\quad\alpha,k.\qquad(5)$$

Here, k ranges from 1 to K and α enumerates all tuples of indices (i,i',j,j') with $1\leqslant i<i'\leqslant N_1$ and $1\leqslant j<j'\leqslant N_2$. As noted before, it is also sufficient to consider only the tuples $(i,i+1,j,j+1)$.

Testing separability requires that the system (5) be solved for T. Another approach, however, is to consider $(T^TA^{(\alpha)}T)_{kk}$ as entries of a matrix indexed by α and k and to try to minimize a matrix norm of this matrix as a function of T. The state is then separable iff this minimum is zero. Obviously, one can use whatever matrix norm one prefers, e.g., the Hilbert-Schmidt norm (also called the Frobenius norm or the l_2 norm) $\|A\|_2^2=\Sigma_{i,j}|A_{i,j}|^2=\mathrm{Tr}AA^\dagger$. Thus ρ is separable iff

$$\min_{T,K}\sum_{\alpha,k}|(T^TA^{(\alpha)}T)_{kk}|^2=0.\qquad(6)$$

where the minimum has to be taken over all $K \geqslant R$ and all $R \times K$ matrices T for which $TT^\dagger = \mathbb{1}_R$. The minimal K is called the *cardinality* of the state.

One can also use the l_1 norm (sum of absolute values) and minimize $\Sigma_{\alpha,k} |(T^T A^{(\alpha)} T)_{kk}|$. For 2×2 systems, the l_1 norm is the *average concurrence* of the ensemble, as introduced by Wootters in [7], and the minimum is the *concurrence* of the state ρ. Note that in the context of separability testing it does not matter whether one uses $(T^T A^{(\alpha)} T)_{kk}$ or $(T^T A^{(\alpha)} T)_{kk}/w_k$.

To end this paragraph, we derive an alternative expression for the l_2 norm $\|(C_2(\tilde{\psi}^k))_k\|_2$. Define $B^k = \tilde{\psi}^k (\tilde{\psi}^k)^\dagger$, with eigenvalue decomposition $B^k = U^k \Sigma^k U^{k\dagger}$ [with $\Sigma^k = \mathrm{Diag}(\sigma_i^k)$]. Using the properties of C_2 we find

$$\begin{aligned}
\|[C_2(\tilde{\psi}^k)]_{k=1}^n\|_2^2 &= \sum_k \mathrm{Tr}[C_2(\tilde{\psi}^k) C_2(\tilde{\psi}^k)^\dagger] = \sum_k \mathrm{Tr}\, C_2(B^k) \\
&= \sum_k \mathrm{Tr}\, C_2(\Sigma^k) = \sum_k \sum_{i<j} \sigma_i^k \sigma_j^k \\
&= \tfrac{1}{2} \sum_k \left[\sum_{i,j} \sigma_i^k \sigma_j^k - \sum_i (\sigma_i^k)^2 \right] \\
&= \tfrac{1}{2} \sum_k \left(\sum_i \sigma_i^k \right)^2 - \sum_i (\sigma_i^k)^2 \\
&= \tfrac{1}{2} \sum_k [(\mathrm{Tr}\Sigma^k)^2 - \mathrm{Tr}(\Sigma^k)^2] \\
&= \tfrac{1}{2} \sum_k [(\mathrm{Tr}\, B^k)^2 - \mathrm{Tr}(B^k)^2].
\end{aligned}$$

This result can be interpreted easily: a positive definite Hermitian matrix is of rank 1 iff the square of its trace equals the trace of its square.

D. Entanglement of formation

Within the same framework, we can also give a variational characterization of the EOF $E(\rho)$ of a mixed state ρ. This quantity is defined as the average entanglement of the pure states in a realizing ensemble, minimized over all possible realizing ensembles [5]. The von Neumann entropy H of a state ρ is $-\mathrm{Tr}\,\rho \log_2 \rho$. Introducing the function $h(x) = -x \log_2 x$, we can express H as a function of the eigenvalues λ_k of ρ: $H(\rho) = \Sigma_k h(\lambda_k)$. The entanglement of a pure state ψ of a bipartite system (A, B) is the entropy of the partial trace of the projector of $|\psi\rangle$: $E(\psi) = H(\rho_A)$ with $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. The average entanglement of an ensemble $\{w_k, \psi^k\}$ is $\Sigma_k w_k E(\psi^k)$; the EOF is then found as the minimal value over all ensembles realizing ρ.

In this paragraph, we will derive an expression for $E(\rho)$ that is better suited for calculation than the defining equation. Let $\{w_k, \psi^k\}$ be the realizing ensemble with least average entanglement and $\{m_p, \phi\}$ the realizing ensemble corresponding to the eigenvalue decomposition of ρ. We first express the partial trace of the projector of ψ^k in terms of $\tilde{\psi}^k$: $\psi^k = \Sigma_{i,j} \tilde{\psi}_{ij}^k e^i \otimes e^j$, hence

$$|\psi^k\rangle\langle\psi^k| = \sum_{i,j,p,q} \tilde{\psi}_{ij}^k (\tilde{\psi}_{pq}^k)^* (e^i \otimes e^j)(e^p \otimes e^q)^\dagger,$$

and the partial trace equals

$$\begin{aligned}
\rho_A^k = \mathrm{Tr}_B(|\psi^k\rangle\langle\psi^k|) &= \sum_{i,p} \left(\sum_q \tilde{\psi}_{iq}^k (\tilde{\psi}_{pq}^k)^* \right) (e^i)(e^p)^\dagger \\
&= \tilde{\psi}^k (\tilde{\psi}^k)^\dagger.
\end{aligned}$$

This is precisely the matrix B^k from the previous paragraph.

Remark: The entropy of this partial trace matrix ρ_A^k can be expressed in terms of the singular values of $\tilde{\psi}^k$. Let $\tilde{\psi}^k = U^k \Sigma^k V^k$ be the singular value decomposition of $\tilde{\psi}^k$ (that is, the Schmidt decomposition of ψ^k), with U^k unitary and V^k right-unitary (supposing that $N_1 \leqslant N_2$) and Σ^k a positive semidefinite diagonal matrix, then $\rho_A^k = U^k (\Sigma^k)^2 (U^k)^\dagger$ and $H(\rho_A^k) = H((\Sigma^k)^2) = -2\Sigma_i (\sigma_i^k)^2 \log_2(\sigma_i^k)$.

In the present framework only the eigenvectors ϕ^p are known, and the vectors ψ^k are to be sought by looking for an appropriate T-matrix. We therefore want to express ρ_A^k in terms of T and the ϕ^p. We get

$$w_k \rho_A^k = \sqrt{w_k} \tilde{\psi}^k \sqrt{w_k} (\tilde{\psi}^k)^\dagger = \sum_{p,q=1}^R T_{pk} T_{qk}^* \sqrt{m_p m_q} \tilde{\phi}^p (\tilde{\phi}^q)^\dagger.$$

Let us use the symbol $\Delta_k(T)$ as a shorthand for the right-hand side of the previous expression

$$\Delta_k(T) = \sum_{p,q=1}^R T_{pk} T_{qk}^* \sqrt{m_p m_q} \tilde{\phi}^p (\tilde{\phi}^q)^\dagger,$$

$$\rho_A^k = \Delta_k(T)/w_k,$$

$$w_k = \mathrm{Tr}\,\Delta_k(T) = (T^\dagger M T)_{kk}.$$

The last equation follows from the fact that ρ_A^k is normalized.

The EOF is thus:

$$E(\rho) = \min_{T,K} \sum_{k=1}^K w_k H(\rho_A^k) = \min_{T,K} \sum_{k=1}^K G[\Delta_k(T)], \qquad (7)$$

with

$$G(A) = -\mathrm{Tr}\{A \log_2[A/\mathrm{Tr}(A)]\} = H(A) - h[\mathrm{Tr}(A)]. \quad (8)$$

The minimum has to be taken over all $K \geqslant R$ and all $R \times K$ matrices T for which $TT^\dagger = \mathbb{1}_R$. Note that, since a state is separable iff its entropy of formation is zero, Eq. (7) gives an alternative for Eq. (6) for testing separability.

Equation (7) can be brought to a more suitable form if we enlarge the set of matrices $\tilde{\phi}^p$ with $K - R$ zero matrices for $p > R$. Then we can always use square and, therefore, unitary T matrices. Following a result by Uhlmann [12], the cardinality K must lie between the rank R and the square of the rank. This guarantees that the EOF can be found by restricting oneself to finite-sized T matrices.

E. Concurrence

The first analytic formula for calculating EOF has been found by Wootters [7] and is valid for 2×2 systems. A basic property used in deriving the formula is the so-called concurrence of a state. The concurrence is also useful for testing separability, because a 2×2 state is separable iff its concurrence equals zero. In this section we do two things: first we rederive Wootters's results in a shorter way, based on the concepts we have introduced above and using an interesting theorem from matrix analysis. This rederivation gives hints toward the generalization of the concurrence concept to higher-dimensional systems, which is the second topic of this section.

1. The 2×2 case

In this paragraph we give a shorter proof of Wootters's results on the EOF of 2×2 systems [7]. For the case of 2×2 systems, formula (5) becomes particularly simple, since there is only one 2×2 minor to consider, so that there is just a single symmetric matrix $A^{(\alpha)}$.

The concurrence of a pure state ψ equals $C(\psi)=|\psi^T S\psi|$. For the pure states ψ^k in a decomposition of ρ, we get $C(\psi^k)=|(\Psi^T S\Psi)_{kk}|=|(W^{-1/2}T^TATW^{1/2})_{kk}|=|(T^TAT)_{kk}|/w_k$.

The average concurrence of a realization of ρ is thus given by $\Sigma_k|(T^TAT)_{kk}|$ and the concurrence of ρ is the minimal average concurrence over all possible realizations, i.e., over all possible right-unitary matrices T. Since A is symmetric, its singular-value decomposition assumes a special form, known as the Takagi eigenvalue decomposition ([10], 4.4.4): $A=U^T\Sigma U$ (again, U is unitary and Σ is positive semidefinite diagonal). Since we consider all possible T, the matrix U can be absorbed in T, so that the expression for the concurrence becomes $\min_T\Sigma_k|(T^T\Sigma T)_{kk}|$. So, $T^T\Sigma T$ runs through all possible complex symmetric $K\times K$ matrices with R prescribed singular values Σ (if $K>R$ then $K-R$ zero singular values have to be added to Σ) and the average concurrence equals the sum of the moduli of the diagonal elements.

The following theorem by Thompson gives a precise relationship between the moduli of the diagonal elements of a complex square-symmetric matrix and its singular values [14].

Theorem 1 (Thompson). Let $d_1,\ldots,d_n$ be complex numbers and $s_1,\ldots,s_n$ nonnegative real numbers, enumerated so that $|d_1|\geqslant\cdots\geqslant|d_n|$ and $s_1\geqslant\cdots\geqslant s_n$. A complex symmetric matrix exists with $d_1,\ldots,d_n$ as its diagonal elements and $s_1,\ldots,s_n$ as its singular values, if and only if

$$\sum_{i=1}^{k}|d_i|\leqslant\sum_{i=1}^{k}s_i,\quad 1\leqslant k\leqslant n,$$

$$\sum_{i=1}^{k-1}|d_i|-\sum_{i=k}^{n}|d_i|\leqslant\left(\sum_{i=1,i\neq k}^{n}s_i\right)-s_k,\quad 1\leqslant k\leqslant n,$$

$$\sum_{i=1}^{n-3}|d_i|-|d_{n-2}|-|d_{n-1}|-|d_n|\leqslant\sum_{i=1}^{n-2}s_i-s_{n-1}-s_n.$$

The last inequality does not apply when $n<3$.
The second inequality gives, for $k=1$,

$$\sum_{i=1}^{n}|d_i|\geqslant s_1-\left(\sum_{i=2}^{n}s_i\right).$$

Applied to the problem at hand, we find that the minimal average concurrence must be $\sigma_1-(\Sigma_{i=2}^{K}\sigma_i)$, or zero if this quantity is negative. Here we have put $K=4$. Letting K be larger than 4 can give no improvement, since this amounts to just adding $K-4$ zero singular values, and this does not influence the inequalities of the theorem.

If $R<4$, we could try to decrease K to 3, but then the third inequality comes into play,

$$\sum_{i=1}^{3}|d_i|\geqslant-\left(\sigma_1-\sum_{i=2}^{3}\sigma_i\right),$$

so that

$$C(\rho)_{K=3}=|\sigma_1-\sigma_2-\sigma_3|.$$

Therefore, if $R=3$ and $\sigma_1-\sigma_2-\sigma_3<0$, putting $K=4$ gives zero concurrence, while $K=3$ gives nonzero concurrence. In other words, these states are separable in (at least) four product states ($K=4$). Furthermore, a rank-3 state is separable in three product states ($K=3$) iff $\sigma_1-\sigma_2-\sigma_3=0$.

If $R=2$, we can safely put $K=2$, since then the third inequality does not apply.

We have thus proven the following theorem.

Theorem 2. The concurrence of a 2×2 state with eigenvalue decomposition $\rho=\Phi M\Phi^\dagger$ equals

$$C(\rho)=\max\left(0,\sigma_1-\left(\sum_{i=2}^{R}\sigma_1\right)\right),$$

where σ_i are the singular values of the matrix

$$A=\sqrt{M}\Phi^T\sigma_y\otimes\sigma_y\Phi\sqrt{M},$$

sorted in descending order. The optimal cardinality K equals the rank R, except in the case when $R=3$ and $\sigma_1<\sigma_2+\sigma_3$, where the optimal K is 4.
Because of the statement about the optimal cardinality, this theorem is an improvement over Wootters's theorem.

2. Relation between concurrence and entanglement of formation

For the sake of completeness, we rephrase the rest of Wootters's results of [7] in the present setting.

The entanglement of a pure state is a convex, monotonic function $\mathcal{E}$ of the concurrence of the state: $E(\psi)=\mathcal{E}(C(\psi))$. Hence, the EOF, which is the average pure-state entanglement, equals

$$E(\rho)=\min_T\sum_k w_k\mathcal{E}(|(T^TAT)_{kk}|/w_k).$$

Because of the convexity of $\mathcal{E}$, this gives $E(\rho)\geqslant\min_T\mathcal{E}(\Sigma_k|(T^TAT)_{kk}|)$, where equality holds only if all

quantities $|(T^TAT)_{kk}|/w_k$ are equal. Using Thompson's theorem again and the monotonicity of $\mathcal{E}$, this minimum is equal to $\mathcal{E}(\sigma_1-\Sigma_{j>1}\sigma_j)=\mathcal{E}(C(\rho))$.

We therefore look for an optimal T matrix, yielding minimal average concurrence [thus equal to $C(\rho)$], and for which, additionally, all the quantities $|(T^TAT)_{kk}|/w_k$—the ensemble member concurrences—are equal [and thus also equal to $C(\rho)$]. There exists a T' for which $\Sigma_k(T'^TAT')_{kk}$ is equal to $C(\rho)$; indeed, with $A=U^T\Sigma U$, set $UT'=\mathrm{Diag}(1,i,i,\ldots,i)$, then $T'^TAT'=\mathrm{Diag}(1,-1,-1,\ldots,-1)\Sigma$, and the trace of this matrix is $\sigma_1-(\sigma_2+\ldots+\sigma_K)$. If this quantity is positive, it is equal to $C(\rho)$; if not, ρ is separable and we immediately have that a matrix T'' exists such that all $|(T''^TAT'')_{kk}|/w_k$ are equal (zero).

Concerning the nonseparable states, for any orthogonal matrix O, $\mathrm{Tr}(T'O)^TA(T'O)=\mathrm{Tr}\,T'^TAT'$. As shown in [7], using a suitable O we can make all $((T'O)^TAT'O)_{kk}$ equal to a constant α times w_k (exploiting the fact that T'^TAT' is a real diagonal matrix here). Summing over k then yields $C(\rho)=|\Sigma_k((T'O)^TAT'O)_{kk}|=|\alpha\Sigma_k w_k|=|\alpha|$, so that $((T'O)^TAT'O)_{kk}=C(\rho)w_k$. Then, $\Sigma_k|((T'O)^TAT'O)_{kk}|=C(\rho)$, so that $T=T'O$ is the matrix we were looking for.

If one is interested in obtaining the optimal ensemble exhibiting a member concurrence of $C(\rho)$, one is forced to actually calculate the required orthogonal matrix O. In [7] the existence of such an O is proven. Here, we show that O can be found as a product of three rotation matrices O_{12},O_{13},O_{14}, corresponding to rotations in the 12 plane, 13 plane, and 14 plane, respectively. For example,

$$O_{12}=\begin{pmatrix}\cos\phi_{12} & \sin\phi_{12} & 0 & 0\\ -\sin\phi_{12} & \cos\phi_{12} & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}.$$

After applying these rotations (with rotation angles ϕ_{1j} as yet to be determined), we get four different T matrices in succession: $T_1=T'$, $T_2=T_1O_{12}$, $T_3=T_2O_{13}$, and $T=T_4=T_3O_{14}$. The corresponding rotation angles are chosen so that after every step at least one member concurrence becomes equal to $C(\rho)$, i.e., $(T_j^TAT_j)_{jj}=C(\rho)(T_j^\dagger MT_j)_{jj}$ for $j=2$, 3, 4, respectively. Here we have used the formula $w_k=(T^\dagger MT)_{kk}$. Denoting $A_j=(T_j^TAT_j)$ and $B_j=(T_j^\dagger MT_j)$, this leads to the condition that the vector $(\sin\phi_{1j},\cos\phi_{1j})$ must be in the null space of the 2×2 submatrix of $A_{j-1}-C(\rho)B_{j-1}$ consisting of its first and jth rows and columns. A short calculation then yields the optimal rotation angle at each step. Note that in the last step ($j=4$) not only the fourth member concurrence should become equal to $C(\rho)$, but also the first one.

3. Towards a generalized concurrence

According to Eq. (5), a state is separable iff a right-unitary matrix T can be found such that the diagonal elements of every $T^TA^{(\alpha)}T$ are zero. In analogy with defining the average concurrence of a realization of a 2×2 state as the l_1 norm of the diagonal elements of T^TAT, in the general case we could define a *concurrence vector* as the vector of l_1 norms of the diagonal elements of $T^TA^{(\alpha)}T$,

$$C_{(\alpha)}(T)=\sum_k|(T^TA^{(\alpha)}T)_{kk}|. \tag{9}$$

A state is therefore separable iff a T exists such that the concurrence vector is zero. From the previous paragraph, a necessary condition then follows immediately:

$$\sigma_1^{(\alpha)}\leqslant\sum_{i=2}^{R}\sigma_i^{(\alpha)}\quad\forall(\alpha), \tag{10}$$

where the $\sigma_i^{(\alpha)}$ are the singular values of $A^{(\alpha)}$, sorted in descending order.

Unfortunately, this condition is not a sufficient one for separability. Numerical experiments showed that criterion (10) is weaker than the Peres criterion, which is a nonsufficient criterion itself. The main reason for this failure is that all the components of the vector concurrence (9) must be made zero by one and the same T. Typically, however, the matrices $A^{(\alpha)}$ all have different singular vectors (the rows of the U matrix), so that the $U^{(\alpha)}$ matrices in the decomposition $A^{(\alpha)}=U^{(\alpha)T}\Sigma^{(\alpha)}U^{(\alpha)}$ cannot all be absorbed in T at the same time.

It is easy, however, to find a stronger criterion than criterion (10): as Eq. (9) is linear in the matrices $A^{(\alpha)}$, the condition (10) must also hold for every linear combination of the matrices $A^{(\alpha)}$. Denoting the jth singular value (sorted in descending order) of the linear combination $\Sigma_{(\alpha)}x_{(\alpha)}A^{(\alpha)}$ by $\sigma_j(x)$, it follows that another, and potentially stronger, necessary condition for separability is given by

$$\max_{x\in\mathbb{C}^M}\sigma_1(x)-\sum_{j=2}^{R}\sigma_j(x)\leqslant0, \tag{11}$$

where M is the number of tuples (α). Again, one could choose to consider all possible $A^{(\alpha)}$ or just the minimal subset with $(\alpha)=(i,i+1,j,j+1)$.

Numerical experiments now showed that criterion (11) is actually stronger than the Peres criterion, provided *all* $A^{(\alpha)}$ are used. In the section on numerical results we will give an example where condition (11) even seems to be sufficient for determining separability. It would be very interesting if one could prove this to be true for every state, but we have not yet been able to do this.

In the remainder of this paragraph, we will present another possible generalization of the concurrence. This generalization has the benefit that we can prove that a state is separable iff its generalized concurrence is zero, but it also has the drawback that it is as hard to calculate as the entanglement of formation. Some properties of this generalized concurrence are presented and a number of open questions are formulated.

Consider first the pure states. A pure state ψ is a product state iff $\tilde{\psi}$ is a rank-1 matrix. This means that all 2×2 minors of $\tilde{\psi}$ must be zero. Denote the generalization of the matrix $S=\sigma_y\otimes\sigma_y$ to the $n_1\times n_2$ case as

$$S=(\sigma_y\oplus 0_{n_1-2})\otimes(\sigma_y\oplus 0_{n_2-2}). \tag{12}$$

The matrix $\psi^T S\psi$ then picks out one specific 2×2 minor of $\tilde{\psi}$. In order to consider all minors, we can apply local unitary operations to the state ψ and put the result again under the action of S. Specifically, we define the generalized concurrence of a pure state as follows.

Definition 1. The generalized concurrence of a pure state $|\psi\rangle$ is

$$C(\psi)=\max_{U,V}|\psi^T(U\otimes V)^T S(U\otimes V)\psi|, \tag{13}$$

where the maximum is taken over all special unitary matrices $U\in \mathrm{SU}(n_1)$ and $V\in \mathrm{SU}(n_2)$.

Theorem 3. The generalized concurrence of a pure state ψ with $\tilde{\psi}=U_1\Sigma V_1^T$ and $\Sigma=\mathrm{diag}(\sigma_1,\sigma_2,\ldots,\sigma_n)$ $[n=\min(n_1,n_2)]$ equals

$$C(\psi)=2\sigma_1\sigma_2, \tag{14}$$

independent of the dimensions of the system. A pure state is a product state if its generalized concurrence is zero.

Proof. Rewriting $\tilde{\psi}=U_1\Sigma V_1^T$ in vector form, we have $\psi=U_1\otimes V_1\mathrm{vec}\Sigma=U_1\otimes V_1\Sigma_i\sigma_i e^i\otimes e^i$, with e^i being a basis vector of the standard vector basis. Let also $e^{ij}=e^i(e^j)^T$ be a basis vector of the standard matrix basis. Then

$$\begin{aligned}C(\psi)&=\max_{U,V}\left|\sum_{i,j}\sigma_i\sigma_j\mathrm{Tr}[(e^{ij}\otimes e^{ij})(U\otimes V)^T S(U\otimes V)]\right|\\&=\max_{U,V}\Big|\sum_{i,j}\sigma_i\sigma_j\mathrm{Tr}[e^{ij}U^T(\sigma_y\oplus 0)U]\\&\quad\times\mathrm{Tr}[e^{ij}V^T(\sigma_y\oplus 0)V]\Big|\\&=\max_{U,V}\left|\sum_{i,j}\sigma_i\sigma_j w_{ij}\right|,\end{aligned}$$

with

$$w=u\circ v=[U^T(\sigma_y\oplus 0)U]\circ[U^T(\sigma_y\oplus 0)U]. \tag{15}$$

Here, $\circ$ denotes the Hadamard product (componentwise, product).

Denoting by $|w|$ the matrix obtained from w by taking the absolute values of all matrix entries, we can easily prove that every row sum and every column sum of $|w|$ is not larger than 1, and the sum of all entries of $|w|$ is not larger than 2.

Now, as u and v are antisymmetric, w is symmetric and has a zero diagonal. Therefore, w and $|w|$ lie in the span of the generalized Pauli matrices $\sigma_{x,ij}=e^{ij}+e^{ji}$. Moreover, by the above sum statements, and noting that the sum of all entries of every σ_x is equal to 2, we have that $|w|$ must lie in the convex closure of the set $\mathcal{S}=\{0\}\cup\{\sigma_{x,ij};i<j\}$. Hence,

$$\begin{aligned}C(\psi)&=\max_{U,V}\left|\sum_{i,j}\sigma_i\sigma_j w_{ij}\right|\leqslant\max_{U,V}\sum_{i,j}\sigma_i\sigma_j|w_{ij}|\\&\leqslant\max_{w\in S}\sum_{i,j}\sigma_i\sigma_j|w_{ij}|=\max_{k<l}\sum_{i,j}\sigma_i\sigma_j(\sigma_{x,kl})_{ij}\\&=2\max_{k<l}\sigma_k\sigma_l=2\sigma_1\sigma_2.\end{aligned}$$

Here we have used the well-known fact that the constrained maximum of a linear function over a convex set is reached on an extreme point of the set. We, therefore, find an upper bound on $C(\psi)\leqslant 2\sigma_1\sigma_2$. Moreover, this bound can be reached by setting $U=V=\mathbb{1}$, which gives $w=\sigma_y\oplus 0$ and $|w|=\sigma_{x,12}$. This proves the theorem.

We now turn our attention to mixed states.

Definition 2. The generalized concurrence of a mixed state ρ is the minimal generalized concurrence of all ensembles that realize ρ,

$$C(\rho)=\min_{\{p_i,\psi^i\}}\sum_i p_i\max_{U^i,V^i}|\psi^{iT}(U^i\otimes V^i)^T S(U^i\otimes V^i)\psi^i|. \tag{16}$$

Again, U^i and V^i are special unitary matrices.

Theorem 4. The generalized concurrence function is convex, i.e., $C(x\rho_1+[1-x]\rho_2)\leqslant xC(\rho_1)+(1-x)C(\rho_2)$.

Proof. Actually, any function f defined in this way is convex: starting from an f defined on pure states, first extend the definition to ensembles of pure states as the ensemble average of the fs of the pure states; then to mixed states as the minimal value of f of all possible realizing ensembles. Let $\{p_{i;j},\psi^{i;j}\}$ $(j=1,2)$ be an optimal realizing ensemble of ρ_j. Then $\{xp_{i;1},\psi^{i;1}\}\cup\{(1-x)p_{i;2},\psi^{i;2}\}$ is a realizing ensemble of $x\rho_1+(1-x)\rho_2$ with ensemble f equal to $xf(\rho_1)+(1-x)f(\rho_2)$. As this combined ensemble need not be optimal, $f(x\rho_1+[1-x]\rho_2)$ could be smaller than this ensemble f, but, in any case, it is not larger.

The first important question, concerning the relevance of this definition of generalized concurrence, is: is it true that ρ is separable if and only if $C(\rho)=0$? It is easy to see that this is indeed the case.

Theorem 5. A mixed state ρ is separable if and only if $C(\rho)=0$.

Proof. A state ρ is separable iff it is contained in the convex closure of the set of pure product states. A pure state is a product state iff it has zero concurrence. By the previous theorem it then follows that if a state ρ is separable, then its concurrence cannot exceed the value of zero. From the definition of concurrence we see that negative values cannot occur, so the concurrence of ρ must equal zero. On the other hand, if a state ρ has zero concurrence, then, by the definition of concurrence, there must exist an ensemble realizing ρ in which every pure state has zero concurrence. Hence, these pure states are product states and ρ is separable.

Consider the pure state sets $\psi_C=\{\psi:C(\psi)=C\}$. By the convexity of C, every mixed state in the convex closure of ψ_C has $C(\rho)\leqslant C$. Letting C run from its minimal to its

maximal value, we get a one-parameter family of convex subsets $\mathrm{conv}(\psi_C)$ of the total state space. A given state ρ with concurrence $C(\rho)$ can only belong to those convex subsets with $C \geqslant C(\rho)$.

By its very definition, the generalized concurrence is a locally invariant measure: any local unitary rotation can be absorbed in the U^i and V^i. In the 2×2 case this definition reduces to the conventional one for concurrence due to the special property of matrices $U \in \mathrm{SU}(2)$ that $U^T \sigma_y U = \sigma_y$.

While this generalization of concurrence has a number of desirable properties, it also has a number of undesirable ones: first of all, the generalized concurrence is *not generally* an entanglement monotone (EM). According to a theorem concerning entanglement monotones in Ref. [15] (Theorem 3), the restriction of any EM to pure states should yield a unitarily invariant concave function of the partial trace of the pure state. In this case, this function equals $f = 2\sqrt{\lambda_1 \lambda_2}$, where $\lambda_{1,2}$ are the two largest eigenvalues of the partial trace [this follows from the fact that $\mathrm{Tr}_B(\psi\psi^\dagger) = \tilde{\psi}\tilde{\psi}^\dagger = U\Sigma^2 U^\dagger$, where $\tilde{\psi} = U\Sigma V$]. However, this function is not concave as can be readily checked numerically, unless this partial trace is a 2×2 matrix, i.e., we are dealing with a $2\times N$ system.

Secondly, the entanglement of formation will in general not be related to this generalized concurrence even for pure states: while the former depends on all Schmidt coefficients σ_i, the latter depends only on the two largest ones. So only for $2\times N$ systems is there an unambiguous relation between generalized concurrence and EOF (the same relation as in the 2×2 case). Furthermore, it remains to be proven that in the mixed-state case, an optimal ensemble can be found for which every member has a generalized concurrence equal to the generalized concurrence of the mixed state.

III. NUMERICAL RESULTS

In this section we present an application of the variational characterizations of separability and EOF. Since these characterizations involve looking for the minimum of a function over a finite-dimensional manifold, it must be possible to find a numerical algorithm that actually calculates that minimum. As a result, it must be possible to calculate the EOF for *any* bipartite state and, moreover, to give the optimal realization of the state (from the optimal T matrix).

Actually, such an approach has already been taken by Zyczkowski [16], who used the method of simulated annealing in order to find the global minimum. Unfortunately, while this method is generally known for its good local-minima-avoidance properties, it requires an inordinate amount of iteration steps if high accuracy is required. If one is interested in calculating and comparing the EOF of a family of parametrized states, a large number of significant digits is required. In our experience, this is only possible in a reasonable amount of time when the utmost attention is given to the gradient-following properties of the method, especially when considering larger system dimensions.

In the following paragraphs, we present a minimization algorithm that is based on a conjugate-gradient method. To avoid local minima, the algorithm is executed a number of times starting from different initial values. It achieves very high accuracy (up to 10 significant digits) in a relatively short time (on a 300-MHz PC it takes typically 1 min for a 3×3 state). We then apply the algorithm to the calculation of EOF for certain families of 3×3 states.

A. Algorithm for minimization

Our algorithm for calculating the entanglement of formation is based on a modified conjugate-gradient minimization procedure. Starting from an initial point $T = T_0$, conjugate-gradient algorithms iteratively seek a direction along which progress in minimizing the objective function $g(T)$ is maximal and then perform a so-called line search to actually find the minimum along that direction. Recall from Sec. II D that

$$E(\rho) = \min_{T,K} \sum_{k=1}^{K} G(\Delta_k(T)),$$

so that, in the present case

$$g(T) = \sum_{k=1}^{K} G(\Delta_k(T)).$$

We see here that minimization is to be done over the unitary manifold. This manifold is not Euclidean, so that the standard line search has to be replaced by a geodesic search [17]. A geodesic on the unitary manifold is a one-parameter subgroup of the unitary group: $T(t) = T_0 \exp(tX)$, where X is a skew-Hermitian matrix giving the direction (tangent vector) of the geodesic. Through a geodesic search one looks for the optimal t for which $g[T_0 \exp(tX)]$ is minimal.

In steepest-descent minimization, the direction for the line search is taken to be minus the gradient of the objective function in the current point. Conjugate-gradient methods improve on this by taking the direction of the previous step also in account; if not, the progress made in the previous step could be partly undone by the new iteration. We have used a modification of the Polak-Ribière formula for calculating the search direction [18]; the search direction for iteration i is based on the gradient at the current point and on the search direction for the previous iteration $i-1$,

$$X_i = -(\nabla g)_i + \gamma X_{i-1},$$

$$\gamma = \frac{\langle (\nabla g)_i - \tau(\nabla_g)_{i-1}, (\nabla g)_i \rangle}{\langle (\nabla g)_{i-1}, (\nabla g)_{i-1} \rangle},$$

where $\langle , \rangle$ is the inner product of the embedding space, being in this case the standard Hilbert-Schmidt inner product $\langle x, y \rangle = \mathrm{Tr}\, xy^\dagger$. The symbol τ denotes parallel transport of the gradient vector at the $(i-1)$th point to the ith point along the geodesic [17],

$$\tau(\nabla_g)_{i-1} = \exp(X_{i-1}t_{i-1}/2)(\nabla_g)_{i-1} \exp(-X_{i-1}t_{i-1}/2).$$

For the line search, we have used the method described in [18], again modified to take into account that the search is performed along the geodesic $g(T_i \exp(tX_i))$.

Any minimization algorithm actually finds local minima. To find the global minimum, we select a number of starting points at random and let the minimization algorithm work from these points. The minimum is then taken over all the results. While this procedure does not guarantee that the global minimum is actually found, we found that trying about ten starting points gives satisfactory results.

B. Calculation of the gradient

In this paragraph we give an analytic expression for the gradient of the target function $g(T)$. Conjugate-gradient methods perform better if an explicit expression is given; in the absence of such an expression, the gradient has to be approximated numerically.

To calculate the gradient, we have to select an arbitrary direction or tangent vector X, which for the unitary manifold is a skew-Hermitian matrix. The geodesic on the unitary manifold along this direction and passing through T_0 is given by $T_\epsilon = T_0 \exp(\epsilon X)$ or $T_0(\mathbb{1}+\epsilon X)$, for small ϵ. The gradient of a scalar function on the manifold can be calculated from the variation of the function along the geodesic using

$$\frac{\partial f(T_\epsilon)}{\partial \epsilon} = \langle \nabla f, X \rangle,$$

where $\langle , \rangle$ is the Hilbert-Schmidt inner product.

The gradient of the target function $g(T)$ is given as follows.

Lemma 2.

$$(\nabla g(T))_{kp}|_{T=1} = \mathcal{G}(Q^{pk}, Q_{pp}) - \mathcal{G}(Q^{pk}, Q^{kk}),$$

where

$$Q^{pq} = \sqrt{m_p m_q}\, \tilde{\phi}^p (\tilde{\phi}^q)^\dagger$$

and

$$\mathcal{G}(B,A) = -\operatorname{Tr} B \log_2 \frac{A}{\operatorname{Tr} A}.$$

The details of the calculation are given in Appendix B.

C. Results

As a preliminary test, we have calculated the entanglement of formation of several states of a 2×2 system, and compared the numerical values with those obtainable from Wootters's formula. Furthermore, we considered a one-parameter family of 3×3 states called isotropic states, and compared the numerical values with the EOF calculated from Terhal and Vollbrecht's formula [8]. In all cases, agreement was complete within numerical-machine precision, except for some isotropic states where there was a very small deviation from the formula for parameter values close to $\frac{8}{9}$. This can be explained by the fact that for these parameter values, there are two local minima of the target function that are extremely close in value, and that the minimum with lowest value has a very small "basin of attraction." Situations like this are tough nuts for any numerical routine to crack.

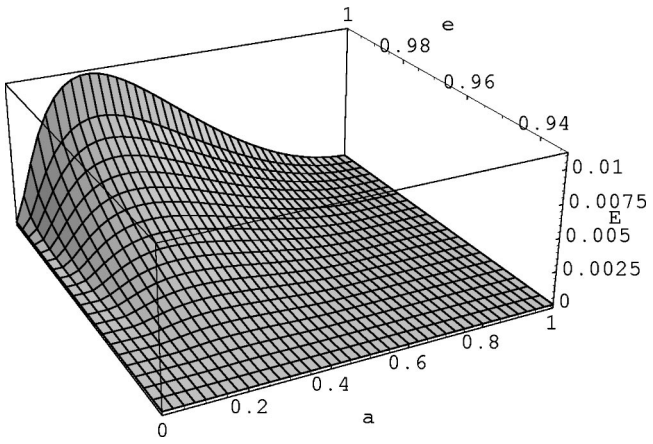

FIG. 1. Entanglement of formation for Horodecki states as a function of a and e; linear scale.

The first interesting results were obtained on the Horodecki 3×3 states [11]. These states were introduced to show that the Peres criterion is not sufficient for determining separability. These states exhibit *bound entanglement*: their entanglement of formation is nonzero, while their entanglement of distillation is zero (they have positive partial transposition). The density matrix of a Horodecki 3×3 state is

$$\rho(a) = \frac{1}{1+8a}\begin{bmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 & c \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & c & 0 & b \end{bmatrix},$$

where a is a parameter between 0 and 1, inclusively, and $b = (1+a)/2$ and $c = \sqrt{1-a^2}/2$. Note that, since these states are not full rank (their rank is 7) and neither is their partial transpose, these states lie on the boundary of the set of states and also on the boundary of the set of bound entangled states.

The result of the calculation is shown in Fig. 1. Here the entanglement of formation has been calculated for a mixture of the Horodecki states with the maximally mixed state $e\rho(a) + (1-e)\mathbb{1}/9$. In Fig. 1, the scale is linear, while in Fig. 2 the scale is logarithmic, so that the borderline of the set of separable states is clearly visible. The "floor" in the logarithmic picture at -10 is an artifact; the algorithm stops when the entanglement gets below 10^{-10}.

Note from these results that the Horodecki states have a rather low entanglement of formation (about 0.0109 for $a = 0.225$) and that their distance to the manifold of separable

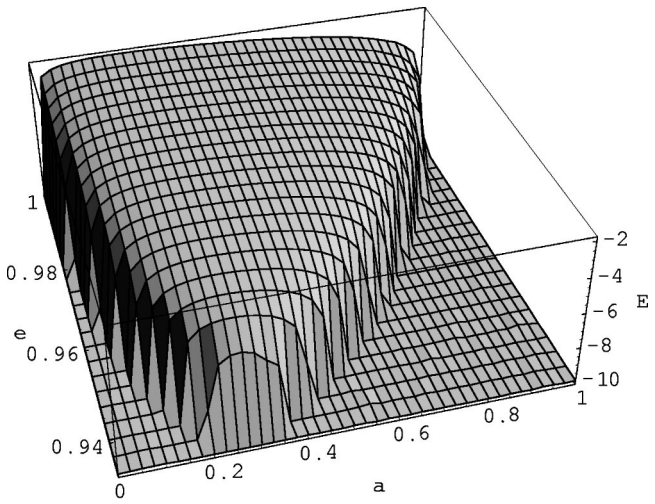

FIG. 2. Entanglement of formation for Horodecki states as a function of a and e; logarithmic scale.

states is also small ($e=0.93$ for $a=0.225$, that is, mixing the state with just 7% of the identity destroys all entanglement). At first sight, the fact that the appearance of the set of separable states is not convex might seem confusing. However, the parameter a appears in a nonlinear way in the density matrix so that the matrices lie on a nonrectilinear curve in the Euclidean state space. The figure, on the other hand, has a as parameter and therefore gives a distorted image.

Figure 3 shows the entanglement of formation for the particular value of $a=0.225$ and for e going to 1. From this figure, we are led to conjecture that the derivative to e becomes infinite at $e=1$.

The above-mentioned calculations have been performed with the cardinality K set to 14. Figure 4 shows the effect of using different K in the calculations; here $e=1$ and $a=0.225$. It is seen that the value $K=14$ is optimal for calculating the entanglement of formation in this case.

For these same Horodecki states, we have also tested the conjectured condition for separability [Eq. (11)] based on the generalized concurrence. It turned out, quite surprisingly, that the condition correctly pinpointed all separable states, which was verified by comparing the results to Fig. 2. This leads us to hope that Eq. (11) might be an important step

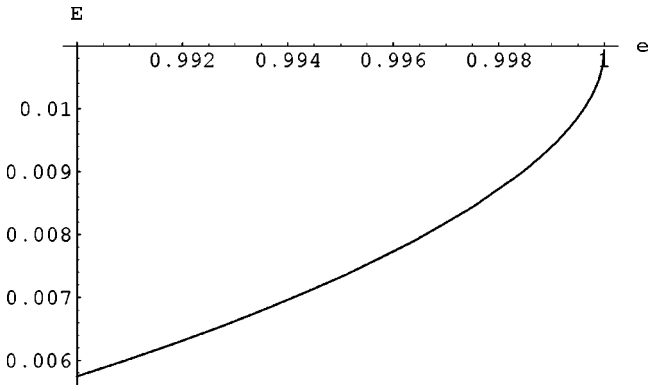

FIG. 3. Entanglement of formation for Horodecki state $a=0.225$ as a function of e; linear scale.

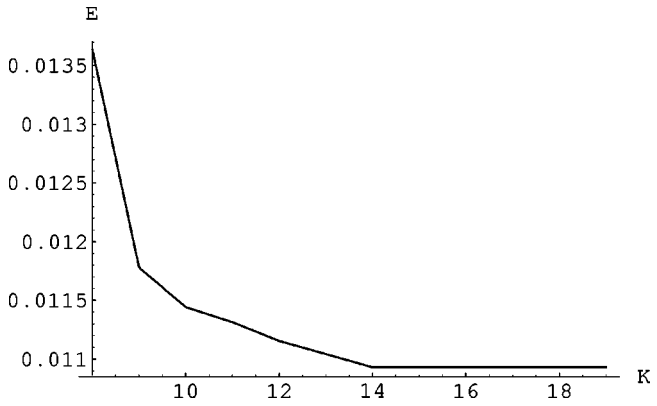

FIG. 4. Effect of cardinality on calculation of entanglement of formation.

towards finding a simple and efficient operational criterion for testing separability.

IV. CONCLUSIONS

We have presented a matrix analytical framework within which the questions of separability of mixed states and calculating their entanglement of formation can be formulated in an elegant and practical way. A main result is that, at least in principle, it is now possible to calculate the EOF of any state, or determining whether it is a separable state or not. Of course, for larger dimensions the subproblem of minimizing the respective target function becomes increasingly more time consuming. Not only the EOF itself, but also an optimal ensemble realizing the state can be calculated.

We have extended results on the concurrence and EOF of 2×2 systems by also including the cardinality of the optimal ensembles. More importantly, we have tried to generalize the concept of concurrence to general systems and have shown that this generalized concurrence has potential to supply a fast test for separability of general bipartite states.

In the future, we will use the presented methods to generate more numerical results about EOF of higher-dimensional states, for example, to chart the ''unknown territory'' of bound-entangled states, or just as a means for testing various conjectures. Another interesting topic for future work is trying to prove the conjectured sufficiency of the generalized concurrence test for separability.

ACKNOWLEDGMENTS

We thank Nicolas Cerf, Henri Verschelde, Roland Puystjens, Jeroen Dehaene, Lieven De Lathauwer, Bob Lockhart, and Karol Zyczkowski for useful comments and discussions. This work was supported by several institutions: the Flemish Government (Research Council K. U. Leuven: Concerted Research Action Mefisto-666; FWO Projects Nos. G.0240.99 and G.0256.97, and Research Communities ICCoS and ANMMM; IWT projects EUREKA 2063-IMPACT and STWW), the Belgian State (IUAP P4-02 and IUAP P4-24; Sustainable Mobility Program, Project No. MD/01/24), the European Commission (TMR Networks: ALAPEDES and System Identification; Brite/Euram Thematic Network

NICONET and Industrial Contract Research (ISMC, Electrabel, Laborelec, Verhaert, Europay). The scientific responsibility is assumed by the authors.

APPENDIX A: PRESELECTION OF *T* MATRIX

The topic of this appendix is a method for reducing the set of T matrices over which the minimum (5) has to be taken in a separability test. In some cases the method already yields the optimal T matrix without need for performing a minimization procedure. This method is based on a method used in blind identification for array processing [19].

Consider the expression

$$\sum_{p,q} B_{pq} A_{pq}^{(\alpha)},$$

where $A_{pq}^{(\alpha)}$ is as defined in Eq. (4) and B_{ij} is a symmetric matrix. When we substitute Eq. (2) in it, we get, using bilinearity of C,

$$\begin{aligned}\sum_{p,q} B_{pq} A_{pq} &= \sum_{p,q=1}^{R} B_{pq} C(\sqrt{m_p}\phi^p, \sqrt{m_q}\phi^q) \\ &= \sum_{p,q=1}^{R} B_{pq} \sum_{k,l=1}^{K} T_{kp}^{\dagger} T_{lq}^{\dagger} \sqrt{w_k w_l} C(\psi^k, \psi^l) \\ &= \sum_{k,l=1}^{K} \left(\sum_{p,q=1}^{R} B_{pq} T_{kp}^{\dagger} T_{lq}^{\dagger} \right) \sqrt{w_k w_l} C(\psi^k, \psi^l) \\ &= \sum_{k,l=1}^{K} (T^{\dagger} B T^{*})_{kl} \sqrt{w_k w_l} C(\psi^k, \psi^l).\end{aligned}$$

Note that, just like B, $(T^{\dagger}BT^{*})$ is also symmetric.

Suppose that the state ρ is indeed a separable one, then there exist matrices T leading to a product-state decomposition, i.e., to $C(\psi^k, \psi^l)$ being identically zero for $k=l$. Consider one such matrix T. There exist symmetric matrices B for which $(T^{\dagger}BT^{*})$ is diagonal, say equal to some Λ. Indeed, by right unitarity of T one just has to take

$$B = T \Lambda T^{T}. \tag{A1}$$

Using such a B in the above expression, we find

$$\sum_{p,q} B_{pq} A_{pq}^{(\alpha)} = 0 \tag{A2}$$

for all α.

We can now reverse the reasoning and say that any T leading to a product-state decomposition must be found from some symmetric B that satisfies Eq. (A2). That is, instead of searching for a T in the complete set of unitary matrices, we only have to consider T that follow, using Eqs. (A1) and (A2), from such B. If T is square (that is, $K=R$), T is unitary, and since $B = T \Lambda T^{T}$,

$$\begin{aligned} BB^{*} &= T \Lambda T^{T} T^{*} \Lambda^{*} T^{\dagger} \\ &= T |\Lambda|^{2} T^{\dagger}. \end{aligned}$$

Hence, the column vectors of T must be the eigenvectors of BB^{*}. Given then, all the symmetric matrices B that satisfy Eq. (A2), we only have to consider matrices T whose column vectors are the eigenvectors of one such BB^{*}.

We have thus found a general method for reducing the search space. We will now show that under some conditions this reduced search space contains nothing but the optimal T, so that no search has to be done at all. In that case, one just has to take one B satisfying Eq. (A2), and construct a T from its eigenvectors. The first requirement for this is that the cardinality K must equal the rank R, so that T is then unitary; the reason is that otherwise Eq. (A1) has no unique solution. Let us suppose that the first $P(P \leqslant K)$ state vectors in the ensemble realizing ρ are product vectors: $|\psi^k\rangle = |\alpha^k\rangle \otimes |\beta^k\rangle, 1 \leqslant k \leqslant P$. Therefore, $C(\psi^k, \psi^k)$ will be zero for $k \leqslant P$. Now, the matrices $C(\psi^k, \psi^l)$ for $k<l$ and $k=l>P$ are in general (that is, for all states except for a subset of measure zero) linearly independent as long as the number of matrices does not exceed the number of matrix elements. If the latter requirement is not fulfilled, then of course a dependence must exist between the matrices. If the requirement is fulfilled then the matrices can still be dependent provided the K vectors ψ^k (being $m = KN_1N_2$ complex variables) satisfy a system of $N_1(N_1-1)N_2(N_2-1)/4 - K(K-1)/2 - K + P + 1$ polynomial equations of degree $d = K(K-1) + 2(K-P)$ [each equation corresponds to a minor of rank $K(K-1)/2 + K - P$ of a matrix containing $(\Psi^{T} S^{(\alpha)} \Psi)_{kl}$ as elements]. Using the Schwarz-Zippel theorem [20], we find that the set of vectors obeying just one of those polynomial equations has measure zero with respect to the set of all possible sets of K vectors. *A fortiori*, this also holds for the set of vectors obeying all polynomial equations. We thus get a second requirement for the automatic optimality of T, namely, that the cardinality K must satisfy the inequality

$$\frac{K(K-1)}{2} + K - P \leqslant \frac{N_1(N_1-1)}{2} \frac{N_2(N_2-1)}{2}. \tag{A3}$$

It then follows that $\Sigma_{p,q} B_{pq} A_{pq}$ can only be zero if $(T^{\dagger}BT^{*})_{kl} = 0$ for all $k \neq l$ and $k = l > P$. In other words, $(T^{\dagger}BT^{*})$ is necessarily a diagonal matrix for *any* B satisfying Eq. (A2), and any T obeying Eq. (A1) for such a B is optimal.

We have not investigated whether this technique for reducing the search space is also applicable for calculating the EOF, that is, whether some T that is optimal with respect to Eq. (7) can be found in the reduced search space.

APPENDIX B: CALCULATION OF THE GRADIENT OF THE AVERAGE ENTANGLEMENT

The geodesic on the unitary manifold along a direction X (skew-Hermitian matrix) and passing through T_0 is given by $T_{\epsilon} = T_0 \exp(\epsilon X)$ or $T_0(1 + \epsilon X)$, for small ϵ. The gradient of a

scalar function on the manifold can be calculated from the variation of the function along the geodesic using

$$\frac{\partial f(T_\epsilon)}{\partial \epsilon} = \langle \nabla f, X \rangle.$$

To avoid notational clutter, we have set T_0 equal to $\mathbb{1}$ in the rest of the appendix.

Let us recollect that the function of T that is to be minimized is $g(T) = \Sigma_k G(\Delta_k(T))$, where $G(A) = -\mathrm{Tr}(A \log_2[A/A\mathrm{Tr}(A)])$ and $\Delta_k(T) = \Sigma_{p,q=1}^{R} T_{pk} T_{qk}^* \sqrt{m_p m_q}\, \tilde{\phi}^p (\tilde{\phi}^q)^\dagger$.

Lemma 3. For Hermitian A and B,

$$\frac{\partial}{\partial \epsilon} G(A+\epsilon B)\bigg|_{\epsilon=0} = \mathcal{G}(B,A),$$

where

$$\mathcal{G}(B,A) = -\mathrm{Tr}(B \log_2 A) + \mathrm{Tr}(B) \log_2 \mathrm{Tr}(A).$$

Proof. We use the following formula from [21] (formula 6.6.31), which applies for a Hermitian matrix $A(t)$ function of a parameter t with eigendecomposition $A(t) = U(t)\Lambda(t)U(t)^\dagger$, and for analytic functions f,

$$\frac{d}{dt} f(A(t)) = U[(\Delta f(\lambda_i, \lambda_j))_{ij} \circ U^\dagger A' U] U^\dagger.$$

Here, $\circ$ is the Hadamard product and $\Delta f(\lambda_i(t), \lambda_j(t))$ are the ''divided differences''

$$\Delta f(\lambda_i(t), \lambda_j(t)) = \begin{cases} \dfrac{f(\lambda_i(t)) - f(\lambda_j(t))}{\lambda_i(t) - \lambda_j(t)} & \text{for } i \neq j \\ f'(\lambda_i(t)) & \text{for } i = j \end{cases}.$$

For $A(t) = A + tB$, it follows that

$$\frac{d}{dt} \mathrm{Tr}\, f(A(T))\bigg|_{t=0} = \sum_i \Delta f(\lambda_i(t), \lambda_i(t)) (U^\dagger B U)_{ii}$$
$$= \mathrm{Tr}\, f'(\Lambda) U^\dagger B U = \mathrm{Tr}\, f'(A) B.$$

Setting $f(x) = h(x) = -x \log_2(x)$ so that $f(A) = H(A)$, we have $f'(x) = -(1 + \ln x)/\ln 2$ and

$$\frac{d}{dt} \mathrm{Tr}\, H(A+tB)\bigg|_{t=0} = -\mathrm{Tr}(\mathbb{1} + \ln A) B / \ln 2.$$

Furthermore,

$$\frac{d}{dt} h(A+tB)\bigg|_{t=0} = -(1 + \ln \mathrm{Tr}\, A)\, \mathrm{Tr}\, B / \ln 2,$$

so that the lemma follows.

Proceeding in a similar fashion, we can expand $\Delta_k(T_\epsilon)$ up to first order in ϵ. Putting $Q^{pq} = \sqrt{m_p m_q}\, \tilde{\phi}^p (\tilde{\phi}^q)^\dagger$,

$$\Delta_k(T_\epsilon) = \sum_{p,q} T_{pk} T_{qk}^* Q_{pq}$$
$$= \sum_{p,q} [\delta_{pk}\delta_{qk} + \epsilon(X_{pk}\delta_{qk} + \delta_{pk} X_{qk}^*)] Q^{pq}$$
$$= Q^{kk} + \epsilon \sum_p (X_{pk} Q^{pk} - X_{kp} Q^{kp}),$$

where we have used the fact that X is skew Hermitian. Inserting this expression in $(\partial/\partial\epsilon)\Sigma_k G(\Delta_k(T_\epsilon))|_{\epsilon=0}$ we see that Q^{kk} serves the role of ''A'' and $\Sigma_p (X_{pk} Q^{pk} - X_{kp} Q^{kp})$ that of ''B.'' Exploiting linearity of $\mathcal{G}$ with respect to its first argument, we arrive at the expression

$$\frac{\partial g(T_\epsilon)}{\partial \epsilon} = \sum_{p,k} X_{pk} (\mathcal{G}(Q^{pk}, Q^{kk}) - \mathcal{G}(Q^{pk}, Q^{pp}))$$

(in the last term we have interchanged the indices k and p). Therefore,

$$(\nabla g(T))_{kp}|_{T=1} = \mathcal{G}(Q^{pk}, Q^{pp}) - \mathcal{G}(Q^{pk}, Q^{kk}).$$

[1] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[2] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[3] M. Lewenstein, D. Bruß, J. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach, e-print quant-ph/0006064.
[4] B. Terhal, e-print quant-ph/0101032.
[5] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996).
[6] V. Vedral, M. Plenio, M. Rippin, and P. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[7] W. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[8] B. Terhal and K. Vollbrecht, e-print quant-ph/0005062.
[9] L. Hughston, R. Jozsa, and W. Wootters, Phys. Lett. A **183**, 14 (1993).
[10] R. Horn and C. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, England, 1985).
[11] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[12] A. Uhlmann, e-print quant-ph/9704017 (1997).
[13] B. Lockhart, J. Math. Phys. **41**, 6766 (2001).
[14] R. C. Thompson, Linear Algebr. Appl. **26**, 65 (1979).
[15] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[16] K. Zyczkowski, Phys. Rev. A **60**, 3496 (1999).
[17] J. Dehaene, Cheng Yi, and B. De Moor, IEEE Trans. Autom. Control **42**, 1596 (1997).
[18] R. Fletcher, *Practical Methods of Optimization* (Wiley,

New York, 1987).
[19] J.-F. Cardoso, in *Proceedings of ICASSP '91*, (IEEE, Piscataway, NJ, 1991), Vol. 5, pp. 3109–3112.
[20] R. Zippel, in *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM '79), Marseille, France, 1979*, edited by E. Ng, Lecture Notes in Computer Science Vol. 72 (Springer, New York 1979), pp. 216–226.
[21] R. Horn and C. Johnson, *Topics in Matrix Analysis* (Cambridge University Press, Cambridge, England, 1991).