Entanglement Criteria for All Bipartite Gaussian States

G. Giedke,[1] B. Kraus,[1] M. Lewenstein,[2] and J. I. Cirac[1]

[1]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*

[2]*Institut für Theoretische Physik, Universität Hannover, 30163 Hannover, Germany*

(Received 10 April 2001; revised manuscript received 9 July 2001; published 1 October 2001)

We provide a necessary and sufficient condition for separability of Gaussian states of bipartite systems of arbitrarily many modes. The condition provides an operational criterion since it can be checked by simple computation. Moreover, it allows us to find a pure product-state decomposition of any given separable Gaussian state. We also show that all bipartite Gaussian states with nonpositive partial transpose are distillable.

DOI: 10.1103/PhysRevLett.87.167904 PACS numbers: 03.65.Ud, 03.65.Ca, 03.67.Hk

Entanglement is the basic ingredient in the philosophical implications of quantum theory. It also plays a crucial role in some fundamental issues of this theory, such as decoherence or the measurement process. Furthermore, it is the basis of most applications in the field of quantum information. However, in spite of their importance, the entanglement properties of systems are far from being understood. In particular, we do not even know how to answer the following question [1]: given two systems A and B in a state described by a density operator ρ, are those systems entangled? This question constitutes the so-called separability problem, and it represents one of the most important theoretical challenges of the emerging theory of quantum information.

During the last few years a significant amount of work in the field of quantum information has been devoted to the separability problem [2]. Until now, the basic tool to study this problem is a *linear* map called partial transposition. Introduced in this context by Peres [3], it provides us with a necessary condition for a density operator to be separable. This condition turns out to be also sufficient in two cases: (a) A and B are two qubits or one qubit and one qutrit [4]; (b) A and B are two modes (continuous variable systems) in a Gaussian state [5]. Thus, in these cases the separability problem is fully solved. However, for higher dimensional systems as well as in the case in which A and B consist of several modes in a joint Gaussian state, partial transposition alone does not provide a general criterion for separability. In both cases, examples of states which in spite of being entangled satisfy the partial transposition criterion have been found [6,7].

In this Letter we solve the separability problem for Gaussian states of an arbitrary number of modes per site. Our method does not rely in any sense on partial transposition, and therefore is entirely different from the ones that have been introduced so far to study this problem [2]. It is based on a *nonlinear* map f: $\gamma_N \rightarrow \gamma_{N+1}$ between matrices γ_N which reveals whether a state ρ is an entangled state or not. In addition, we show that if ρ is entangled and has nonpositive partial transpose then it is distillable [2,8].

Let us start by fixing the notation and recalling some properties of correlation matrices (CMs). A Gaussian state of n modes is completely characterized by a matrix $\gamma \in M_{2n,2n}$ (the set of $2n \times 2n$ matrices), called correlation matrix [9], whose elements are directly measurable quantities. A matrix $\gamma \in M_{2n,2n}$ is a CM if it is real, symmetric, and $\gamma - iJ_n \geq 0$. Here we use [10]

$$J_n \equiv \oplus_{k=1}^{n} J_1, \qquad J_1 \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{1}$$

In the following we will consider two systems A and B, composed of n and m modes, respectively, in a Gaussian state. The corresponding CM will be written as

$$\gamma_0 = \begin{pmatrix} A_0 & C_0 \\ C_0^T & B_0 \end{pmatrix} \geq iJ_{n,m} \tag{2}$$

where $A_0 \in M_{2n,2n}$ and $B_0 \in M_{2m,2m}$ are CM themselves, $C_0 \in M_{2n,2m}$ and $J_{n,m} \equiv J_n \oplus J_m$. In order to simplify the notation, when it is clear from the context we will not write the subscripts to the matrices J and we will not specify the dimensions of the matrices involved in our derivations. In [7] it was shown that a CM of the form (2) is separable (i.e., it corresponds to a separable state) iff there exist two CMs $\gamma_{A,B}$, such that

$$\gamma_0 \geq \gamma_A \oplus \gamma_B . \tag{3}$$

This condition, even though it can be very useful to show that some particular states are entangled [7,11], cannot be directly used in practice to determine whether an arbitrary state is entangled or not, since there is no way of determining $\gamma_{A,B}$ in general. If one can determine them, however, then one can automatically construct an explicit decomposition of the corresponding density operator as a convex combination of product states [7].

Below we present a criterion which allows one to determine whether a given CM, γ_0, is separable or not. To this aim, we define a sequence of matrices $\{\gamma_N\}_{N=0}^{\infty}$ of the form (2). The matrix γ_{N+1} is determined by a discrete map defined as follows: (i) if γ_N is not a CM then $\gamma_{N+1} = 0$;

(ii) if γ_N is a CM then

$$A_{N+1} \equiv B_{N+1} \equiv A_N - \mathrm{Re}(X_N), \tag{4a}$$

$$C_{N+1} \equiv -\mathrm{Im}(X_N), \tag{4b}$$

where $X_N \equiv C_N(B_N - iJ)^{-1}C_N^T$ [12]. Note that for $N \geq 1$ we have that $A_N = A_N^T = B_N$ and $C_N = -C_N^T$ are real matrices. The importance of this sequence is that γ_0 is separable iff γ_N is a valid separable CM, and, after some finite number of iterations, γ_N acquires a form in which separability is simple to check. Moreover, starting from that CM we are able to construct the CMs $\gamma_{A,B}$ of Eq. (3) for the original γ_0. Now we state several propositions from which the above results follow. For two technical lemmas, see the Appendix.

First we show that if γ_N is separable, so is γ_{N+1}. Moreover, the CMs $\gamma_{A,B}$ associated to γ_N [cf. Eq. (3)] allow us to construct the corresponding CMs for γ_{N+1}.

Proposition 1: *If for some CMs $\gamma_{A,B}$, we have $\gamma_N \geq \gamma_A \oplus \gamma_B$ then $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$.*

Proof: We use the equivalence (i)–(iii) of Lemma 1 to obtain that $B_N - C_N^T(A_N - \gamma_A)^{-1}C_N \geq \gamma_B \geq iJ$, where the last inequality follows from the fact that γ_B is a CM. Using the equivalence (ii)–(iii) of Lemma 1 we obtain $\gamma_A \leq A_N - C_N(B_N - iJ)^{-1}C_N^T = A_{N+1} + iC_{N+1}$, where we have also used the map (4). According to Lemma 2, this immediately proves the proposition. ■

Now, we show that the converse of Proposition 1 is true. That is, if γ_{N+1} is separable, so is γ_N. Apart from that, the following proposition exhibits how to construct the matrices $\gamma_{A,B}$ [cf. Eq. (3)] related to γ_N starting from the ones corresponding to γ_{N+1}.

Proposition 2: *If for some CM γ_A we have $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$ then $\gamma_N \geq \gamma_A \oplus \gamma_B$ for the CM*

$$\gamma_B \equiv B_N - C_N^T(A_N - \gamma_A)^{-1}C_N. \tag{5}$$

Proof: We use Lemma 2 and the map (4) to transform the inequality $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$ into $A_N - C_N(B_N - iJ)^{-1}C_N^T \geq \gamma_A$. According to the equivalence (ii)–(iii) of Lemma 1 this implies that $\gamma_B \geq iJ$. Since it is clear from its definition (5), γ_B is also real and symmetric, it is a CM. On the other hand, using the equivalence (i)–(iii) of Lemma 1 we immediately obtain that $\gamma_N \geq \gamma_A \oplus \gamma_B$. ■

Using the fact that for $N \geq 1$, $A_N = B_N$ and the symmetry of the corresponding matrix γ_N we have

Corollary 1: *Under the conditions of Proposition 2, we have $\gamma_N \geq \tilde{\gamma}_A \oplus \tilde{\gamma}_A$, and $\tilde{\gamma}_A \equiv (\gamma_A + \gamma_B)/2 \geq iJ$ is a CM.*

The above propositions imply that γ_0 is separable iff γ_N is separable for all $N > 0$. Thus, if we find some γ_N fulfilling (3) then γ_0 is separable. Thus, we can establish now the main result of this work.

Theorem 1 (separability criterion):

(1) If for some $N \geq 1$ we have $A_N \ngeq iJ$ then γ_0 is not separable.

(2) If for some $N \geq 1$ we have

$$L_N \equiv A_N - \|C_N\|_{\mathrm{op}}\mathbb{1} \geq iJ \tag{6}$$

then γ_0 is separable [13].

Proof: (1) It follows directly from Proposition 1; (2) We will show that $\gamma_N \geq L_N \oplus L_N$, so that according to Proposition 2 γ_0 is separable. We have

$$\gamma_N = L_N \oplus L_N + \begin{pmatrix} \|C_N\|_{\mathrm{op}}\mathbb{1} & C_N \\ C_N^T & \|C_N\|_{\mathrm{op}}\mathbb{1} \end{pmatrix}, \tag{7}$$

so that we just have to prove that the last matrix is positive. But using Lemma 1 this is equivalent to $\|C_N\|_{\mathrm{op}}^2\mathbb{1} \geq C_N^T C_N$, which is always the case. ■

This theorem tells us how to proceed in order to determine if a CM is separable or not. We just have to iterate the map (4) until we find that either A_N is no longer a CM or L_N is a CM. In the first case, we have that γ_0 is not separable, whereas in the second one it is separable. If we wish to find a decomposition of the corresponding density operator as a convex sum of product vectors we simply use the construction given in Corollary 1 until $N = 1$ and then the one of Proposition 2. This will give us the CMs $\gamma_{A,B}$, such that $\gamma_0 \geq \gamma_A \oplus \gamma_B$, from which the decomposition can be easily found [7].

In order to check how fast our method converges we have taken families of CMs and applied to them our criterion. We find that typically with less than five iterations we are able to decide whether a given CM is entangled or not. The most demanding states for the criterion are those which lie very close to the border of the set of separable states (see Proposition 3 below). We challenged the criterion by applying it to states close to this border and still the convergence was very fast (always below 30 steps). Figure 1 illustrates this behavior. We have taken $n = m = 2$ modes, an entangled CM γ_a of the GHZ form [14] (Fig. 1a) and an entangled CM γ_b with positive partial transpose [7] (Fig. 1b). We produced two families of CMs as $\gamma_{a,b}(\epsilon) = \gamma_{a,b} + \epsilon\mathbb{1}$. We have determined $\epsilon_{a,b}$

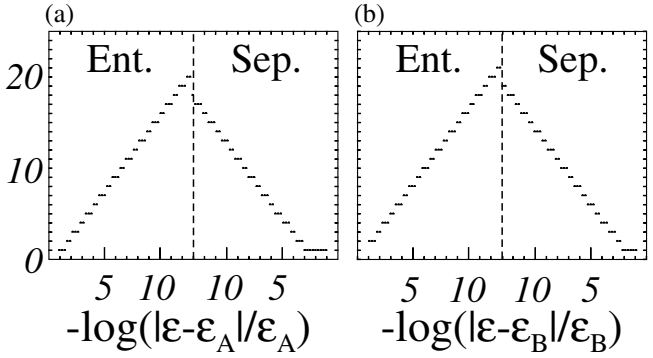

FIG. 1. Number of steps as a function ϵ for CMs of the form $\gamma_{a,b}(\epsilon) = \gamma_{a,b} + \epsilon\mathbb{1}$ where: (a) γ_a taken from Eq. (1) in Ref. [14] with $r = 1/4$, and $\epsilon_a = 0.305\,774\,915\,510(1)$; (b) γ_b taken from Eq. (9) in Ref. [7] and $\epsilon_b = 0.097\,866\,790\,222\,8(4)$.

such that $\gamma_{a,b}(\epsilon)$ become separable. In Fig. 1 we see that in both cases, as we approach $\epsilon_{a,b}$ exponentially fast, the number of needed steps increases linearly. The same behavior is found using instead of $\mathbb{1}$ other positive projectors with different ranks and for different initial CMs. Even though we have tested numerically the rapid convergence of our method, we still have to prove that, except for a zero measure set, it can decide whether a CM is entangled or not after a finite number of steps [15]. We start by considering the set of separable states, defined by $\gamma_0 \geq \gamma_A \oplus \gamma_B$ with $\gamma_{A,B} \geq iJ$. If we just consider those with $\gamma_A > iJ$, we will omit a zero measure set. But then we can show that after a *finite* number of steps these separable states will be detected by our procedure.

Proposition 3: *If* $\gamma_0 \geq \gamma_A \oplus \gamma_B$ *with* $\gamma_A \geq iJ + \epsilon\mathbb{1}$, *then there exists some*

$$N < N_0 \equiv \frac{1}{\epsilon}\left(\|A_0\|_{\mathrm{tr}} - 2n\right) + 1\,, \tag{8}$$

for which condition (6) is fulfilled.

Proof: Using Proposition 1 we have that for all N,

$$A_N - iJ \geq \epsilon\mathbb{1}\,. \tag{9}$$

Thus, $0 \leq \mathrm{Re}(X_N) = A_N - A_{N+1}$. Since all the matrices in this expression are positive, taking the trace norm we have $\|A_N\|_{\mathrm{tr}} - \|A_{N+1}\|_{\mathrm{tr}} = \|\mathrm{Re}(X_N)\|_{\mathrm{tr}}$. Adding both sides of this equation from $N = 0$ to N_0, taking into account that $\|\cdots\|_{\mathrm{tr}} \geq \|\cdots\|_{\mathrm{op}}$, and $\|\mathrm{Re}(X_N)\|_{\mathrm{op}} \geq \|C_{N+1}\|_{\mathrm{op}}$ [since $\mathrm{Re}(X_N) \geq \pm i\,\mathrm{Im}(X_N)$], we have

$$\sum_{N=0}^{N_0-1} \|C_{N+1}\|_{\mathrm{op}} \leq \|A_0\|_{\mathrm{tr}} - \|A_{N_0}\|_{\mathrm{tr}} \leq \|A_0\|_{\mathrm{tr}} - 2n\,,$$

where the last inequality is a consequence of the fact that $A_N \geq iJ$ for all N. Thus, among $\{C_N\}_{N=1}^{N_0}$ there must be at least one for which $\|C_N\|_{\mathrm{op}} \leq \epsilon$. Thus, $A_N - \|C_N\|_{\mathrm{op}}\mathbb{1} \geq A_N - \epsilon\mathbb{1} \geq 0$ where for the last inequality we have used Eq. (9), and therefore, for that particular value of N, condition (6) must be fulfilled. ■

It is worth stressing that from the proof of Proposition 3 it follows directly that if γ_0 is separable, then the sequence γ_N converges to a fixed point $\gamma_\infty = A_\infty \oplus B_\infty$, where $A_\infty = B_\infty \geq iJ$ are CMs. For the sake of completeness, we now show that if γ_0 is inseparable, then we can always detect it in a finite number of steps. We will use the fact that the CMs of inseparable Gaussian states form an open set, a fact that follows directly from condition (3). Therefore, if γ_0 is inseparable, there always exist $\epsilon_0 > 0$ such that if $\epsilon < \epsilon_0$ then $\gamma_0 + \epsilon\mathbb{1}$ is still inseparable and thus condition (6) is never fulfilled. However, if γ_0 were separable, then, according to Proposition 3, $\gamma_0 + \epsilon\mathbb{1}$ should fulfill that condition before reaching $N = N_0$. This can be summarized as follows.

Corollary 2: *If* γ *is inseparable then there exists some* $\epsilon > 0$ *such that starting out from* $\gamma_0 = \gamma + \epsilon\mathbb{1}$, *condition (6) is not fulfilled for any* $N \leq N_0 \equiv (\|A_0\|_{\mathrm{tr}} - 2n)/\epsilon$.

Together, Proposition 3 and Corollary 2 show that — whether γ_0 is separable or not, and except for a set of measure zero — we will be able to detect it in a finite number of steps. However, as mentioned above, according to our numerical calculations we see that the process always converges very fast and in practice one can directly use the method sketched after Theorem 1.

To conclude this Letter, we show that not only separability but also distillability [2,8], can be determined for all Gaussian states. The proof is based on the result that for 1×1 Gaussian states nonpositive partial transpose (npt) implies distillability [16]. This result can be extended to *all* bipartite Gaussian states, i.e., a Gaussian density matrix ρ is distillable iff its partial transpose is not positive. For the proof, it suffices to show that any $n \times m$ npt Gaussian state can be locally transformed into an 1×1 npt Gaussian state. This is achieved as follows: For Gaussian states, the npt condition is equivalent to $\gamma \not\geq i\tilde{J}$ [7]. Hence, for every npt CM γ there exists a vector $z = z_A \oplus z_B \in \mathbb{C}^{2(n+m)}$ such that for some $\epsilon > 0$ we have

$$z^\dagger(\gamma - i\tilde{J})z \leq -\epsilon < 0\,. \tag{10}$$

It is always possible to pick z such that $(\mathrm{Re}z_x)^T J\,\mathrm{Im}z_x \neq 0$ for both $x = A, B$. But then there exist symplectic maps S_A, S_B such that S_x maps $\mathrm{span}\{\mathrm{Re}z_x, \mathrm{Im}z_x\}$ to $\mathrm{span}\{e_1, e_2\}$ [17]. It follows that $\hat{z}_x \equiv S_x^{-1} z_x$ have nonzero entries only in the first two components. Thus not only is $\hat{z}^\dagger[(S_A \oplus S_B)^T \gamma (S_A \oplus S_B) - i\tilde{J}]\hat{z} < 0$ but by construction this still holds for the CM of the *reduced state* obtained by discarding all but the first mode at each side. Discarding subsystems is a local operation, hence all npt Gaussian states can be transformed locally into an npt 1×1 state and are thus distillable by [16]. ■

To summarize, we have obtained a necessary and sufficient condition for Gaussian states to be separable. The condition provides an operational criterion in that it can be easily checked by direct computation. It is worth mentioning that our criterion can be used to study the separability properties with respect to bipartite splittings of multipartite systems in Gaussian states [11,18]. Our criterion is based on a nonlinear map that is more powerful than partial transposition. In addition we proved that a bipartite Gaussian state is distillable if and only if it has nonpositive partial transpose. While in general, i.e., for non-Gaussian states, both the separability and the distillability problems remain open, these results represent a significant step towards understanding the separability problem, which is one of the most challenging problems in the field of quantum information. With the results presented here, one can decide for any bipartite Gaussian state by direct computation whether it is distillable and/or inseparable: it is distillable iff it is npt, and it is separable iff $\gamma_N \geq iJ\ \forall\ N$.

G. G. thanks the Friedrich-Naumann-Stiftung for financial support. This work was supported by the Austrian Science Found (SFB "Control and Measurement of Coherent Quantum Systems," Project 11), the EU (EQUIP,

contr. IST-1999-11053), the ESF, the Institute for Quantum Information GmbH Innsbruck, and the DFG (SFB 407 and SPP "Quanteninformationsverarbeitung").

Appendix.— In this Appendix we present the lemmas which are needed in order to prove Propositions 1 and 2. Let us consider three real matrices $0 \leq A = A^T \in M_{n,n}$, $0 \leq B = B^T \in M_{m,m}$, $C \in M_{n,m}$, and

$$M = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} = M^T \in M_{n+m,n+m}\,. \tag{11}$$

Lemma 1: *The following statements are equivalent:*
(i) $M \geq 0$.
(ii) $\ker(B) \subseteq \ker(C)$ *and* $A - CB^{-1}C^T \geq 0$.
(iii) $\ker(A) \subseteq \ker(C^T)$ *and* $B - C^TA^{-1}C \geq 0$ [12].

Proof: We will just prove the first equivalence since the other one is analogous. We use that $M \geq 0$ iff for any two real vectors $a \in \mathbb{R}^n$ and $b \in \mathbb{R}^m$

$$a^TAa + b^TBb + a^TCb + b^TC^Ta \geq 0\,. \tag{12}$$

Conversely, $A - CB^{-1}C^T \geq 0$ iff for any $a \in \mathbb{R}^n$ we have

$$a^TAa - a^TCB^{-1}C^Ta \geq 0\,. \tag{13}$$

(i) $\Rightarrow$ (ii): We assume (12). First, $\ker(B) \subseteq \ker(C)$ since otherwise we could always choose a $b \in \ker(B)$ so that $-2a^TCb > a^TAa$. Second, if we choose $b = -B^{-1}C^Ta$ then we obtain (13). (ii) $\Rightarrow$ (i): We now assume (13). Then, $A = CB^{-1}C^T + P$, where $P \geq 0$. Defining $\tilde{a} \equiv B^{-1}C^Ta$, we have that $C^Ta = B\tilde{a}$ [since $\ker(B) \subseteq \ker(C)$], and thus the left-hand side of (12) can be expressed as $a^TPa + (\tilde{a} + b)^TB(\tilde{a} + b)$, which is positive. ■

In the derivations of Propositions 1 and 2 we have not included explicitly the conditions imposed by the present lemma on the kernels of B and C. However, one can easily verify that all the problems that may arise from these kernels are eliminated by using pseudoinverses [12] instead of inverses of matrices.

Let us consider two real matrices $A = A^T \in M_{n,n}$ and $C = -C^T \in M_{n,n}$, and

$$M = \begin{pmatrix} A & C \\ C^T & A \end{pmatrix} = M^T \in M_{2n,2n}\,. \tag{14}$$

Lemma 2: $M \geq 0$ iff $A + iC \geq 0$.

Proof: This follows from the observation that M is real, and that for any pair of real vectors $a, b \in \mathbb{R}^N$ we have $(a - ib)^\dagger(A + iC)(a - ib) = (a \oplus b)^TM(a \oplus b)$. ■

[1] R. Werner, Phys. Rev. A **40**, 4277 (1989).
[2] For a review of the problem and its progress see, e.g., M. Lewenstein *et al.,* J. Mod. Opt. **47**, 2481 (2000); P. Horodecki *et al.,* J. Quant. Inf. Comp. **1**, 45 (2001).
[3] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[4] M. Horodecki *et al.,* Phys. Lett. A **223**, 1 (1996).
[5] L.-M. Duan *et al.,* Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[6] P. Horodecki, Phys. Lett. A **232**, 333 (1997); C. H. Bennett *et al.,* Phys. Rev. Lett. **82**, 5385 (1999).
[7] R. Werner *et al.,* Phys. Rev. Lett. **86**, 3658 (2001).
[8] C. Bennett *et al.,* Phys. Rev. A **54**, 3824 (1996); M. Horodecki *et al.,* Phys. Rev. Lett. **80**, 5239 (1998).
[9] If X_k, P_k are position- and momentum-like operators in each mode with canonical commutator $[X_k, P_k] = i$, we define $\gamma_{kl} \equiv 2\,\mathrm{Re}[\langle (R_k - d_k)(R_l - d_l)\rangle]$, where $d_k = \langle R_k\rangle \equiv \mathrm{tr}(\rho R_k)$ and $R_{2k-1} = X_k$ and $R_{2k} = P_k$ $(k = 1, \ldots, n)$.
[10] For convenience we use direct sum notation for matrices and vectors. That is, if $A \in M_{n,n}$ and $B \in M_{m,m}$, $A \oplus B \in M_{n+m,n+m}$ is a block diagonal matrix of blocks A and B. Similarly, if $f_1 \in \mathbb{R}^n$ and $f_2 \in \mathbb{R}^m$ are two vectors, then $f_1 \oplus f_2 \in \mathbb{R}^{n+m}$ is a vector whose first n components are given by the entries of f_1 and the last m by those of f_2.
[11] G. Giedke *et al.,* e-print quant-ph/01030137 [Phys. Rev. A (to be published)].
[12] Throughout this work we will denote by B^{-1} the pseudoinverse of B, that is, $BB^{-1} = B^{-1}B$ is the projector on the range of B.
[13] $\|A\|_{\mathrm{tr}} \equiv \mathrm{tr}(A^\dagger A)^{1/2}$ denotes the trace norm of A. The operator norm of A, $\|A\|_{\mathrm{op}}$ is the maximum eigenvalue of $(A^\dagger A)^{1/2}$.
[14] P. v. Loock *et al.,* Phys. Rev. A **63**, 022106 (2001).
[15] Note that the existence of a zero measure set which cannot be characterized in a finite number of steps is not particular for our method, but a simple consequence of finite precision. E.g., if we have a density matrix ρ for two qubits such that the partial transpose has a negative eigenvalue $-\epsilon$, it will be increasingly difficult to check whether $\rho^T \geq 0$ as $\epsilon \to 0$.
[16] G. Giedke *et al.,* e-print quant-ph/0007061 [J. Quant. Inf. Comp. (to be published)].
[17] V. I. Arnold, *Mathematical Methods of Classical Mechanics* (Springer-Verlag, New York, 1989), 2nd ed.
[18] W. Dür *et al.,* Phys. Rev. Lett. **83**, 3562 (1999); Phys. Rev. A **61**, 042314 (2000).