Characterizing Entanglement via Uncertainty Relations

Otfried Gühne

Institut für Theoretische Physik, Universität Hannover, Appelstraße 2, D-30167 Hannover, Germany
(Received 28 June 2003; revised manuscript received 6 November 2003; published 18 March 2004)

We derive a family of necessary separability criteria for finite-dimensional systems based on inequalities for variances of observables. We show that every pure bipartite entangled state violates some of these inequalities. Furthermore, a family of bound entangled states and true multipartite entangled states can be detected. The inequalities also allow us to distinguish between different classes of true tripartite entanglement for qubits. We formulate an equivalent criterion in terms of covariance matrices. This allows us to apply criteria known from the regime of continuous variables to finite-dimensional systems.

The detection of entanglement is one of the fundamental problems in quantum information theory. From a theoretical point of view, one can try to answer the question whether a given entirely known state is entangled or not but, despite a lot of progress in past years [1], no general solution of this problem is known. In experiments, one aims at detecting entanglement without knowing the state completely. Bell inequalities [2] and entanglement witnesses [3] are the main tools to tackle this task. Both rely on inequalities for *mean values* of observables, and violation of them implies entanglement. Entanglement criteria based on inequalities for *variances* of observables have also been studied, mainly designed for continuous variable systems [4]. Recently, it has been shown that variances of observables of a special type can detect entanglement also in finite-dimensional bipartite systems [5]. Even an example of bound entanglement, allowing detection in this way, has been found [6].

In this Letter, we present a generalization of this approach by considering arbitrary observables. This leads to new results in various directions. First, we show how the entanglement of every pure bipartite entangled state can be detected with our method. Second, we present inequalities for the detection of a class of bound entangled states. Third, we show how multipartite entanglement can be detected. Our approach even admits to distinguish different classes of true multipartite entanglement. Finally, we show that our criteria are equivalent to a criterion in terms of covariance matrices. This formulation allows us to translate separability criteria known from continuous variables [7,8] to finite-dimensional systems.

We start with the following observation. Let ϱ be a density matrix, and let M be an observable. We denote the expectation value of M by $\langle M \rangle_\varrho := \mathrm{Tr}(\varrho M)$ and the variance (or uncertainty) of M by

$$\delta^2(M)_\varrho := \langle (M - \langle M \rangle_\varrho)^2 \rangle_\varrho = \langle M^2 \rangle_\varrho - \langle M \rangle_\varrho^2. \quad (1)$$

We suppress the dependence on ϱ in our notation, when there is no risk of confusion. If ϱ is a pure state, the variance is zero iff ϱ is an eigenstate of M. Now we have the following.

Lemma 1.—Let M_i be some observables and $\varrho = \sum_k p_k \varrho_k$ be a convex combination (i.e., $p_k \geq 0$, $\sum_k p_k = 1$) of some states ϱ_k within some subset S. Then

$$\sum_i \delta^2(M_i)_\varrho \geq \sum_k p_k \sum_i \delta^2(M_i)_{\varrho_k} \quad (2)$$

holds. We call a state "violating Lemma 1" iff there are no states $\varrho_k \in S$ and no p_k such that Eq. (2) is fulfilled.

Proof.—This fact is known (see, e.g., [5,9]). The inequality holds for each M_i: $\delta^2(M_i)_\varrho = \sum_k p_k \langle (M_i - \langle M_i \rangle_\varrho)^2 \rangle_{\varrho_k} = \sum_k p_k [\delta^2(M_i)_{\varrho_k} + (\langle M_i \rangle_{\varrho_k} - \langle M_i \rangle_\varrho)^2] \geq \sum_k p_k \delta^2(M_i)_{\varrho_k}$. □

Please note that this Lemma has a clear physical meaning: One cannot decrease the uncertainty of an observable by mixing several states.

In most cases we will be interested in separable states. They can be written as a convex combination of product states. So, unless stated otherwise, we will assume that in Lemma 1 the set S denotes the set of product states. Violation of this Lemma implies entanglement of the state ϱ, which can be detected with uncertainties. In fact, the main idea of this paper is to show that Eq. (2) yields strong sufficient entanglement criteria, if we choose the M_i appropriately.

For completeness, let us remind the reader of the so-called "local uncertainty relations" (LURs), introduced by Hofmann and Takeuchi [5]. Let A_i be observables on Alice's space of a bipartite system. If they do not share a common eigenstate, there is a number $C_A > 0$ such that $\sum_i \delta^2(A_i)_{\varrho_A} \geq C_A$ holds for all states ϱ_A on Alice's space. Hofmann and Takeuchi showed the following.

Proposition 1.—Let ϱ be separable and let A_i, B_i, $i = 1, \ldots, n$ be operators on Alice's (respectively, Bob's) space, fulfilling $\sum_{i=1}^n \delta^2(A_i)_{\varrho_A} \geq C_A$ and $\sum_{i=1}^n \delta^2(B_i)_{\varrho_B} \geq C_B$. We define $M_i := A_i \otimes \mathbb{1} + \mathbb{1} \otimes B_i$. Then

$$\sum_{i=1}^n \delta^2(M_i)_\varrho \geq C_A + C_B \quad (3)$$

holds.

The LURs provide strong criteria which can by construction be implemented with local measurements. Nevertheless, they have some disadvantages: It is not clear which operators A_i and B_i one should choose to detect a given entangled state. Also, LURs can by construction characterize separable states only; they do not apply for other convex sets. Finally, it is not clear how to generalize them to multipartite systems. In fact, no LUR for the detection of true multipartite entanglement in finite-dimensional systems is known thus far.

A way to overcome these disadvantages is to consider *nonlocal* observables. For an experimental implementation, one can decompose any nonlocal observable into local operators, i.e., write it as a sum of projectors onto product vectors [10]. Each of the terms in this sum can then be measured locally. The measurement of a nonlocal observable in this way has recently been implemented [11]. Let us start with the case of two qubits.

Proposition 2.—Let $|\psi_1\rangle = a|00\rangle + b|11\rangle$ be an entangled two qubit state written in the Schmidt decomposition, with $a \geq b$. Then, there exist M_i such that, for $|\psi_1\rangle$, $\sum_i \delta^2(M_i)_{|\psi_1\rangle\langle\psi_1|} = 0$ holds, while for separable states

$$\sum_i \delta^2(M_i) \geq 2a^2b^2 \qquad (4)$$

is fulfilled. The M_i are explicitly given (see below).

Proof.—We define $|\psi_2\rangle = a|01\rangle + b|10\rangle$, $|\psi_3\rangle = b|01\rangle - a|10\rangle$, $|\psi_4\rangle = b|00\rangle - a|11\rangle$, and further $M_i := |\psi_i\rangle\langle\psi_i|$, $i = 1, \ldots, 4$. Then $\sum_i \delta^2(M_i)_{|\psi_1\rangle\langle\psi_1|} = 0$. We only need to prove the bound (4) for a pure product vector $|\phi\rangle$. We have $\sum_{i=1}^4 \delta^2(M_i)_{|\phi\rangle\langle\phi|} = 1 - \sum_i(|\langle\phi|\psi_i\rangle|^2)^2$. Now, we use the fact that $|\langle\phi|\psi_i\rangle|^2 \leq a^2$. To see this, we expand $|\psi_i\rangle$ in a product basis $|\psi_i\rangle = \sum_{kl} C_{kl}^i|kl\rangle$ and also any product vector: $|a,b\rangle = \sum_{kl} a_k b_l|kl\rangle$. Then $\max_{|a,b\rangle}|\langle a,b|\psi_i\rangle| = \max_{a_m,b_n}|\sum_{m,n} a_m^* C_{mn}^i b_n| = \max\{\mathrm{sv}(C^i)\}$ holds, where $\mathrm{sv}(C^i)$ are the singular values of C^i, i.e., the Schmidt coefficients of $|\psi_i\rangle$. With this bound we have $\sum_i(|\langle\phi|\psi_i\rangle|^2)^2 \leq (a^2)^2 + (1 - a^2)^2$ and finally $\delta^2(M_i)_{|\phi\rangle\langle\phi|} \geq 2a^2b^2$. □

Note that Eq. (4) allows one to detect a mixed state of the form $\varrho(p) = p|\psi_1\rangle\langle\psi_1| + (1-p)\mathbb{1}/4$ for $p \geq \sqrt{1 - 8a^2b^2/3}$.

The idea to take one M_i as the projector onto the range of ϱ, and the others as projectors onto a basis of the kernel, can be applied also to other cases.

Proposition 3.—Let $|\psi_1\rangle$ be an entangled pure state in a bipartite $N \times M$ system. Then $|\psi_1\rangle$ violates Lemma 1 for properly chosen M_i.

Proof.—Let U be the space orthogonal to $|\psi_1\rangle$. It is clear that U contains at least one entangled vector $|\psi_e\rangle$.

We can choose a basis $|\psi_i\rangle$, $i = 2, \ldots, NM$ of U which consists only of entangled vectors. (To do this, we choose an arbitrary, not necessarily orthogonal, basis. If it contains product vectors, we perturb them by adding $\varepsilon|\psi_e\rangle$.) Then we take $M_i = |\psi_i\rangle\langle\psi_i|$. The only possible common eigenstates of the M_i are the $|\psi_i\rangle$. So for product states the sum over all uncertainties is bounded from below, while it is zero for $|\psi_1\rangle$. □

The class of bound entangled states which we want to consider are those arising from an unextendible product basis (UPB) [12]. They can be constructed as follows: Let $\{|\phi_i\rangle = |e_i\rangle|f_i\rangle, i = 1, \ldots, n\}$ be a UPB, i.e., all $|\phi_i\rangle$ are (pairwise orthogonal) product vectors, not spanning the whole space, and there is no product vector orthogonal to all $|\phi_i\rangle$. Then the state

$$\varrho_{\mathrm{UPB}} := \mathcal{N}\left(\mathbb{1} - \sum_i|\phi_i\rangle\langle\phi_i|\right) \qquad (5)$$

is a bound entangled state. $\mathcal{N}$ denotes the normalization.

Proposition 4.—Let ϱ_{UPB} be a bound entangled state, constructed from a UPB. Then ϱ_{UPB} violates Lemma 1 for appropriate M_i.

Proof.—Let U be the subspace spanned by the UPB. Then U must contain at least one entangled vector. To see this, note that subspaces containing only product vectors are of the form $\{|v\rangle = |a\rangle|b\rangle\}$ with a fixed $|a\rangle$ (or $|b\rangle$) for all $|v\rangle$. There would then be product vectors orthogonal to U. Because of the existence of an entangled vector in U, there is, according to the proof of Proposition 3, an entangled basis $|\psi_i\rangle$; $i = 1, \ldots, n$ of U. We take $M_i = |\psi_i\rangle\langle\psi_i|$; $i = 1, \ldots, n$ and $M_{n+1} = \mathbb{1} - \sum_i|\phi_i\rangle\langle\phi_i|$. The common eigenstates of the M_i are not product vectors, and we have $\sum_i \delta^2(M_i)_{\varrho_{\mathrm{UPB}}} = 0$. □

Before we demonstrate that our method is also useful for multipartite systems, we recall some facts about three-qubit systems [13,14]. A three-qubit state is called fully separable iff it can be written as a convex combination of triseparable pure states, and it is called biseparable (BS) iff it is a convex combination of pure states, which are separable with respect to a bipartite splitting. Otherwise, it is called fully entangled. There are two classes of fully entangled states which are not convertible into each other by stochastic local operations and classical communication. These classes are called the *GHZ* class and the *W* class, and the *W* class forms a convex set inside the *GHZ* class [14]. The following inequalities are formulated so that they can be checked with local measurements.

Proposition 5.—Let ϱ be a three-qubit state. We define a sum of variances as

$$E(\varrho) := 1 - 1/8(\langle\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}\rangle^2 + \langle\mathbb{1} \otimes \sigma_z \otimes \sigma_z\rangle^2 + \langle\sigma_z \otimes \mathbb{1} \otimes \sigma_z\rangle^2 + \langle\sigma_z \otimes \sigma_z \otimes \mathbb{1}\rangle^2 + \langle\sigma_x \otimes \sigma_x \otimes \sigma_x\rangle^2$$

$$+ \langle\sigma_x \otimes \sigma_y \otimes \sigma_y\rangle^2 + \langle\sigma_y \otimes \sigma_y \otimes \sigma_x\rangle^2 + \langle\sigma_y \otimes \sigma_x \otimes \sigma_y\rangle^2). \qquad (6)$$

If $E < 1/2$, the state ϱ is fully tripartite entangled. If $E < 3/8$, the state ϱ belongs even to the *GHZ* class. For the *GHZ* state $|GHZ\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle)$, we have $E = 0$.

Proof.—We define the eight states $|\psi_{1/5}\rangle = (|000\rangle \pm |111\rangle)/\sqrt{2}$, $|\psi_{2/6}\rangle = (|100\rangle \pm |011\rangle)/\sqrt{2}$, $|\psi_{3/7}\rangle = (|010\rangle \pm |101\rangle)/\sqrt{2}$, $|\psi_{4/8}\rangle = (|001\rangle \pm |110\rangle)/\sqrt{2}$, and as usual $M_i = |\psi_i\rangle\langle\psi_i|$, $i = 1, \dots, 8$, and $E = \sum_i \delta^2(M_i)$. Then the proof is quite similar to the proof of Proposition 2. One needs only the maximal squared overlaps, which are known [14]: $\max_{|\phi\rangle\in\mathrm{BS}}|\langle GHZ|\phi\rangle|^2 = 1/2$, $\max_{|\phi\rangle\in W}|\langle GHZ|\phi\rangle|^2 = 3/4$. By decomposing the M_i as in [15], one gets E in the form of Eq. (6). $\square$

Let us compare this with the witness for this detection problem [14,15]. A witness is given by $W = 1/2 \cdot \mathbb{1} - |GHZ\rangle\langle GHZ|$; if $\mathrm{Tr}(W\varrho) < 0$, the state ϱ is fully entangled, and if $\mathrm{Tr}(W\varrho) < -1/4$ it even belongs to the *GHZ* class. Assuming states of the type $\varrho(p) = p|GHZ\rangle\langle GHZ| + (1-p)\mathbb{1}/8$, the method based on E detects them for $p \geq \sqrt{3/7} \approx 0.65$ as tripartite entangled, and for $p \geq \sqrt{4/7} \approx 0.76$ as *GHZ* states. The witness detects them for $p \geq 3/7 \approx 0.43$ as tripartite entangled and for $p \geq 5/7 \approx 0.71$ as belonging to the *GHZ* class. While the witness seems to detect more states in the vicinity of $|GHZ\rangle$, the variance method has, in contrast to the witness, the property that it detects also all orthogonal $|\psi_i\rangle$. The uncertainty relations are thus in this respect stronger that the witness.

The method presented here can be extended to more parties. For four qubits one can write down 16 orthogonal *GHZ* states of the type $|\psi_i\rangle = (|x_1^{(1)}x_1^{(2)}x_1^{(3)}x_1^{(4)}\rangle \pm |x_2^{(1)}x_2^{(2)}x_2^{(3)}x_2^{(4)}\rangle)/\sqrt{2}$ with $x_l^{(k)} \in \{0,1\}$ and $x_1^{(k)} \neq x_2^{(k)}$. If we then define $M_i = |\psi_i\rangle\langle\psi_i|$, it follows as in the proof of Proposition 5, that for all biseparable states $\sum_i \delta^2(M_i) \geq 1/2$ holds. The same idea can be used to construct uncertainty relations for an arbitrary number of qubits, but the number of M_i increases exponentially.

Now we want to put our results in a more general framework. Let $\varrho = \sum_k p_k \varrho_k^A \otimes \varrho_k^B$ be a separable state and let M_i, for $i = 1, \dots, n$ be some observables. We can define two functionals $Z(\varrho)[X]$ and $W(\varrho)[X]$ with $X = (x_1, \dots, x_n) \in \mathbb{R}^n$ by

$$Z(\varrho)[X] := \langle e^{\sum_{i=1}^n x_i M_i}\rangle, \qquad W(\varrho)[X] := \ln\{Z(\varrho)[X]\}.$$

Z is called the generating functional of the moments and W generates the cumulants [16]. We have $Z(\varrho) = \sum_k p_k Z(\varrho_k^A \otimes \varrho_k^B)$, and due to the concavity of the logarithm it follows that

$$W(\varrho) - \sum_k p_k W(\varrho_k^A \otimes \varrho_k^B) \geq 0 \qquad (7)$$

holds. The left-hand side (lhs) of this equation has a minimum at $X = 0$. Thus, the matrix of the second derivatives with respect to X of the lhs is positive semi-definite at $X = 0$. The matrix of the second derivatives of W is the so-called covariance matrix (CM) $\gamma(\varrho, M_i)$. Its entries are

$$\gamma(\varrho, M_i)_{kl} := \partial_k \partial_l W[X]|_{X=0}, \qquad (8)$$

where we have denoted $\partial_i := \frac{\partial}{\partial x_i}$. Thus, we can state the following.

Lemma 2.—Let ϱ be separable, and let M_i be observables. Then there exist product states $\varrho_k^A \otimes \varrho_k^B$ and p_k such that

$$\gamma(\varrho, M_i) \geq \sum_k p_k \gamma(\varrho_k^A \otimes \varrho_k^B, M_i) \qquad (9)$$

holds. We call a state "violating Lemma 2" iff there are no product states $\varrho_k^A \otimes \varrho_k^B$ and convex weights p_k, such that Eq. (9) is fulfilled.

Proposition 6.—γ has the following properties.
(i) The entries are given by

$$\gamma_{kl} = (\langle M_k M_l\rangle + \langle M_l M_k\rangle)/2 - \langle M_k\rangle\langle M_l\rangle. \qquad (10)$$

The diagonal entries are the variances $\gamma_{ii} = \delta^2(M_i)$.
(ii) We have for an arbitrary $(x_1, \dots, x_n) \in \mathbb{R}^n$

$$\sum_{i,j=1}^n x_i \gamma_{ij} x_j = \delta^2\left(\sum_{i=1}^n x_i M_i\right) \geq 0. \qquad (11)$$

In particular, we have $\gamma \geq 0$.

Proof.—Property (i) can be directly calculated from the definition with the help of standard formulas for differentiating operators [17] and the power expansion of the logarithm. Property (ii) can be proven by calculating $\delta^2(\sum_{i=1}^n x_i M_i)$. $\square$

Theorem 1.—A state ϱ violates Lemma 1 with S being the set of product states iff it violates Lemma 2. The observables leading to a violation may differ.

Proof.—A state violating Lemma 1 violates also Lemma 2 with the same M_i, since the sum of all variances is the trace of γ. To show the other direction, let us assume that γ violates Lemma 2 and look at the set of symmetric matrices of the form $T := \{\sum_k p_k \gamma(\varrho_k^A \otimes \varrho_k^B, M_i) + P\}$, where $P \geq 0$ is positive. T is convex and closed. We have $\gamma \notin T$, and due to a corollary of the Hahn-Banach theorem [18] there exists a symmetric matrix W and a number C such that $\mathrm{Tr}(W\gamma) < C$ while $\mathrm{Tr}(W\mu) > C$ for all $\mu \in T$ [19]. Since $\mathrm{Tr}(WP) \geq 0$ for all $P \geq 0$, we have $W \geq 0$. Now we use the spectral decomposition and write $W_{ij} = \sum_l \lambda_l a_i^l a_j^l$ with $\lambda_l \geq 0$. Let us define $N_l = \sqrt{\lambda_l} \sum_i a_i^l M_i$. Then $\mathrm{Tr}(W\gamma) = \sum_l \delta^2(N_l) < C$ according to Eq. (11), while for all convex combinations of product states $\sum_k p_k \sum_l \delta^2(N_l)_{\varrho_k^A \otimes \varrho_k^B} > C$ holds. This is a violation of Lemma 1 for the N_l. $\square$

So Lemma 2 is equivalent to Lemma 1. The advantage of Lemma 2 is that it allows us to relate the uncertainty relations to entanglement criteria known from continuous variables, mainly Gaussian states. Let us note some facts about Gaussian states [7,8]. The nonlocal properties of a Gaussian state are completely encoded in a real symmetric CM $\tilde{\gamma}$, which is the CM of the canonical conjugate observables position and momentum. A Gaussian state $\tilde{\gamma}$ in a bipartite system is separable iff there are CMs $\tilde{\gamma}^A$, $\tilde{\gamma}^B$ for Alice and Bob such that $\tilde{\gamma} \geq \tilde{\gamma}^A \oplus \tilde{\gamma}^B$ [7,20]. In fact, the separability problem for Gaussian states was solved in Ref. [8], where a map $\tilde{\gamma}_1 \mapsto \tilde{\gamma}_2$ was defined which maps a

separable (respectively, entangled) CM to another separable (respectively, entangled) CM. By iterating this map, one gets a CM for which separability is easy to check. We can now formulate criteria similar to [7,8].

Proposition 7.—Let ϱ be separable and let A_i, $i = 1, \ldots, n$ and B_i, $i = 1, \ldots, m$ be observables on Alice's, respectively, Bob's, space. Define $M_i = A_i \otimes \mathbb{1}$, $i = 1, \ldots, n$ and $M_i = \mathbb{1} \otimes B_i$, $i = n + 1, \ldots, n + m$. Then there are states ϱ_k^A and ϱ_k^B and convex weights p_k such that if we define $\kappa_A := \sum_k p_k \gamma(\varrho_k^A, A_i)$ and $\kappa_B := \sum_k p_k \gamma(\varrho_k^B, B_i)$ the inequality

$$\gamma(\varrho, M_i) \geq \kappa_A \oplus \kappa_B \tag{12}$$

holds. Moreover, we write $\gamma(\varrho, M_i)$ in a block structure:

$$\gamma(\varrho, M_i) = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{13}$$

where $A = \gamma(\varrho, A_i)$ [respectively, $B = \gamma(\varrho, B_i)$] is an $n \times n$ (respectively, $m \times m$) matrix. Then we have [21]

$$A - CB^{-1}C^T \geq \kappa_A, \tag{14}$$

$$B - C^T A^{-1} C \geq \kappa_B. \tag{15}$$

Proof.—Equation (12) follows from Lemma 2 and the fact that, for these special M_i for product states, $\gamma(\varrho^A \otimes \varrho^B, M_i) = \gamma(\varrho^A, A_i) \oplus \gamma(\varrho^B, B_i)$ holds.

Equations (14) and (15) arise from the first step of the algorithm in [8]. We arrived already after the first step at a block diagonal matrix and thus at a fixed point. We prove it as in [8] with a Lemma proven there: Let γ be matrix with a block structure as in (13). Equivalent are [21] (a) $\gamma \geq 0$, (b) $\ker(B) \subseteq \ker(C)$ and $A - CB^{-1}C^T \geq 0$, and (c) $\ker(A) \subseteq \ker(C^T)$ and $B - C^T A^{-1} C \geq 0$. Applying the equivalence (a) and (b) to Eqs. (12) and (13) yields with Proposition 6, $A - C(B - \kappa_B)^{-1}C^T \geq \kappa_A \geq 0$. With the equivalence (b) and (c), we get $B - \kappa_B - C^T A^{-1} C \geq 0$, which proves Eq. (15). The proof of (14) is similar. $\square$

In view of the first part of the Letter, we can state that any pure entangled state and any bound entangled UPB state can be detected with the methods of Lemma 2. Identifying more general classes of states which allow a detection leads to the difficult problem of characterizing the possible $\sum_k p_k \gamma(\varrho_k^A \otimes \varrho_k^B, M_i)$ in Eq. (9), respectively, the $\kappa_{A/B}$ in Eqs. (14) and (15). We only know some properties of them: Taking $A_i = B_i = \sigma_i$, $i = x, y, z$ for two qubits, we know that $\sum_i \delta^2(A_i) \geq 2$ [5]; thus, $\mathrm{Tr}(\kappa_A) \geq 2$. Applying this to the Werner states $\varrho(p) = p|\psi\rangle\langle\psi| + (1 - p)\mathbb{1}/4$ with $|\psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, one can calculate that they are detected via Eq. (14) for $p \geq 1/\sqrt{3}$.

In conclusion, we have developed a family of necessary separability criteria based on inequalities for variances. We have shown that they are strong enough to detect the entanglement in various experimental relevant situations. We have formulated an equivalent criterion in terms of covariance matrices, which enabled us to connect continuous variable systems with finite-dimensional systems. The question whether there are entangled states

which do not violate any uncertainty relation is a very interesting one; here, it remains open.

[1] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); O. Rudolph, quant-ph/0202121; K. Chen and L. Wu, Quant. Inf. Comp. **3**, 193 (2003); M. Horodecki, P. Horodecki, and R. Horodecki, quant-ph/0206008; for a review, see D. Bruß *et al.*, J. Mod. Opt. **49**, 1399 (2002).
[2] See, e.g., A. Peres, Found. Phys. **29**, 589 (1999).
[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996); B. M. Terhal, *ibid.* **271**, 319 (2000); M. Lewenstein *et al.*, Phys. Rev. A **62**, 052310 (2000).
[4] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988); M. D. Reid, Phys. Rev. A **40**, 913 (1989); L.-M. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000); S. Mancini *et al.*, *ibid.* **88**, 120401 (2002); N. Korolkova *et al.*, Phys. Rev. A **65**, 052306 (2002); V. Giovannetti *et al.*, *ibid.* **67**, 022320 (2003); P. van Loock and A. Furusawa, *ibid.* **67**, 052315 (2003); G. Tóth, C. Simon, and J. I. Cirac, *ibid.* **68**, 062310 (2003).
[5] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).
[6] H. F. Hofmann, Phys. Rev. A **68**, 034307 (2003).
[7] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
[8] G. Giedke *et al.*, Phys. Rev. Lett. **87**, 167904 (2001).
[9] A. Galindo and P. Pascual, *Problemas de Mecánica Cuántica* (Eudema Universidad Manuales, Madrid, 1989), p. 56.
[10] B. M. Terhal, Theor. Comput. Sci. **287**, 313 (2002); O. Gühne *et al.*, Phys. Rev. A **66**, 062305 (2002).
[11] M. Barbieri *et al.*, Phys. Rev. Lett. **91**, 227901 (2003); M. Bourennane *et al.*, *ibid.* **92**, 087902 (2004).
[12] C. H. Bennett *et al.*, Phys. Rev. Lett. **82**, 5385 (1999).
[13] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A, **62**, 062314 (2000).
[14] A. Acín *et al.*, Phys. Rev. Lett. **87**, 040401 (2001).
[15] O. Gühne and P. Hyllus, Int. J. Theor. Phys. **42**, 1001 (2003).
[16] See, e.g., I. Montvay and G. Münster, *Quantum Fields on a Lattice* (Cambridge University Press, Cambridge, England, 1994).
[17] R. M. Wilcox, J. Math. Phys. (N.Y.) **8**, 962 (1967).
[18] See, e.g., F. Hirzebruch and W. Scharlau, *Einführung in die Funktionalanalysis* (BI, Mannheim, 1971).
[19] Similar witnesslike constructions have been considered before for CMs in continuous variables [G. Giedke and M. Lewenstein (private communication)].
[20] The symbol $A \oplus B$ denotes a 2×2-block matrix consisting of A and B on the diagonal and zero matrices elsewhere.
[21] Here, X^{-1} denotes the pseudoinverse of the matrix X, i.e., the inversion on the range.