Entanglement criteria based on local uncertainty relations are strictly stronger than the computable cross norm criterion

Otfried Gühne,[1] Mátyás Mechler,[2] Géza Tóth,[3,4] and Peter Adam[2,3]

[1]*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, A-6020 Innsbruck, Austria*
[2]*Research Group for Nonlinear and Quantum Optics, Hungarian Academy of Sciences, University of Pécs, Ifjúság út 6, H-7624 Pécs, Hungary*
[3]*Research Institute for Solid State Physics and Optics, Hungarian Academy of Sciences, P. O. Box 49, H-1525 Budapest, Hungary*
[4]*Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, D-85748 Garching, Germany*

We show that any state that violates the computable cross norm (or realignment) criterion for separability also violates the separability criterion of the local uncertainty relations. The converse is not true. The local uncertainty relations provide a straightforward construction of nonlinear entanglement witnesses for the cross norm criterion.

Entanglement plays a central role in quantum-information processing. Thus its characterization is important for the field: It is crucial to be able to decide whether or not a given quantum state is entangled. However, this so-called separability problem remains one of the most challenging unsolved problems in quantum physics.

Several sufficient conditions for entanglement are known. The first of such criteria was the criterion of the positivity of the partial transpose (PPT) [1]. This criterion is necessary and sufficient for 2×2 and 2×3 systems [2], but in higher-dimensional systems some entangled states escape detection. The characterization of these PPT entangled states is thus of great interest. Recently, the computable cross norm (CCN) or realignment criterion was put forward by Rudolph [3] and Chen and Wu [4]. The original condition has been reformulated in several ways and extended to multipartite systems [5–7]. The CCN criterion allows one to detect the entanglement of many states where the PPT criterion fails; however, some states that are detected by the PPT criterion cannot be detected by the CCN criterion [5]. In this way, one may view the CCN criterion as complementary to the PPT criterion. In addition to the CCN criterion, there are also algorithmic approaches to the separability problem, which allow the detection of entanglement when the PPT criterion fails [8].

A different approach to the separability problem tries to formulate separability criteria directly in mean values or variances of observables. Typically, these conditions are formulated as Bell inequalities [9], entanglement witnesses [2,10], or uncertainty relations [11–16]. Here, the local uncertainty relations (LURs) by Hofmann and Takeuchi are remarkable [12]. They have a clear physical interpretation and are quite versatile. It has been shown that they can be used to detect PPT entangled states [13]. It is further known that in certain situations they can provide a nonlinear refinement of linear entanglement witnesses [14]. Consequently, the investigation of LURs has been undertaken in several directions [15,16].

In this paper we investigate the relation between the CCN criterion and the LURs. We show that any state that can be detected by the CCN criterion can also be detected by a LUR. By providing counterexamples, we prove that the converse does not hold. Our results show that the LURs can be viewed as nonlinear entanglement witnesses for the CCN criterion. In this way, we demonstrate a surprising connection between permutation separability criteria (to which the CCN criterion belongs) [7], criteria in terms of covariance matrices, such as LURs [16,17], and the theory of nonlinear entanglement witnesses [18,19]. Further, in two Appendixes we discuss the relation of our constructions to other entanglement witnesses that have been proposed for the CCN criterion, and we calculate other nonlinear entanglement witnesses for the CCN criterion [18].

Let us start by recalling the definition of separability. A quantum state ϱ is called separable if its density matrix can be written as a convex combination of product states,

$$\varrho = \sum_k p_k \varrho_k^{(A)} \otimes \varrho_k^{(B)}, \tag{1}$$

where $p_k \geq 0$, $\Sigma_k p_k = 1$, and A and B denote the two subsystems. Throughout this paper, we denote by $\mathcal{H}_A$ and $\mathcal{H}_B$ the (finite dimensional) Hilbert spaces of Alice and Bob, and by $\mathcal{B}(\mathcal{H}_A)$ and $\mathcal{B}(\mathcal{H}_B)$ the real vector space of the Hermitian observables on them. We first assume that both $\mathcal{H}_A$ and $\mathcal{H}_B$ are d dimensional; later we discuss what happens if this is not the case.

The CCN criterion can be formulated in different ways. We use here a formulation given in Ref. [3] in Corollary 18, since it is best suited for our approach. It makes use of the Schmidt decomposition in operator space. For that reason, any density matrix ϱ can be written as

$$\varrho = \sum_k \lambda_k G_k^A \otimes G_k^B, \tag{2}$$

where $\lambda_k \geq 0$ and G_k^A and G_k^B are orthogonal bases of the observable spaces $\mathcal{B}(\mathcal{H}_A)$, $[\mathcal{B}(\mathcal{H}_B)]$. Such a basis consists of d^2 observables that have to satisfy

$$\mathrm{Tr}(G_k^A G_l^A) = \mathrm{Tr}(G_k^B G_l^B) = \delta_{kl}. \tag{3}$$

We refer to such observables as *local orthogonal observables* (LOOs) [20]. For instance, for qubits the (appropriately normalized) Pauli matrices together with the identity form a set of LOOs [see Eq. (12)]. Note that, given a set G_k^A of LOOs,

any other set $\widetilde{G}_l^A$ of LOOs is of the form $\widetilde{G}_l^A = \Sigma_k O_{lk} G_k^A$, where O_{lk} is a $d^2 \times d^2$ real orthogonal matrix [20].

As for the usual Schmidt decomposition, the λ_k are (up to a permutation) unique and if the λ_k are pairwise different, the G_k^A and G_k^B are also unique (up to a sign). The λ_k can be computed as in the Schmidt decomposition: First, one decomposes $\varrho = \Sigma_{kl} \mu_{kl} \widetilde{G}_k^A \otimes \widetilde{G}_l^B$ with arbitrary LOOs $\widetilde{G}_k^A$ and $\widetilde{G}_l^B$; then, by performing the singular value decomposition of μ_{kl}, one arrives at Eq. (2); the λ_k are the roots of the eigenvalues of the matrix $\mu\mu^\dagger$.

The CCN criterion states that if ϱ is separable, then the sum of all λ_k is smaller than 1:

$$\varrho \text{ is separable} \Rightarrow \sum_k \lambda_k \leq 1. \tag{4}$$

Hence, if $\Sigma_k \lambda_k > 1$ the state must be entangled. For states violating this criterion, an entanglement witness can directly be written down. Recall that an entanglement witness $\mathcal{W}$ is an observable with a positive expectation value on all separable states; hence a negative expectation value signals the presence of entanglement [10]. Given a state in the form (2) that violates the CCN criterion, a witness is given by [21]

$$\mathcal{W} = \mathbb{1} - \sum_k G_k^A \otimes G_k^B, \tag{5}$$

since for this state we have $\mathrm{Tr}(\mathcal{W}\varrho) = 1 - \Sigma_k \lambda_k < 0$ due to the properties of the LOOs. On the other hand, if $\varrho = \Sigma_{kl} \mu_{kl} G_k^A \otimes G_l^B$ were separable, then $\mathrm{Tr}(\mathcal{W}\varrho) = 1 - \Sigma_k \mu_{kk} \geq 1 - \Sigma_k \lambda_k \geq 0$, since $\Sigma_k \mu_{kk} \leq \Sigma_k \lambda_k$ due to the properties of the singular value

decomposition [22]. It is clear that any state violating the CCN criterion can be detected by a witness of the type (5). Note that other forms of entanglement witnesses for the CCN criterion have also been proposed [6]; we will discuss them in Appendix A.

Let us now discuss the LURs. This criterion is formulated as follows. Given some noncommuting observables A_k on Alice's space and B_k on Bob's space, one may compute strictly positive numbers C_A and C_B such that

$$\sum_{k=1}^{n} \Delta^2(A_k) \geq C_A, \quad \sum_{k=1}^{n} \Delta^2(B_k) \geq C_B \tag{6}$$

hold for all states for Alice (Bob). Here, $\Delta^2(A) = \langle A^2 \rangle - \langle A \rangle^2$ denotes the variance of an observable A. Then it can be proved that for separable states

$$\sum_{k=1}^{n} \Delta^2(A_k \otimes \mathbb{1} + \mathbb{1} \otimes B_k) \geq C_A + C_B \tag{7}$$

has to hold. Any quantum state that violates Eq. (7) is entangled. Physically, Eq. (7) may be interpreted as stating that separable states always inherit the uncertainty relations that hold for their reduced states [23].

To connect the LURs with the CCN criterion, first note that for any LOOs G_k^A the relation

$$\sum_{k=1}^{d^2} \Delta^2(G_k^A) \geq d - 1 \tag{8}$$

holds. This can be seen as follows. If we choose the d^2 LOOs

$$G_k^A = \begin{cases} \dfrac{1}{\sqrt{2}}(|m\rangle\langle n| + |n\rangle\langle m|) & \text{for } 1 \leq k \leq [d(d-1)]/2, & 1 \leq m < n \leq d, \\[2mm] \dfrac{1}{\sqrt{2}}(i|m\rangle\langle n| - i|n\rangle\langle m|) & \text{for } [d(d-1)]/2 < k \leq [d(d-1)], & 1 \leq m < n \leq d, \\[2mm] |m\rangle\langle m| & \text{for } d(d-1) < k \leq d^2, & 1 \leq m \leq d, \end{cases}$$

one can directly calculate that $\Sigma_k (G_k^A)^2 = d\mathbb{1}$ and that $\Sigma_k \langle G_k^A \rangle^2 = \mathrm{Tr}(\varrho^2) \leq 1$. For general $\widetilde{G}_k^A = \Sigma_l O_{kl} G_l^A$ we have $\Sigma_k (\widetilde{G}_k^A)^2 = \Sigma_{klm} O_{lk}^T O_{km} G_l^A G_m^A = d\mathbb{1}$ since O is orthogonal and again $\Sigma_k \langle \widetilde{G}_k^A \rangle^2 = \mathrm{Tr}(\varrho^2) \leq 1$ [24]. Similarly, we have for Bob's system

$$\sum_{k=1}^{d^2} \Delta^2(-G_k^B) \geq d - 1, \tag{9}$$

where the minus sign has been inserted for later convenience.

Combining Eqs. (8) and (9) with the method of the LURs, using the fact that $\Sigma_k (G_k^A)^2 = \Sigma_k (G_k^B)^2 = d\mathbb{1}$ one can directly calculate that for separable states

$$1 - \sum_k \langle G_k^A \otimes G_k^B \rangle - \frac{1}{2} \sum_k \langle G_k^A \otimes \mathbb{1} - \mathbb{1} \otimes G_k^B \rangle^2 \geq 0. \tag{10}$$

The first, linear part is just the expectation value of the witness (5); from this some positive terms are subtracted. Since any state that violates the CCN criterion can be detected by the witness in Eq. (5), it can also be detected by the LUR in Eq. (10) and we have the following theorem.

Theorem. Any state that violates the computable cross norm criterion can be detected by a local uncertainty relation, while the converse is not true.

To prove the second statement of the theorem we will later give explicit counterexamples of states that can be detected by a LUR, but not by the CCN criterion. Before doing that, let us add some remarks.

First, the theorem above can be interpreted in the following way. While the witness in Eq. (5) is the natural linear criterion for states violating the CCN criterion, the LUR in Eq. (10) is the natural *nonlinear* witness for these states. The fact that LURs can sometimes be viewed as nonlinear witnesses that improve linear witnesses has been observed before [14]. The theorem, however, proves that the LURs provide *in general* improvements for witnesses of the type (5). Note that there are other possible nonlinear improvements on these witnesses as discussed in Appendix B.

Second, we have to discuss what happens if the dimensions of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are not the same. So let us assume that $d_A = \dim(\mathcal{H}_A) < d_B = \dim(\mathcal{H}_B)$. Then, in Eq. (2) there are d_A^2 different G_k^A and G_k^B. The G_l^A form already a set of LOOs for $\mathcal{H}_A$ and one can find further $d_B^2 - d_A^2$ observables G_k^B to complete the set $\{G_k^B\}$ to become a complete set of LOOs for $\mathcal{H}_B$. Using then the LURs with the definition $G_k^A = 0$ for $k = d_A^2 + 1, \dots, d_B^2$ proves the claim.

Now we present two examples that show that the LURs are strictly stronger than the CCN criterion. First, let us consider a noisy singlet state of the form

$$\varrho_{\text{ns}}(p) := p|\psi_{\text{s}}\rangle\langle\psi_{\text{s}}| + (1-p)\varrho_{\text{sep}}, \qquad (11)$$

where the singlet is $|\psi_{\text{s}}\rangle := (|01\rangle - |10\rangle)/\sqrt{2}$, and the separable noise is given as $\varrho_{\text{sep}} := 2/3|00\rangle\langle00| + 1/3|01\rangle\langle01|$. Using the PPT criterion one can see that the state is entangled for any $p > 0$. First we check for which values of p the state ϱ_{ns} is detected as entangled by the CCN criterion. It can be seen that $\varrho_{\text{ns}}(p)$ violates the CCN criterion for all $p > 0.292$. Now we define G_k^A and G_k^B as

$$\{G_k^A\}_{k=1}^4 = \left\{ -\frac{\sigma_x}{\sqrt{2}}, -\frac{\sigma_y}{\sqrt{2}}, -\frac{\sigma_z}{\sqrt{2}}, \frac{\mathbb{1}}{\sqrt{2}} \right\},$$

$$\{G_k^B\}_{k=1}^4 = \left\{ \frac{\sigma_x}{\sqrt{2}}, \frac{\sigma_y}{\sqrt{2}}, \frac{\sigma_z}{\sqrt{2}}, \frac{\mathbb{1}}{\sqrt{2}} \right\}. \qquad (12)$$

These G_k^A and G_k^B are the matrices corresponding to the Schmidt decomposition of $|\psi_{\text{s}}\rangle\langle\psi_{\text{s}}|$. Using Eq. (10) with these LOOs one finds that ϱ_{ns} is detected as entangled by the LURs at least for $p > 0.25$.

For the second example, we consider the 3×3 bound entangled state defined in [25] mixed with white noise:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), \quad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle,$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle), \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle,$$

$$|\psi_4\rangle = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle),$$

$$\varrho_{\text{BE}} = \frac{1}{4}\left(\mathbb{1} - \sum_{i=0}^4 |\psi_i\rangle\langle\psi_i|\right), \quad \varrho(p) = p\varrho_{\text{BE}} + (1-p)\frac{\mathbb{1}}{9}.$$

The states $\varrho(p)$ are detected as entangled via the CCN criterion whenever $p > p_{\text{ccn}} = 0.8897$. Taking the LUR (10) with

the Schmidt matrices of $\varrho(p_{\text{ccn}})$ as LOOs, one finds that the states $\varrho(p)$ must already be entangled for $p > p_{\text{lur}} = 0.8885$. Thus, the LURs are able to detect states that are detected neither by the CCN criterion nor by the PPT criterion. Note that $\varrho(p)$ is known to be entangled at least for $p > 0.8744$ [6].

In conclusion, we showed that entanglement criteria based on local uncertainty relations are strictly stronger than the CCN criterion. The local uncertainty relations can be viewed as the natural nonlinear entanglement witnesses for the CCN criterion. The question of whether there is also a relation between the PPT criterion and local uncertainty relations is very interesting. We leave this problem for future research.

APPENDIX A: CONNECTION TO THE WITNESSES PROPOSED IN REF. [6]

Now we show that the entanglement witness defined in Eq. (5) is identical to the witness defined in Ref. [6] based on a different formulation of the CCN criterion. Let us first review the realignment map. For a density matrix $\varrho = \Sigma_{kl}\mu_{kl}G_k^A \otimes G_l^B$ the realigned matrix is given by [3]

$$R(\varrho) := \sum_{kl} \mu_{kl}|G_k^A\rangle\langle G_l^B|. \qquad (A1)$$

Here $|G_k^A\rangle$ denotes a column vector obtained from G_k^A by joining its columns consecutively while $\langle G_k^B|$ denotes the transposition of a column vector obtained similarly from G_k^B. $R(\varrho)$ can also be computed by a reordering ("realignment") of the matrix entries of ϱ, as explained in Ref. [4]. The CCN criterion states that if $\|R(\varrho)\|_1 > 1$ then ρ is entangled [3–6]. Here $\|A\|_1$ denotes the trace norm, i.e., the sum of the singular values of matrix A. If $\varrho = \Sigma_k\lambda_k A_k \otimes B_k$ is given in its Schmidt decomposition, we have $R(\varrho) = \Sigma_k\lambda_k|A_k\rangle\langle B_k|$ and $\|R(\rho)\|_1 = \Sigma_k\lambda_k$. In this case $R(\varrho)$ is already given in its singular value decomposition. To make this even more transparent, let us define $\Sigma = \text{diag}(\lambda_1, \lambda_2, \dots)$, $U = [|A_1\rangle, |A_2\rangle, \dots]$, and $V = [|B_1\rangle, |B_2\rangle, \dots]$. Then we obtain the decomposition $R(\varrho) = U\Sigma V^\dagger$.

Now we can show that the witness Eq. (5) can be rewritten using the inverse of R. For that we need to observe that $\Sigma_k A_k \otimes B_k = R^{-1}(\Sigma_k|A_k\rangle\langle B_k|) = R^{-1}(UV^\dagger)$. Hence the witness Eq. (5) can be written as

$$\mathcal{W} = \mathbb{1} - R^{-1}(UV^\dagger). \qquad (A2)$$

Since R realigns the matrix entries, we have always $R^{-1}(X^*) = R^{-1}(X)^*$. Furthermore, since $\Sigma_k A_k \otimes B_k$ is Hermitian, $R^{-1}(UV^\dagger)$ is also Hermitian. Thus the witness in Eq. (A2) can be written as $\mathcal{W} = \mathbb{1} - [R^{-1}(U^*V^T)]^T$, which is the witness presented in Ref. [6].

APPENDIX B: MORE NONLINEAR WITNESSES

Recently, a method to calculate nonlinear improvements for a given general witness has been developed [18]. Here, we apply this method to Eq. (5).

To start, we first have to calculate the positive map $\Lambda : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ corresponding to $\mathcal{W}$ [26]. This is $\Lambda(\varrho) = \mathrm{Tr}_A[\mathcal{W}(\varrho^T \otimes \mathbb{1}_B)]$, and one can directly see that for $\varrho = \Sigma_i \alpha_i (G_i^A)^T$ we have $\Lambda(\varrho) = \mathrm{Tr}(\varrho)\mathbb{1}_B - \Sigma_i \alpha_i (G_i^B)$. We can assume without the loss of generality that $d\Lambda$ is trace nonincreasing; otherwise we rescale $\mathcal{W}$ to obtain this. According to the Jamiołkowski isomorphism the witness can then be rewritten as

$$\mathcal{W} = (\mathbb{I}_A \otimes d\Lambda)(|\phi^+\rangle\langle\phi^+|), \qquad (B1)$$

where $|\phi^+\rangle = \Sigma_i |ii\rangle / \sqrt{d}$ is a maximally entangled state on $\mathcal{H}_A \otimes \mathcal{H}_A$. Since for LOOs $\Sigma_i \mathrm{Tr}(G_i^A)G_i^A = \mathbb{1}$ holds, Eq. (B1) implies that $|\phi^+\rangle\langle\phi^+| = \Sigma_i G_i^A \otimes (G_i^A)^T / d$.

To write down a nonlinear improvement, we can take an arbitrary state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_A$ which has a maximal squared Schmidt coefficient $s(\psi)$. Then, defining $X = (\mathbb{I}_A \otimes d\Lambda)(|\phi^+\rangle\langle\psi|)$ the functional

$$\mathcal{F}(\varrho) = \langle\mathcal{W}\rangle - \langle X\rangle\langle X^\dagger\rangle / s(\psi) \qquad (B2)$$

is a nonlinear improvement of $\mathcal{W}$ [18].

To give a first example, let us choose an arbitrary unitary U^A on $\mathcal{H}_A$ and define $|\psi\rangle = (U^A)^\dagger \otimes \mathbb{1}|\phi^+\rangle$, which implies that $s(\psi) = 1/d$. Then direct calculations lead to the nonlinear witness

$$\mathcal{F}(\varrho) = \langle\mathcal{W}\rangle - d\langle\mathcal{W}(U^A \otimes \mathbb{1})\rangle\langle(U^A \otimes \mathbb{1})^\dagger \mathcal{W}\rangle. \qquad (B3)$$

To give a second example, let us define $|\psi\rangle = \mathbb{1} \otimes (U^A)^\dagger |\phi^+\rangle$. Using the coefficients $\eta_{ij} = \mathrm{Tr}[(G_i^A)^T (G_j^A)^T U^A]$ we can directly calculate that $X = (\mathbb{I}_A \otimes \Lambda)[\Sigma_i G_i^A \otimes (G_i^A)^T U^A] = \mathbb{1} - \Sigma_{ij} G_i^A \otimes \eta_{ij} G_j^B$. Hence,

$$\mathcal{F}(\varrho) = \langle\mathcal{W}\rangle - d\left\langle \mathbb{1} - \sum_{ij} G_i^A \otimes \eta_{ij} G_j^B \right\rangle\left\langle \mathbb{1} - \sum_{ij} G_i^A \otimes \eta_{ij}^* G_j^B \right\rangle$$

is another nonlinear witness, improving the witness in Eq. (5). The structure of these witnesses is quite different from the structure of the LURs. Thus other nonlinear witnesses can be derived for the CCN criterion, which do not coincide with the LURs.

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

[2] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[3] O. Rudolph, e-print quant-ph/0202121.

[4] K. Chen and L.-A. Wu, Quantum Inf. Comput. **3**, 193 (2003).

[5] O. Rudolph, Phys. Rev. A **67**, 032312 (2003).

[6] K. Chen and L.-A. Wu, Phys. Rev. A **69**, 022312 (2004).

[7] K. Chen and L.-A. Wu, Phys. Lett. A **306**, 14 (2002); M. Horodecki, P. Horodecki, and R. Horodecki, Open Syst. Inf. Dyn. **13**, 103 (2006); P. Wocjan and M. Horodecki, *ibid.* **12**, 331 (2005); L. Clarisse and P. Wocjan, Quantum Inf. Comput. **6**, 277 (2006).

[8] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004); J. Eisert *et al.*, *ibid.* **70**, 062317 (2004); F. G. S. L. Brandao and R. O. Vianna, Phys. Rev. Lett. **93**, 220503 (2004).

[9] See, e.g., A. Peres, Found. Phys. **29**, 589 (1999).

[10] B. M. Terhal, Phys. Lett. A **271**, 319 (2000); M. Lewenstein *et al.*, Phys. Rev. A **62**, 052310 (2000); G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005); L.-A. Wu *et al.*, Phys. Rev. A **72**, 032309 (2005); F. G. S. L. Brandão, *ibid.* **72**, 022310 (2005).

[11] For nonlinear entanglement criteria see also D. Janzing and Th. Beth, Phys. Rev. A **61**, 052308 (2000); L.-M. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, *ibid.* **84**, 2726 (2000); A. Sørensen *et al.*, Nature (London) **409**, 63 (2001); G. Tóth, C. Simon, and J. I. Cirac, Phys. Rev. A **68**, 062310 (2003).

[12] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).

[13] H. F. Hofmann, Phys. Rev. A **68**, 034307 (2003).

[14] O. Gühne and M. Lewenstein, in *Quantum Communication, Measurement and Computing: The Seventh International Conference on Quantum Communication, Measurement and Computing*, edited by S. M. Barnett, E. Andersson, and J. Jeffers, AIP Conf. Proc. No. 734 (AIP, NY, 2004), p. 230; G. Tóth and O. Gühne, Phys. Rev. A **72**, 022340 (2005).

[15] M. Wiesniak, V. Vedral, and C. Brukner, New J. Phys. **7**, 258 (2005); S. Samuelsson and G. Björk, Phys. Rev. A **73**, 012319 (2006).

[16] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).

[17] E. Shchukin and W. Vogel, Phys. Rev. Lett. **95**, 230502 (2005); J. Rigas, O. Gühne, and N. Lütkenhaus, Phys. Rev. A **73**, 012341 (2006); P. Hyllus and J. Eisert, New J. Phys. **8**, 51 (2006); A. Miranowicz *et al.*, e-print quant-ph/0605001.

[18] O. Gühne and N. Lütkenhaus, Phys. Rev. Lett. **96**, 170502 (2006).

[19] F. A. Bovino *et al.*, Phys. Rev. Lett. **95**, 240407 (2005); R. Augusiak, P. Horodecki, and M. Demianowicz, e-print quant-ph/0604109.

[20] S. Yu and N. L. Liu, Phys. Rev. Lett. **95**, 150504 (2005).

[21] This witness has also been derived in a different formulation in Ref. [20].

[22] See Theorem 7.4.9 in R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, U.K., 1999).

[23] A similar statement holds for entropic uncertainty relations [O. Gühne and M. Lewenstein, Phys. Rev. A **70**, 022316 (2004)].

[24] Alternatively, one may also use that for all LOOs G_i and arbitrary X we have $\Sigma_i G_i X G_i^\dagger = \mathrm{Tr}(X)\mathbb{1}$ [M. Piani (private communication)].

[25] C. H. Bennett *et al.*, Phys. Rev. Lett. **82**, 5385 (1999).

[26] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972); for a review, see M. Horodecki, P. Horodecki, and R. Horodecki, e-print quant-ph/0109124.