

Lower bounds on the entanglement of formation for general Gaussian states

G. Rigolin* and C. O. Escobar†

Departamento de Raios C3smicos e Cronologia, Instituto de F3sica Gleb Wataghin, Universidade Estadual de Campinas, Caixa Postal 6165, Codigo de Enderecamento Postal 13084-971, Campinas, S3o Paulo, Brazil

(Received 5 August 2003; published 13 January 2004)

We derive two lower bounds on entanglement of formation for arbitrary mixed Gaussian states by two distinct methods. To achieve the first one we use a local measurement procedure that symmetrizes a general Gaussian state and the fact that entanglement cannot increase under local operations and classical communications. The second one is obtained via a generalization to mixed states of an interesting result already known for pure states, which says that squeezed states are those that, for a fixed amount of entanglement, maximize Einstein-Podolsky-Rosen-like correlations.

DOI: 10.1103/PhysRevA.69.012307

PACS number(s): 03.67.Mn, 03.65.Ud

I. INTRODUCTION

The quantification of the amount of entanglement a quantum system possesses is still an open problem in quantum-information theory. Restricting our attention to bipartite systems, i.e., systems composed of two subsystems, we have one measure of entanglement, entanglement of formation (EOF) [1], which has a clear physical meaning. Given an entangled state ρ , the EOF for this state expresses the number of maximally entangled states we need to create ρ [2]. The formal definition of the EOF is

$$E_f(\rho) = \inf \sum_j p_j E(\psi_j), \quad (1)$$

where we take the infimum over all pure-state decompositions of $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$, $\sum_j p_j = 1$, and $E(\psi_j)$ is the von Neumann entropy of the pure state ψ_j .

The analytical minimization of Eq. (1) is not an easy task. Dealing with two-qubit systems, which are the simplest entangled bipartite systems, Wootters [3] obtained an analytical expression for the EOF and Giedke *et al.* [4] derived an analytical expression for the EOF for symmetric Gaussian states.

Gaussian states are very useful in quantum-optical implementation of several quantum information protocols. (Quantum cryptography [5] is an important example.) Hence, a complete characterization of the amount of entanglement of Gaussian states is desirable. The natural next step is the search for an analytical expression for the EOF for arbitrary Gaussian states.

In this article we give two analytical expressions that furnish lower bounds for the EOF for Gaussian states. We employ two different methods to derive such lower bounds. The first lower bound is obtained using a local measurement procedure derived by Giedke *et al.* [6] which symmetrizes a general Gaussian state and the fact that entanglement cannot increase under local operations and classical communications (LOCC). The second one is derived via a generalization to mixed states of an interesting result derived by Giedke

et al. [4], who show that squeezed states are those that, for a fixed amount of entanglement, maximize Einstein-Podolsky-Rosen-like correlations. These lower bounds are also useful in ruling out several possible candidates for the analytical expression of the EOF for arbitrary Gaussian states, as we illustrate in this article.

II. FIRST LOWER BOUND

Let us begin setting the notation used in this article and some properties of Gaussian states. Consider a bipartite Gaussian system ρ of two modes described by the annihilation operators $a_j = (X_j + iP_j)/\sqrt{2}$, where $j = 1, 2$ and $[X_j, P_{j'}] = i\delta_{jj'}$. This system can be alternatively described by its characteristic function [6]

$$\chi(r) = \text{tr}[\rho D(r)], \quad (2)$$

where $r = (x_1, p_1, x_2, p_2)^T$ is a column real vector and

$$D(r) = e^{-i(x_1 X_1 + p_1 P_1 + x_2 X_2 + p_2 P_2)}. \quad (3)$$

Equation (2) uniquely defines a state ρ and for Gaussian states it can always be put in the following form:

$$\chi(r) = e^{-r^T \gamma r/4 - id^T r}, \quad (4)$$

where T means transposition, γ is a 4×4 matrix which is called the correlation matrix (CM), and d is a four-dimensional real vector. The first moments of a Gaussian state $\langle X_j \rangle$ and $\langle P_j \rangle$ can always be set to zero using local unitary operations, which implies that we can work with zero mean Gaussian states when studying entanglement properties of such systems. The matrix elements γ_{ij} of the CM can be calculated directly from the density matrix ρ by the following formula:

$$\gamma_{ij} = \text{tr}[(R_i R_j + R_j R_i)\rho] - 2 \text{tr}[R_i \rho] \text{tr}[R_j \rho], \quad (5)$$

where $R = (X_1, P_1, X_2, P_2)^T$. A matrix γ represents a realizable physical state if and only if it is strictly positive, real, symmetric, and satisfies [6]

$$\gamma \geq J^T \gamma^{-1} J, \quad (6)$$

*Electronic address: rigolin@ifi.unicamp.br

†Electronic address: escobar@ifi.unicamp.br

where $J = \bigoplus_{k=1}^2 J_1$ is a 4×4 matrix with $J_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

A Gaussian system can also be represented by its Wigner distribution $W(r)$. Assuming that we are working with a zero-mean Gaussian state, we have [7]

$$W(r) = \frac{1}{\pi^2} \frac{1}{\sqrt{\det \gamma_W}} e^{-r^T \gamma_W r}. \quad (7)$$

The CM's γ and γ_W are related by

$$\gamma_W = J^T \gamma^{-1} J. \quad (8)$$

These two CM's can be brought to the following standard form by suitable local symplectic transformations [6]:

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \quad (9)$$

where

$$A = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}, \quad B = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}, \quad C = \begin{pmatrix} k_x & 0 \\ 0 & k_p \end{pmatrix}. \quad (10)$$

The same set of equations apply to γ_W :

$$\gamma_W = \begin{pmatrix} A_W & C_W \\ C_W^T & B_W \end{pmatrix}, \quad (11)$$

where

$$A_W = \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix}, \quad B_W = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}, \quad (12)$$

$$C_W = \begin{pmatrix} K_x & 0 \\ 0 & K_p \end{pmatrix}. \quad (13)$$

The four real parameters (n, m, k_x, k_p) completely characterize a two-mode Gaussian state and they are related to the four local symplectic transformation invariants as follows [8]:

$$I_1 = n = \sqrt{\det A}, \quad (14a)$$

$$I_2 = m = \sqrt{\det B}, \quad (14b)$$

$$I_3 = k_x k_p = \det C, \quad (14c)$$

$$I_4 = nm(k_x^2 + k_p^2) = \text{tr}(A J_1^T C J_1^T B J_1^T C^T J_1). \quad (14d)$$

Alternatively, the four real parameters (N, M, K_x, K_p) also completely specify a two-mode Gaussian system. They can be also obtained by local symplectic transformation invariants. These invariants, which we call W_1 , W_2 , W_3 , and W_4 , satisfy Eq. (14), where we change A , B , and C to A_W , B_W , and C_W and (n, m, k_x, k_p) to (N, M, K_x, K_p) .

We now pass to the derivation of the first lower bound. A symmetric Gaussian entangled state σ is completely specified by its CM [see Eq. (9)], where $n = m = \bar{n}$. (From now on, every parameter associated with a symmetric Gaussian state

will have a tilde.) Let us assume, without loss of generality, that $\tilde{k}_x > 0$ and $\tilde{k}_p < 0$ [8]. The EOF for this symmetric state is [4]

$$E_f(\sigma) = f(\sqrt{(\bar{n} - |\tilde{k}_x|)(\bar{n} - |\tilde{k}_p|)}), \quad (15)$$

where

$$f(\delta) = c_+(\delta) \log_2[c_+(\delta)] - c_-(\delta) \log_2[c_-(\delta)]. \quad (16)$$

Here $c_{\pm} = (\delta^{-1/2} \pm \delta^{1/2})^2/4$. Using Eq. (14) we can write the EOF given by Eq. (15) in terms of invariants:

$$E_f(\sigma) = f(\sqrt{\tilde{I}_1 - \tilde{I}_3} - \sqrt{\tilde{I}_4 - 2\tilde{I}_1\tilde{I}_3}). \quad (17)$$

Using Eqs. (8) and (14) we obtain the following relations among the invariants of the γ and γ_W matrices:

$$I_1 = \frac{W_2}{W_5}, \quad I_2 = \frac{W_1}{W_5}, \quad I_3 = \frac{W_3}{W_5}, \quad I_4 = \frac{W_4}{W_5^2}, \quad I_5 = \frac{1}{W_5}, \quad (18)$$

where $W_5 = \det \gamma_W$ and $I_5 = \det \gamma$.

Therefore, due to Eq. (18) the EOF for our symmetric Gaussian state, Eq. (17), can be expressed as

$$E_f(\sigma) = f\left(\sqrt{\frac{\tilde{W}_1 - \tilde{W}_3 - \sqrt{\tilde{W}_4 - 2\tilde{W}_1\tilde{W}_3}}{\tilde{W}_5}}\right). \quad (19)$$

But Giedke *et al.* [6] have shown that a general bipartite Gaussian system ρ can be transformed to a symmetrical bipartite Gaussian system σ using LOCC. This implies that $E_f(\rho) \geq E_f(\sigma)$. Schematically, we have

$$\rho \xrightarrow{\text{LOCC}} \sigma \Rightarrow E_f(\rho) \geq E_f(\sigma). \quad (20)$$

Our only task now is to rewrite Eq. (19) in terms of the invariants of the γ matrix of ρ . It is in this step that we use Giedke's symmetrization procedure.

Given a general bipartite Gaussian system ρ and its γ_W matrix, where we assume, without loss of generality, that $N > M$, we can achieve by means of local operations a symmetric state with the following $\tilde{\gamma}_W$ matrix [6]:

$$\gamma_W = \begin{pmatrix} A_W & C_W \\ C_W^T & B_W \end{pmatrix} \xrightarrow{\text{LOCC}} \tilde{\gamma}_W = \begin{pmatrix} \tilde{A}_W & \tilde{C}_W \\ \tilde{C}_W^T & \tilde{B}_W \end{pmatrix}, \quad (21)$$

where

$$\tilde{A}_W = \begin{pmatrix} \frac{N \cos^2 \theta + (NM - K_x^2) \sin^2 \theta}{\cos^2 \theta + M \sin^2 \theta} & 0 \\ 0 & \frac{N \cos^2 \theta + NM \sin^2 \theta}{\cos^2 \theta + M \sin^2 \theta} \end{pmatrix}, \quad (22)$$

$$\tilde{B}_W = \begin{pmatrix} \frac{M}{\cos^2 \theta + M \sin^2 \theta} & 0 \\ 0 & \sin^2 \theta + M \cos^2 \theta \end{pmatrix}, \quad (23)$$

$$\tilde{C}_W = \begin{pmatrix} \frac{K_x \cos \theta}{\cos^2 \theta + M \sin^2 \theta} & 0 \\ 0 & K_p \cos \theta \end{pmatrix}, \quad (24)$$

$$\tan^2 \theta = \frac{N^2 - M^2}{M - N(NM - K_x^2)}. \quad (25)$$

Equation (25) guarantees that $\det \tilde{A}_W = \det \tilde{B}_W$. This condition is the statement that the Gaussian system with the $\tilde{\gamma}_W$ above is symmetrical [6].

Using Eqs. (14) and (22)–(24) and the assumption that $|K_x| \geq |K_p|$ [9], we can write Eq. (19) as follows:

$$E_f(\sigma) = f \left(\sqrt{\frac{\alpha - \sqrt{\beta}}{\epsilon}} \right), \quad (26)$$

where

$$\alpha = W_2 - W_3 + \sqrt{W_2} \tan^2 \theta, \quad (27)$$

$$\epsilon = W_5 + \sqrt{W_1} (\sqrt{W_1 W_2} - K_x^2) \tan^2 \theta, \quad (28)$$

$$\beta = W_4 - 2W_2 W_3 + \tan^2 \theta [(W_4 - 2W_3 - W_3^2) \sqrt{W_2} + (1 - W_2) K_x^2 \sqrt{W_1}], \quad (29)$$

$$\tan^2 \theta = \frac{W_1 - W_2}{\sqrt{W_2} - \sqrt{W_1} (\sqrt{W_1 W_2} - K_x^2)}, \quad (30)$$

$$K_x^2 = \frac{W_4 + \sqrt{W_4^2 - 4W_1 W_2 W_3}}{2\sqrt{W_1 W_2}}. \quad (31)$$

Now, using Eq. (18) we can put Eq. (26) in terms of the invariants of the γ matrix. Hence, if we work with γ in its standard form given by Eq. (9), where we assume, without loss of generality, that $|k_x| \geq |k_p|$, Eq. (26) is rewritten after a tedious but straightforward algebraic manipulation as [10]

$$E_f(\sigma) = f \left(\sqrt{\frac{nmh(n,m) - k_x k_p h(m,n) + |mk_x - nk_p| \sqrt{h(n,m)h(m,n)}}{g(n,m)}} \right), \quad (32)$$

where

$$h(n,m) = n - m(nm - k_p^2) \quad (33a)$$

$$g(n,m) = m(1 - m^2) + nk_p^2. \quad (33b)$$

Equation (32) is our first lower bound for the EOF for general Gaussian states. It is worthnoting that this lower bound reduces to the EOF for symmetric Gaussian states whenever $n = m$.

III. SECOND LOWER BOUND

A two-mode squeezed state [4] is a symmetric Gaussian pure state that belongs to the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ and is described by the following vector:

$$|\Psi_s(r)\rangle = \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} \tanh^n(r) |n\rangle_1 \otimes |n\rangle_2, \quad (34)$$

where $|n\rangle_j$ is the n th Fock state, that is, $a_j^\dagger a_j |n\rangle_j = n |n\rangle_j$, $j = 1, 2$, and $r \in (0, \infty)$ is the squeezing parameter.

There exists an interesting relation between squeezed states and Einstein-Podolsky-Rosen (EPR) correlations, which Giedke *et al.* [4] proved in their proposition 1: Given a squeezed state $|\Psi_s(r)\rangle$ and an arbitrary pure two-mode state $|\psi\rangle$ then, if they have the same EPR correlation, the squeezed state is the least entangled. In other words, if we denote by $\Delta(\Psi_s(r))$ and $\Delta(\psi)$ the EPR correlations for the two mentioned states and if $\Delta(\Psi_s(r)) = \Delta(\psi)$ then $E(\psi) \geq E(\Psi_s(r))$.

The EPR correlation is defined as [4]

$$\Delta(\psi) = \min \left\{ 1, \frac{1}{2} [\Delta_\psi^2(X_1 - X_2) + \Delta_\psi^2(P_1 + P_2)] \right\}, \quad (35)$$

where $\Delta_\psi^2(R_j) = \langle R_j^2 \rangle_\psi - \langle R_j \rangle_\psi^2$ is the dispersion of the observable R_j . The above expression measures the degree of nonlocal correlations and is zero for the original EPR state [4,11]. This means that the more a system is nonlocal the more Eq. (35) approaches zero. We say that a system with

the minimal $\Delta(\psi)$ has the maximal EPR correlation. For our squeezed state the EPR correlation is [4]

$$\Delta(\Psi_s(r)) = e^{-2r}. \quad (36)$$

The EOF, which is equal to the von Neumann entropy, for the squeezed state is [4]

$$E(\Psi_s(r)) = \cosh^2(r) \log_2[\cosh^2(r)] - \sinh^2(r) \log_2[\sinh^2(r)]. \quad (37)$$

And it is shown that [4]

$$E(\Psi_s(r)) = f(\Delta(\Psi_s(r))). \quad (38)$$

Giedke *et al.* [4] have shown that $f:(0,1] \rightarrow [0,\infty)$ is a convex and decreasing function of its argument. Hence, as Eq. (36) can have any value between zero and 1, the EOF for a squeezed state can assume any value between zero and infinity. This property of the EOF for squeezed states, i.e., that they can assume any value, is an essential ingredient in our generalization of Giedke *et al.*'s proposition 1 [4]. Let us now state and then prove the following theorem, which is a generalization to mixed states of proposition 1 of [4].

Theorem 1. For all bipartite Gaussian systems ρ we have $E_f(\rho) \geq E_f(\sigma)$, if $\Delta(\rho) = \Delta(\sigma)$ and σ is a symmetric Gaussian mixed state.

Here $\Delta(\rho)$ is analogously defined as in Eq. (35).

Proof. Applying a suitable symplectic local transformation in the standard form of the γ matrix of σ [4,12] we see that the EPR correlation for this transformed matrix is $\Delta(\sigma) = \sqrt{(\tilde{n} - |\tilde{k}_x|)(\tilde{n} - |\tilde{k}_p|)}$. But the amount of entanglement is invariant by local symplectic transformations. This means that $E_f(\sigma) = f(\Delta(\sigma)) = f(\Delta(\rho))$. Let us write ρ as

$$\rho = \sum_j p_j |\varphi_j\rangle\langle\varphi_j|, \quad (39)$$

where the above decomposition is the one that furnishes the EOF of ρ , i.e.,

$$E_f(\rho) = \sum_j p_j E(\varphi_j). \quad (40)$$

Using the above expansion of ρ , we have that

$$\begin{aligned} E_f(\sigma) &= f\left(\Delta\left(\sum_j p_j |\varphi_j\rangle\langle\varphi_j|\right)\right) \leq f\left(\sum_j p_j \Delta(\varphi_j)\right) \\ &\leq \sum_j p_j f(\Delta(\varphi_j)). \end{aligned} \quad (41)$$

The first inequality is a consequence of the concavity of $\Delta(\rho)$ (see the Appendix) and the fact that f is a decreasing function of its argument [4]. The second inequality is due to the convexity of f [4]. We now use the fact that a squeezed state can assume any value of entanglement. With each pure state in the decomposition of ρ above we associate a squeezed state with the same amount of entanglement: $E(\varphi_j) = E(\Psi_s(r_j))$. Therefore we have the following relation for the EOF of ρ :

$$\begin{aligned} E_f(\rho) &= \sum_j p_j E(\varphi_j) = \sum_j p_j E(\Psi_s(r_j)) \\ &= \sum_j p_j f(\Delta(\Psi_s(r_j))). \end{aligned} \quad (42)$$

Now due to proposition 1 of Giedke *et al.* [4] we know that $\Delta(\varphi_j) \geq \Delta(\Psi_s(r_j))$. Hence, using this fact in Eq. (41) and that f is a decreasing function of its argument, we have

$$E_f(\sigma) \leq \sum_j p_j f(\Delta(\varphi_j)) \leq \sum_j p_j f(\Delta(\Psi_s(r_j))). \quad (43)$$

Combining Eqs. (42) and (43) we see that

$$E_f(\sigma) \leq E_f(\rho). \quad \blacksquare \quad (44)$$

The above theorem tells us that for mixed states the symmetric states are those with less EOF given an EPR correlation. It is interesting to note that σ can be any symmetric state, including symmetric states written as superpositions of squeezed states.

The previous theorem automatically gives us a lower bound for the EOF for general Gaussian states. Using Eq. (44) we get

$$E_f(\rho) \geq E_f(\sigma) = f(\Delta(\rho)). \quad (45)$$

We now implement a local symplectic transformation in the γ matrix of ρ , Eq. (9), before calculating the EPR correlation. (It does not alter the amount of entanglement, since it is equivalent to a unitary local transformation in the density matrix ρ .) This transformation can be viewed as an extension to nonsymmetrical Gaussian states of the transformation introduced by Giedke *et al.* [4] for symmetric states. This transformation multiplies X_j by $[(n+m)/2 - |k_p|]/[(n+m)/2 - |k_x|]^{1/4}$. P_j is divided by the same quantity. Now calculating $\Delta(\rho)$ we get the following expression for our second lower bound:

$$E_f(\rho) \geq f\left(\min\left\{1, \sqrt{\left(\frac{n+m}{2} - |k_x|\right)\left(\frac{n+m}{2} - |k_p|\right)}\right\}\right). \quad (46)$$

Again we see that this lower bound reduces to the EOF for symmetric systems whenever $n=m$. It is important to note that when

$$\sqrt{\left(\frac{n+m}{2} - |k_x|\right)\left(\frac{n+m}{2} - |k_p|\right)} > 1$$

we have $\Delta(\rho) = 1$. For such cases this lower bound is not useful since it simply shows that $E_f(\rho) \geq 0$.

IV. DISCUSSION AND EXAMPLES

We now employ the two lower bounds derived previously, Eqs. (32) and (46), to see their usefulness in analyzing some Gaussian states. For completeness we present in terms of the invariants (n, m, k_x, k_p) three inequalities they must satisfy to be considered parameters that describe physically realizable entangled Gaussian states [6]. We will assume, without loss

TABLE I. The first column shows the parameters of the γ matrix when written in its standard form. The second and third columns represent the two lower bounds for the EOF for mixed Gaussian states. Lower bound 1 is given by Eq. (32) and lower bound 2 is given by Eq. (46).

n, m, k_x, k_p	LB1	LB2
1.5, 2, 1.2, -1	0.146 35	0.289 19
1.5, 2, 1, -1	0.086 87	0.146 72
2, 3, 1.8, -1.2	0.024 48	0.006 81
1.7, 2.6, 1.3, -0.9	0.005 49	0
2, 3, 1.7, -1.2	0.007 25	0.001 42
2, 2.5, 1.3, -1.2	0.001 73	0.000 01

of generality, $m \geq n$ and $|k_x| \geq |k_p|$:

$$\det \gamma + 1 \geq n^2 + m^2 + 2k_x k_p, \quad (47a)$$

$$nm - k_x^2 \geq 1, \quad (47b)$$

$$\det \gamma + 1 < n^2 + m^2 - 2k_x k_p. \quad (47c)$$

The last inequality is the restriction a γ matrix must satisfy to represent an entangled Gaussian system.

Table I shows six entangled Gaussian systems and the values of their two lower bounds (LB1 and LB2).

These six Gaussian systems are very representative. Looking at their lower bounds we see that depending on the parameters of the system LB1 or LB2 is the strongest lower bound. For example, the first two Gaussian systems have LB2 as the strongest lower bound but the four last Gaussian systems have LB1 as the strongest one. LB1 and LB2 are also useful for discarding possible candidates for the EOF of a general mixed Gaussian state. Consider, just for illustration, the functions

$$f_1 = f(\sqrt{(\sqrt{nm} - |k_x|)(\sqrt{nm} - |k_p|)}), \quad (48)$$

$$f_2 = f\left(\sqrt{\left(\sqrt{\frac{n^2 + m^2}{2}} - |k_x|\right)\left(\sqrt{\frac{n^2 + m^2}{2}} - |k_p|\right)}\right). \quad (49)$$

Both f_1 and f_2 reduce to the EOF for symmetric states when $n = m$. For the Gaussian states with $(n, m, k_x, k_p) = (2, 2.5, 1.3, -1.2)$ we have $\text{LB1} = 0.00173 > f_1 = 0.00091$ and for $(n, m, k_x, k_p) = (1.5, 2, 1.1, -1)$ we get $\text{LB2} = 0.208853 > f_2 = 0.18621$. These results show that f_1 and f_2 cannot be proved to be the EOF for general Gaussian systems since we have lower bounds for the EOF that are greater than f_1 and f_2 .

V. CONCLUSION

We presented in this article two lower bounds for the EOF of general Gaussian two-mode systems. They were obtained by two distinct methods.

The first lower bound, Eq. (32), was derived using an interesting procedure derived by Giedke *et al.* [6] that symmetrizes by local operations a Gaussian state and the well

known fact that entanglement does not increase under LOCC.

The second lower bound, Eq. (46), is a corollary of Theorem 1, which can be interpreted as an extension of a previous result obtained by Giedke *et al.* [4]: given two pure bipartite systems with the same amount of entanglement, the squeezed states are those with the maximal EPR correlation. Our theorem generalizes this fact to mixed states in the sense that symmetric Gaussian states are shown to be states with maximal EPR correlation for a fixed amount of entanglement.

ACKNOWLEDGMENTS

The authors would like to express their gratitude for funding from Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) and Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

APPENDIX: PROOF OF CONCAVITY OF $\Delta(\rho)$

We need to prove that $\Delta(\rho) \geq \sum_j p_j \Delta(\phi_j)$, where $\rho = \sum_j p_j |\phi_j\rangle\langle\phi_j|$. Applying the definition of $\Delta(\rho)$ we obtain for the given expansion of ρ and for $\sum_j p_j \Delta(\phi_j)$ the following expressions:

$$\Delta(\rho) = \min \left\{ 1, \frac{1}{2} \left[\sum_j p_j (\langle X^2 \rangle_{\phi_j} + \langle P^2 \rangle_{\phi_j}) - \left(\sum_j p_j \langle X \rangle_{\phi_j} \right)^2 - \left(\sum_j p_j \langle P \rangle_{\phi_j} \right)^2 \right] \right\}, \quad (A1)$$

$$\begin{aligned} \sum_j p_j \Delta(\phi_j) &= \sum_j p_j \min \left\{ 1, \frac{1}{2} [\langle X^2 \rangle_{\phi_j} + \langle P^2 \rangle_{\phi_j} - \langle X \rangle_{\phi_j}^2 - \langle P \rangle_{\phi_j}^2] \right\} \\ &\leq \frac{1}{2} \sum_j p_j [\langle X^2 \rangle_{\phi_j} + \langle P^2 \rangle_{\phi_j} - \langle X \rangle_{\phi_j}^2 - \langle P \rangle_{\phi_j}^2], \end{aligned} \quad (A2)$$

where $X = X_1 - X_2$ and $P = P_1 + P_2$. The inequality is a consequence of the fact that we may have at least one $\langle X^2 \rangle_{\phi_j} + \langle P^2 \rangle_{\phi_j} - \langle X \rangle_{\phi_j}^2 - \langle P \rangle_{\phi_j}^2 > 2$. Looking at Eq. (A2) we see that it is not greater than 1. Thus, if Eq. (A1) is equal to 1 we see that $\Delta(\rho) \geq \sum_j p_j \Delta(\phi_j)$. But if it is less than 1, $\Delta(\rho) \geq \sum_j p_j \Delta(\phi_j)$ if the following inequality is satisfied:

$$\left(\sum_j p_j \langle X \rangle_{\phi_j} \right)^2 + \left(\sum_j p_j \langle P \rangle_{\phi_j} \right)^2 \leq \sum_j p_j [\langle X \rangle_{\phi_j}^2 + \langle P \rangle_{\phi_j}^2]. \quad (A4)$$

Applying the Cauchy-Schwarz inequality [13] for an observable R we get $\sum_j p_j \langle R \rangle_{\phi_j}^2 \geq (\sum_j p_j \langle R \rangle_{\phi_j})^2$. Hence, Eq. (A4) is always satisfied. ■

- [1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [2] W. K. Wootters, *Quantum Inf. Comput.* **1**, 27 (2001).
- [3] W. K. Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998).
- [4] G. Giedke, M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac, e-print quant-ph/0304042.
- [5] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature (London)* **421**, 238 (2003).
- [6] G. Giedke, L-M. Duan, I. Cirac, and P. Zoller, *Quantum Inf. Comput.* **1**, 79 (2001).
- [7] G. Giedke, Ph.D. thesis, University of Innsbruck, 2001.
- [8] R. Simon, *Phys. Rev. Lett.* **84**, 2726 (2000).
- [9] The assumption that $|K_x| \geq |K_p|$ is just for convenience. We do not lose in generality by such a assumption. We need it to correctly express K_x^2 in terms of the γ_W invariants, i.e., $K_x^2 = (W_4 + \sqrt{W_4^2 - 4W_1W_2W_3})/2\sqrt{W_1W_2}$. If we had assumed that $|K_x| < |K_p|$ we would have obtained a minus sign before the square root.
- [10] We have $m \geq n$ in the standard form of γ because we have assumed $N \geq M$ in the standard form for γ_W . This can be seen to be true by looking at Eq. (18), where we have $n^2 = M^2/\det \gamma_W$ and $m^2 = N^2/\det \gamma_W$.
- [11] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [12] This transformation multiplies X_j by $[(n - k_p)/(n - k_x)]^{1/4}$ and divides P_j by the same quantity [4].
- [13] L-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **84**, 2722 (2000).