PHYSICAL REVIEW A **76**, 012334 (2007)

Optimal entanglement witnesses based on local orthogonal observables

Cheng-Jie Zhang,* Yong-Sheng Zhang,† Shun Zhang, and Guang-Can Guo
Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China

(Received 15 May 2007; published 31 July 2007)

We show that the entanglement witnesses based on local orthogonal observables, which were introduced by Yu and Liu [Phys. Rev. Lett. **95**, 150504 (2005)] and Gühne *et al.* [Phys. Rev. A **74**, 010301(R) (2006)] in linear and nonlinear forms, respectively, can be optimized. As applications, we use our method to calculate the optimal nonlinear witnesses of pure bipartite states and to show a lower bound on the *I* concurrence of bipartite higher-dimensional systems.

DOI: 10.1103/PhysRevA.76.012334 PACS number(s): 03.67.Mn, 03.65.Ta, 03.65.Ud

I. INTRODUCTION

Entanglement is one of the most fascinating features of quantum mechanics, and has recently been recognized as a basic resource in quantum-information processing such as teleportation, dense coding, and quantum key distribution [1,2]. Thus, it becomes particularly important to detect and quantify entanglement [3]. Despite a great deal of effort in recent years, many things are still unclear to us in this field (see the reviews [4–6] and references therein). Nevertheless, on the one hand, several sufficient conditions for detection of entanglement have been found, such as the famous Peres-Horodecki positive partial transpose (PPT) criterion [7,8], the realignment criterion [9], entanglement witnesses (EWs) [10], local uncertainty relations (LURs) [11,12], Bell-type inequalities [13–15], etc. The PPT criterion is necessary and sufficient for 2×2 and 2×3 systems, but only necessary for higher-dimensional cases [8]. It is believed that the realignment criterion complements the PPT criterion, since it can detect many entangled states which the PPT criterion cannot detect. It is easier to detect entanglement experimentally using EWs, which have recently been generalized to nonlinear EWs [16,17]. On the other hand, a considerable amount of effort has also been spent on quantification of entanglement. For instance, Wootters has analytically derived a perfect measure of two qubits [18], the so-called *concurrence*. Furthermore, generalized concurrence in bipartite higher-dimensional cases [19,20], such as *I* concurrence [20], has been pointed out as well. Unfortunately, the *I* concurrence of mixed states is given as a convex roof for all possible ensemble realizations. Therefore, it is generally difficult to calculate. Lately, lower bounds on the *I* concurrence have attracted much interest [21–24]; they are easier to obtain than *I* concurrence itself.

Recently, Yu and Liu introduced an entanglement witness [Eq. (3)] based on local orthogonal observables (LOOs) in Ref. [25]. Moreover, Gühne *et al.* generalized the witness to the nonlinear form [Eq. (4)] via local uncertainty relations [26]. Both the witnesses have the common property that each set of LOOs in the witnesses can be replaced by any other complete set of LOOs; thus one does not know which set of LOOs is the best one for the witnesses. Actually, witnesses using different sets of LOOs can obtain distinct results. For example, the Bell state $(|00\rangle+|11\rangle)/\sqrt{2}$ can be detected as entangled states by the linear witness under the set of LOOs $\{\sigma_x,\sigma_y,\sigma_z,I\}^A/\sqrt{2}$, $\{\sigma_x,-\sigma_y,\sigma_z,I\}^B/\sqrt{2}$, but cannot be detected under the LOOs $\{\sigma_x,\sigma_y,\sigma_z,I\}^A/\sqrt{2}$, $\{\sigma_x,\sigma_y,\sigma_z,I\}^B/\sqrt{2}$. Therefore, it is necessary to determine the optimal case. In this paper, the optimal witnesses for the linear and nonlinear forms will be presented. As applications, we will calculate the optimal witnesses of pure bipartite states, and show a lower bound on the *I* concurrence of bipartite higher-dimensional systems.

The paper is organized as follows. Section II presents the optimal witnesses in linear and nonlinear forms, which are constructed using LOOs. In Sec. III we calculate the optimal nonlinear witnesses of pure bipartite states based on our method. Moreover, we obtain a lower bound on the *I* concurrence in bipartite systems. Section IV discusses what happens if the dimensions of the subsystems *A* and *B* are not the same.

II. OPTIMAL WITNESSES BASED ON LOOS

For convenience, we consider a $d\times d$ bipartite system, just as Refs. [25,26] did (in Sec. IV, we will discuss the situation when the dimensions of subsystems *A* and *B* are not the same). Each subsystem has a complete set of local orthogonal bases $\{G_k^A\}$ and $\{G_k^B\}$, which are the so-called LOOs. Such a basis consists of d^2 observables and satisfies

$$\mathrm{Tr}(G_k^A G_l^A)=\mathrm{Tr}(G_k^B G_l^B)=\delta_{kl}. \tag{1}$$

Any other complete set of LOOs are related to the original one by an orthogonal $d^2\times d^2$ real matrix, i.e.,

$$\widetilde{G_k^A}=\sum_l O_{kl}G_l^A,\quad \widetilde{G_k^B}=\sum_l O'_{kl}G_l^B, \tag{2}$$

where $OO^T=O^TO=O'O'^T=O'^TO'=I$.

In Ref. [25], a linear witness was introduced as follows (for convenience, the witness has been written in an equivalent form introduced in [26]):

*zhangcj@mail.ustc.edu.cn
†yshzhang@ustc.edu.cn

$$\mathcal{W}=1-\sum_k G_k^A\otimes G_k^B, \tag{3}$$

where $\{G_k^A\}$ and $\{G_k^B\}$ are arbitrary complete sets of LOOs for subsystems A and B. Later, Ref. [26] provided a nonlinear form,

$$\mathcal{F}(\rho)=1-\sum_k \langle G_k^A\otimes G_k^B\rangle-\frac{1}{2}\sum_k \langle G_k^A\otimes I-I\otimes G_k^B\rangle^2. \tag{4}$$

For every separable state ρ, it must satisfy $\mathrm{Tr}\,\mathcal{W}\rho\geqslant 0$ and $\mathcal{F}(\rho)\geqslant 0$. Conversely, if any state violates one of the two inequalities, it is indeed entangled.

In Refs. [25,26], there is a little mention of how to choose a set of LOOs so that $\mathrm{Tr}\,\mathcal{W}\rho$ or $\mathcal{F}(\rho)$ attains its minimum; obviously, the minimum value means the optimal one, since one can obtain distinct results by using different sets of LOOs. Consider the simple example $|\psi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$ introduced in Sec. I. Under the set of LOOs $\{\sigma_x,\sigma_y,\sigma_z,I\}^A/\sqrt{2}$, $\{\sigma_x,\sigma_y,\sigma_z,I\}^B/\sqrt{2}$, $\mathrm{Tr}(\mathcal{W}|\psi^+\rangle\langle\psi^+|)=0$ and $\mathcal{F}(|\psi^+\rangle\langle\psi^+|)=0$, which does not allow one to conclude that $|\psi^+\rangle$ is entangled. However, under the set of LOOs $\{\sigma_x,\sigma_y,\sigma_z,I\}^A/\sqrt{2}$, $\{\sigma_x,-\sigma_y,\sigma_z,I\}^B/\sqrt{2}$, $\mathrm{Tr}(\mathcal{W}|\psi^+\rangle\langle\psi^+|)=-1$ and $\mathcal{F}(|\psi^+\rangle\langle\psi^+|)=-1$. This suggests that $|\psi^+\rangle$ has entanglement. Therefore, it is important to look for the minimal values. In the following, we will show that the minimum is invariant under local unitary (LU) transformations, and obtain an analytical formula for the minimum.

Lemma 1. For a given state ρ, the minimum of $\mathrm{Tr}\,\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ is LU invariant.

Proof. (*Reductio ad absurdum*.) For a given state ρ, suppose that, under the set of LOOs $\{M_k^A\}$, $\{M_k^B\}$, $\mathrm{Tr}\,\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ attains its minimum L_1. We operate an arbitrary LU transformation on ρ, i.e., $\rho'=U_A\otimes U_B\rho U_A^\dagger\otimes U_B^\dagger$. For the state ρ', suppose that, under the set of LOOs $\{\widetilde{M_k^A}\}$, $\{\widetilde{M_k^B}\}$, $\mathrm{Tr}\,\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ attains its minimum L_2.

Case (i). $L_1>L_2$. For the state ρ, under the set of LOOs $\{U_A^\dagger\widetilde{M_k^A}U_A\}$, $\{U_B^\dagger\widetilde{M_k^B}U_B\}$, $\mathrm{Tr}\,\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ is equal to L_2. This contradicts the statement that L_1 is the minimum of $\mathrm{Tr}\,\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$.

Case (ii). $L_1<L_2$. For the state ρ', under the set of LOOs $\{U_AM_k^AU_A^\dagger\}$, $\{U_BM_k^BU_B^\dagger\}$, $\mathrm{Tr}\,\mathcal{W}\rho'$ $[\mathcal{F}(\rho')]$ is equal to L_1. This contradicts the statement that L_2 is the minimum of $\mathrm{Tr}\,\mathcal{W}\rho'$ $[\mathcal{F}(\rho')]$.

In a word, if $L_1\neq L_2$, a contradiction is derived immediately. Therefore, $L_1=L_2$ always holds, and the minimum of $\mathrm{Tr}\,\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ is LU invariant. ■

Remark. From an experimental point of view, it is valuable for the minimum to satisfy the LU-invariant condition, since a shared spatial reference frame is no longer needed when one makes a measure of the minimum [27].

Theorem 1. The minimum of $\mathrm{Tr}\,\mathcal{W}\rho$ is equal to $1-\Sigma_k\sigma_k(\mu)$, where $\sigma_k(\mu)$ stands for the kth singular value of a real matrix μ which is defined as $\mu_{lm}=\mathrm{Tr}(\rho G_l^A\otimes G_m^B)$.

Proof. Before embarking on our proof, it is worth noticing that a similar result to Theorem 1 has also been pointed out in [25]. However, for convenience in understanding Theorem 2, we provide a complete proof. For a given state ρ, we choose an arbitrary complete set of LOOs $\{G_k^A\}$, $\{G_k^B\}$. We define

$$\mu_{lm}=\mathrm{Tr}(\rho G_l^A\otimes G_m^B), \tag{5}$$

and the density matrix can be written as

$$\rho=\sum_{l,m}\mu_{lm}G_l^A\otimes G_m^B. \tag{6}$$

According to Eq. (2), any other complete set of LOOs $\{\widetilde{G_k^A}\}$, $\{\widetilde{G_k^B}\}$ can be written as $\widetilde{G_k^A}=\Sigma_lU_{kl}G_l^A$, $\widetilde{G_k^B}=\Sigma_mV_{km}G_m^B$, where U and V are $d^2\times d^2$ real orthogonal matrices, i.e., $UU^T=U^TU=VV^T=V^TV=I$. Therefore,

$$\begin{aligned}\min \mathrm{Tr}(\mathcal{W}\rho)&=1-\max\sum_k\langle\widetilde{G_k^A}\otimes\widetilde{G_k^B}\rangle\\&=1-\max\sum_k\sum_{lm}U_{kl}V_{km}\langle G_l^A\otimes G_m^B\rangle\\&=1-\max\sum_k\sum_{lm}U_{kl}V_{km}\mu_{lm}\\&=1-\max\sum_k[U\mu V^T]_{kk}\\&=1-\max\mathrm{Tr}(U\mu V^T).\end{aligned} \tag{7}$$

Moreover,

$$\max\mathrm{Tr}(U\mu V^T)=\max\mathrm{Tr}(\mu V^TU)=\sum_k\sigma_k(\mu), \tag{8}$$

where we have used the following theorem [28].

Let $A\in M_n$ be a given matrix, and let $A=V\Sigma W^\dagger$ be a singular value decomposition of A. Then the problem $\max\{\mathrm{Re}\,\mathrm{tr}\,AU:U\in M_n$ is unitary$\}$ has the solution $U=WV^\dagger$, and the value of the maximum is $\sigma_1(A)+\cdots+\sigma_n(A)$, where $\{\sigma_i(A)\}$ is the set of singular values of A.

Notice that μ is a real matrix and its singular value decomposition can be written as $\mu=\mathcal{U}^T\Sigma\mathcal{V}$, where $\mathcal{U}$, $\mathcal{V}$ are real orthogonal matrices and $\Sigma=\mathrm{diag}\{\sigma_1(\mu),\sigma_2(\mu),\ldots,\sigma_{d^2}(\mu)\}$. When $U=\mathcal{U}$ and $V=\mathcal{V}$, $\mathrm{Tr}(U\mu V^T)$ attains its maximum $\Sigma_k\sigma_k(\mu)$. In other words, under the new complete set of LOOs $\{\mathcal{G}_k^A\}$, $\{\mathcal{G}_k^B\}$, where $\mathcal{G}_k^A=\Sigma_l\mathcal{U}_{kl}G_l^A$, $\mathcal{G}_k^B=\Sigma_m\mathcal{V}_{km}G_m^B$, $\mathcal{W}=1-\Sigma_k\mathcal{G}_k^A\otimes\mathcal{G}_k^B$, $\mathrm{Tr}\,\mathcal{W}\rho$ attains its minimum $1-\Sigma_k\sigma_k(\mu)$. ■

Remark. In fact, this is equivalent to the realignment criterion when $\mathrm{Tr}\,\mathcal{W}\rho$ gets its minimum [25]. Note that, under the new complete set of LOOs $\{\mathcal{G}_k^A\}$, $\{\mathcal{G}_k^B\}$, the density matrix can be written in its operator–Schmidt decomposition form [29]:

$$\rho=\sum_k\sigma_k(\mu)\mathcal{G}_k^A\otimes\mathcal{G}_k^B. \tag{9}$$

The realignment criterion states that, if ρ is separable, the sum of all $\sigma_k(\mu)$ is smaller than 1. It is equivalent to $\min\mathrm{Tr}\,\mathcal{W}\rho\geqslant 0$. Hence, it is concluded that any entangled state detected by a witness of Eq. (3) must violate the realignment criterion.

Example. Let us consider the noisy singlet state introduced in Ref. [26], $\rho=p|\psi_s\rangle\langle\psi_s|+(1-p)\rho_{sep}$, where $|\psi_s\rangle$ stands for the singlet state $(|01\rangle-|10\rangle)/\sqrt{2}$, and the separable noise is $\rho_{sep}=2/3|00\rangle\langle 00|+1/3|01\rangle\langle 01|$. Actually, the state is entangled for any $p>0$ [26]. Under the complete set of LOOs $\{-\sigma_x,-\sigma_y,-\sigma_z,I\}^A/\sqrt{2}$, $\{\sigma_x,\sigma_y,\sigma_z,I\}^B/\sqrt{2}$, the witness of Eq. (3) can detect the entanglement for all $p>0.4$. However, the optimal witness using Theorem 1 can detect the entanglement for all $p>0.292$, which is equivalent to the realignment criterion.

Theorem 2. The minimum of $\mathcal{F}(\rho)$ is equal to $1-\Sigma_k\sigma_k(\tau)-(\mathrm{Tr}\,\rho_A^2+\mathrm{Tr}\,\rho_B^2)/2$, where $\sigma_k(\tau)$ stands for the kth singular value of matrix τ defined as $\tau_{lm}=\langle G_l^A\otimes G_m^B\rangle-\langle G_l^A\otimes I\rangle\langle I\otimes G_m^B\rangle$.

Proof. For a given state ρ, we choose an arbitrary complete sets of LOOs $\{G_k^A\}$, $\{G_k^B\}$, and calculate the real matrix τ according to the definition

$$\tau_{lm}=\langle G_l^A\otimes G_m^B\rangle-\langle G_l^A\otimes I\rangle\langle I\otimes G_m^B\rangle. \tag{10}$$

Similarly to Theorem 1, any other complete set of LOOs $\{\widetilde{G_k^A}\}$, $\{\widetilde{G_k^B}\}$ can be written as $\widetilde{G_k^A}=\Sigma_l U_{kl}G_l^A$, $\widetilde{G_k^B}=\Sigma_m V_{km}G_m^B$, where U and V are $d^2\times d^2$ real orthogonal matrices, i.e., $UU^T=U^TU=VV^T=V^TV=I$. Therefore,

$$\min\left(1-\sum_k\langle\widetilde{G_k^A}\otimes\widetilde{G_k^B}\rangle-\frac{1}{2}\sum_k\langle\widetilde{G_k^A}\otimes I-I\otimes\widetilde{G_k^B}\rangle^2\right)$$
$$=1-\max\left(\sum_k\langle\widetilde{G_k^A}\otimes\widetilde{G_k^B}\rangle+\frac{1}{2}\sum_k\langle\widetilde{G_k^A}\otimes I-I\otimes\widetilde{G_k^B}\rangle^2\right).$$

Moreover,

$$\sum_k\langle\widetilde{G_k^A}\otimes I-I\otimes\widetilde{G_k^B}\rangle^2=\sum_k[\langle\widetilde{G_k^A}\otimes I\rangle^2+\langle I\otimes\widetilde{G_k^B}\rangle^2-2\langle\widetilde{G_k^A}\otimes I\rangle\langle I\otimes\widetilde{G_k^B}\rangle],$$

where $\Sigma_k\langle\widetilde{G_k^A}\otimes I\rangle^2$ and $\Sigma_k\langle I\otimes\widetilde{G_k^B}\rangle^2$ are invariant under LOO transformations, i.e.,

$$\begin{aligned}\sum_k\langle\widetilde{G_k^A}\otimes I\rangle^2&=\sum_k\sum_{ll'}U_{kl}U_{kl'}\langle G_l^A\otimes I\rangle\langle G_{l'}^A\otimes I\rangle\\&=\sum_{ll'}[U^TU]_{ll'}\langle G_l^A\otimes I\rangle\langle G_{l'}^A\otimes I\rangle\\&=\sum_l\langle G_l^A\otimes I\rangle^2\\&=\mathrm{Tr}\rho_A^2,\end{aligned}$$

where ρ_A is the reduced density matrix after tracing over subsystem B. Without loss of generality, substituting Eq. (11) into $\Sigma_l\langle G_l^A\otimes I\rangle^2$, one can obtain the final result $\mathrm{Tr}\rho_A^2$. Similarly, $\Sigma_k\langle I\otimes\widetilde{G_k^B}\rangle^2=\Sigma_l\langle I\otimes G_l^B\rangle^2=\mathrm{Tr}\rho_B^2$ holds.

$$G_k^A=\begin{cases}\frac{1}{\sqrt{2}}(|m\rangle\langle n|+|n\rangle\langle m|), & 1\le m<n\le d,\\ \frac{1}{\sqrt{2}}(i|m\rangle\langle n|-i|n\rangle\langle m|), & 1\le m<n\le d,\\ |m\rangle\langle m|, & 1\le m\le d.\end{cases} \tag{11}$$

$$G_k^B=(G_k^A)^T, \tag{12}$$

where $\{|m\rangle_A\}$ and $\{|m\rangle_B\}$ are the standard complete bases. Thus,

$$\begin{aligned}&\max\left(\sum_k\langle\widetilde{G_k^A}\otimes\widetilde{G_k^B}\rangle+\frac{1}{2}\sum_k\langle\widetilde{G_k^A}\otimes I-I\otimes\widetilde{G_k^B}\rangle^2\right)\\&=\frac{1}{2}\sum_k[\langle\widetilde{G_k^A}\otimes I\rangle^2+\langle I\otimes\widetilde{G_k^B}\rangle^2]\\&\quad+\max\left(\sum_k(\langle\widetilde{G_k^A}\otimes\widetilde{G_k^B}\rangle-\langle\widetilde{G_k^A}\otimes I\rangle\langle I\otimes\widetilde{G_k^B}\rangle)\right)\\&=\frac{1}{2}(\mathrm{Tr}\rho_A^2+\mathrm{Tr}\rho_B^2)+\max\sum_k\sum_{lm}U_{kl}V_{km}\tau_{lm}\\&=\frac{1}{2}(\mathrm{Tr}\rho_A^2+\mathrm{Tr}\rho_B^2)+\max\sum_k[U\tau V^T]_{kk}\\&=\frac{1}{2}(\mathrm{Tr}\rho_A^2+\mathrm{Tr}\rho_B^2)+\sum_k\sigma_k(\tau).\end{aligned} \tag{13}$$

In other words, $\min\mathcal{F}(\rho)=1-\Sigma_k\sigma_k(\tau)-(\mathrm{Tr}\rho_A^2+\mathrm{Tr}\rho_B^2)/2$. ■

Example. Bennett *et al.* introduced a 3×3 bound entangled state constructed from unextendible product bases in Ref. [30]:

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

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

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

$$\rho=\frac{1}{4}\left(I-\sum_{i=0}^{4}|\psi_i\rangle\langle\psi_i|\right). \tag{14}$$

Let us consider a mixture of this state with white noise,

$$\rho(p)=p\rho+(1-p)\frac{I}{9}. \tag{15}$$

Using the realignment criterion, one finds that the state $\rho(p)$ still has entanglement when $p>0.8897$. In Ref. [26], it is found that the state $\rho(p)$ must be entangled for $p>p_{lur}=0.8885$, using the nonlinear witness Eq. (4) (but not the optimal one). According to Theorem 2, one can obtain an optimal witness of Eq. (4), and find that when $p>p_{opt}=0.8822$ the state is still entangled. Obviously, the optimal witness is stronger than the one in Ref. [26]. In addition, in Sec. III we will present a lower bound on the I concurrence for the state based on Theorem 2 (see Fig. 1). From the figure, it is worth noticing that the bound is positive when $p>p_{opt}=0.8822$.

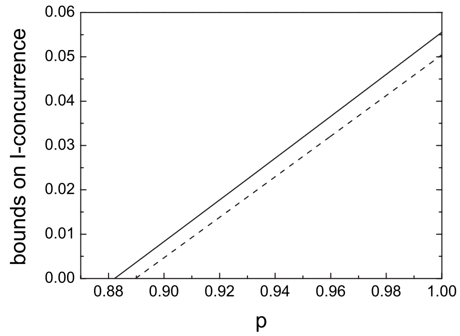

FIG. 1. Two lower bounds of I concurrence for the state $\rho(p)$. One is the lower bound based on the realignment criterion (dashed line), the other is obtained from $\mathcal{L}_{max}$ (solid line).

III. APPLICATIONS

In this section, the optimal nonlinear witnesses of pure bipartite states will be obtained using Theorem 2. Moreover, we will show a lower bound on the I concurrence of bipartite systems by means of our method. Before embarking on our investigation, we first define that $\mathcal{L}=\frac{1}{2}\Sigma_k\langle G_k^A\otimes I-I\otimes G_k^B\rangle^2+\Sigma_k\langle G_k^A\otimes G_k^B\rangle$, and obviously $\mathcal{L}_{max}=\Sigma_k\sigma_k(\tau)+(\mathrm{Tr}\,\rho_A^2+\mathrm{Tr}\,\rho_B^2)/2$, according to Theorem 2.

A. Optimal witnesses of bipartite pure states

Let us calculate $\mathcal{L}_{max}$ of a bipartite pure state $|\psi\rangle$ with its Schmidt decomposition $|\psi\rangle=\Sigma_i\sqrt{\mu_i}|ii\rangle$.

Since Schmidt decomposition of a pure state is a LU transformation, $\mathcal{L}_{max}(|\psi\rangle)$ remains invariant after the transformation according to Lemma 1. Therefore, we can directly use the Schmidt decomposition form for convenience. We choose a complete set of LOOs Eqs. (11) and (12) for the A and B subsystems, respectively (obviously any other complete set of LOOs can be chosen, and it does not affect the final result).

According to Theorem 2,

$$\tau_{lm}=\langle G_l^A\otimes G_m^B\rangle-\langle G_l^A\otimes I\rangle\langle I\otimes G_m^B\rangle=[D\oplus D\oplus T]_{lm}, \tag{16}$$

where $D=\mathrm{diag}\{\sqrt{\mu_1\mu_2},\ldots,\sqrt{\mu_m\mu_n},\ldots,\sqrt{\mu_{d-1}\mu_d}\}$ and

$$T=\begin{pmatrix}\mu_1-\mu_1^2 & -\mu_1\mu_2 & \cdots & -\mu_1\mu_d\\ -\mu_1\mu_2 & \mu_2-\mu_2^2 & \cdots & -\mu_2\mu_d\\ \vdots & \vdots & \ddots & \vdots\\ -\mu_1\mu_d & -\mu_2\mu_d & \cdots & \mu_d-\mu_d^2\end{pmatrix}. \tag{17}$$

Therefore,

$$\sum_k\sigma_k(\tau)=2\sum_{m<n}\sqrt{\mu_m\mu_n}+2\sum_{m<n}\mu_m\mu_n, \tag{18}$$

$$\frac{1}{2}(\mathrm{Tr}\,\rho_A^2+\mathrm{Tr}\,\rho_B^2)=\sum_i\mu_i^2, \tag{19}$$

$$\mathcal{L}_{max}(|\psi\rangle)=\left(\sum_i\sqrt{\mu_i}\right)^2. \tag{20}$$

Note that Eq. (20) has also been derived with another totally different method in Ref. [23], and it completely accords with our result. Compared with the method in Ref. [23], Theorem 2 in this paper is more general, i.e., it suits not only bipartite pure states but also any bipartite mixed state.

B. Lower bound on the I concurrence

The I concurrence of a bipartite pure state is given by $C(|\psi\rangle)=\sqrt{2(1-\mathrm{Tr}\,\rho_A^2)}$, where the reduced density matrix ρ_A is obtained by tracing over the subsystem B. It can be extended to mixed states ρ by the convex roof,

$$C(\rho)=\inf_{\{p_i,|\psi_i\rangle\}}\sum_i p_iC(|\psi_i\rangle),\quad \rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|, \tag{21}$$

for all possible decompositions into pure states, where $p_i\geqslant 0$ and $\Sigma_ip_i=1$.

Several bounds have already been derived [21–24], e.g., an analytical lower bound based on the PPT criterion and the realignment criterion has been shown by Chen *et al.*:

$$C(\rho)\geqslant\sqrt{\frac{2}{m(m-1)}}[\max(\|\rho^{T_A}\|,\|\mathcal{R}(\rho)\|)-1], \tag{22}$$

where T_A, $\mathcal{R}$, and $\|\cdot\|$ stand for the partial transpose, realignment, and the trace norm (i.e., the sum of the singular values), respectively. In Ref. [23], another bound based on LOOs has been obtained, which used Eq. (20) and the fact that $\Sigma_ip_i\mathcal{L}_{max}(|\psi_i\rangle)\geqslant\Sigma_ip_i\mathcal{L}(|\psi_i\rangle)\geqslant\mathcal{L}(\Sigma_ip_i|\psi_i\rangle\langle\psi_i|)$ (for convenience, the lower bound has been rewritten in an equivalent form):

$$C(\rho)\geqslant\sqrt{\frac{2}{m(m-1)}}(\mathcal{L}-1). \tag{23}$$

Notice that Eq. (23) holds for arbitrary sets of LOOs, including the optimal one. Therefore, a tighter form of Eq. (23) can be obtained according to Theorem 2,

$$C(\rho)\geqslant\sqrt{\frac{2}{m(m-1)}}(\mathcal{L}_{max}-1), \tag{24}$$

where $\mathcal{L}_{max}=\Sigma_k\sigma_k(\tau)+(\mathrm{Tr}\,\rho_A^2+\mathrm{Tr}\,\rho_B^2)/2$. Since the entanglement criteria based on LURs are strictly stronger than the realignment criterion [26], the following inequality can be stated:

$$C(\rho)\geqslant\sqrt{\frac{2}{m(m-1)}}\{\max[\|\rho^{T_A}\|,\mathcal{L}_{max}(\rho)]-1\}. \tag{25}$$

For example, reconsider the bound entangled state Eq. (14). Because it belongs to a PPT entangled state, the lower bound based on the PPT criterion is unhelpful. One can obtain that $C(\rho)\geqslant 0.050$ via the realignment criterion, and $C(\rho)\geqslant 0.052$ was obtained in Ref. [23] by using Eq. (23). In fact, $\mathcal{L}_{max}(\rho)$ can be directly calculated, and it suggests that $C(\rho)\geqslant 0.055$ via Eq. (24), which is better than the bound in Ref. [23]. Furthermore, one can consider the bound entangled state with white noise, i.e., Eq. (15). The lower bounds of I concurrence for $\rho(p)$ are shown in Fig. 1; the lower bound based on $\mathcal{L}_{max}$ has been strictly improved compared with the one based on the realignment criterion, and it provides a tighter form of Eq. (23).

IV. DISCUSSION AND CONCLUSION

In the last two sections, we considered a simple situation: the $d\times d$ bipartite system for convenience. However, if the dimensions of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are not the same, what will happen? Actually, it does not affect any one of the conclusions in Secs. II and III.

Without loss of generality, suppose that $m=\dim(\mathcal{H}_A)<n=\dim(\mathcal{H}_B)$. There are m^2 elements in a complete set of LOOs $\{G_k^A\}$, and n^2 elements in $\{G_k^B\}$. Therefore, we need to reconsider Eqs. (8) and (13) in Theorems 1 and 2, respectively:

$$\max \sum_k \sum_{lm} U_{kl}V_{km}\mu_{lm} = \max \operatorname{Tr}(U\mu V^T), \tag{26}$$

$$\max \sum_k \sum_{lm} U_{kl}V_{km}\tau_{lm} = \max \operatorname{Tr}(U\tau V^T), \tag{27}$$

where U is an $m^2\times m^2$ real orthogonal matrix; μ and τ are $m^2\times n^2$ real matrices; V belongs to $n^2\times n^2$ real orthogonal matrices. The two equations have the same form, so we just need to consider Eq. (27), for instance.

As in Ref. [26], one can define $G_k^A=0$ for $k=m^2+1,\ldots,n^2$. Thus, the matrix τ is changed into an $n^2\times n^2$ real matrix, i.e.,

$$\tau' = \begin{pmatrix}\tau\\ 0\end{pmatrix}, \tag{28}$$

where 0 stands for an $(n^2-m^2)\times n^2$ matrix with every element being equal to 0.

Define $U'=U\oplus I$, where I is an $(n^2-m^2)\times(n^2-m^2)$ identity matrix. It is easy to see that U' is an $n^2\times n^2$ real orthogonal matrix since U belongs to $m^2\times m^2$ real orthogonal matrices.

Notice that $(l\equiv n^2-m^2)$

$$\begin{pmatrix}U_{m^2\times m^2} & 0\\ 0 & I_{l\times l}\end{pmatrix}\begin{pmatrix}\tau_{m^2\times n^2}\\ 0_{l\times n^2}\end{pmatrix}\left(V^T_{n^2\times n^2}\right) = \begin{pmatrix}[U\tau V^T]_{m^2\times n^2}\\ 0_{l\times n^2}\end{pmatrix},$$

which means that $\operatorname{Tr}(U'\tau' V^T)=\operatorname{Tr}(U\tau V^T)$. Therefore,

$$\begin{aligned}\max \operatorname{Tr}(U\tau V^T) &= \max \operatorname{Tr}(U'\tau' V^T)\\ &= \max \operatorname{Tr}(\tau' V^T U')\\ &= \sum_k \sigma_k(\tau').\end{aligned} \tag{29}$$

Since $\tau'\tau'^T=(\tau\tau^T)\oplus 0_{l\times l}$, $\tau'\tau'^T$ and $\tau\tau^T$ have the same nonzero eigenvalues. Hence,

$$\sum_k \sigma_k(\tau') = \sum_k \sigma_k(\tau). \tag{30}$$

Consequently, Eqs. (29) and (30) suggest that Theorems 1 and 2 still hold, even if the dimensions of subsystems A and B are not the same, and the applications in Sec. III that used Theorem 2 can also be extended to this case.

In conclusion, we have optimized the linear and nonlinear entanglement witnesses based on local orthogonal observables, which were introduced by Yu and Liu and Gühne *et al.*, respectively, and several examples have been given as well. Moreover, we have obtained the optimal witnesses based on LOOs in pure bipartite systems, and a lower bound on the I concurrence of bipartite systems as applications of our method. In fact, Theorem 2 presents a separability criterion with Ky Fan norm of τ, the covariance term defined in [27]. Similarly, another separability criterion with Ky Fan norm of correlation matrix has been shown in [31]. It is worth investigating a deeper relation between these two criteria. In addition, the term "optimal" in this paper is used in the sense of choosing the best complete set of LOOs such that the witness attains its minimum, which has little relation to traditional optimal EWs [32].

Note added. Recently, a similar result has been shown in [33], which is based on the covariance matrix criterion. Interestingly, Proposition 3 in [33] can be optimized to a similar form as Theorem 2 in this paper.

ACKNOWLEDGMENTS

This work was funded by the National Fundamental Research Program Grant No. (2006CB921900), the National Natural Science Foundation of China (Grants No. 10674127 and No. 60121503), the Innovation Funds from the Chinese Academy of Sciences, and the Program for New Century Excellent Talents in University.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
[2] *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation and Quantum Computation*, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer, New York, 2000).
[3] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[4] D. Bruß, J. Math. Phys. **43**, 4237 (2002).
[5] M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007).
[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, e-print arXiv:quant-ph/0702225.
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[9] O. Rudolph, e-print arXiv:quant-ph/0202121; K. Chen and L.-A. Wu, Quantum Inf. Comput. **3**, 193 (2003).
[10] B. Terhal, Phys. Lett. A **271**, 319 (2000); G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005); M. A. Jafarizadeh, M. Rezaee, and S. K. A. Seyed Yagoobi, Phys. Rev. A **72**, 062106 (2005).

[11] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003); H. F. Hofmann, *ibid.* **68**, 034307 (2003).
[12] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).
[13] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[14] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[15] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990); M. Ardehali, Phys. Rev. A **46**, 5375 (1992); A. V. Belinskii and D. N. Klyshko, Phys. Usp. **36**, 653 (1993); N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).
[16] O. Gühne and N. Lütkenhaus, Phys. Rev. Lett. **96**, 170502 (2006).
[17] F. A. Bovino, G. Castagnoli, A. Ekert, P. Horodecki, C. M. Alves, and A. V. Sergienko, Phys. Rev. Lett. **95**, 240407 (2005); R. Augusiak, P. Horodecki, and M. Demianowicz, e-print arXiv:quant-ph/0604109.
[18] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[19] A. Uhlmann, Phys. Rev. A **62**, 032307 (2000).
[20] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).
[21] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **92**, 167902 (2004).
[22] K. Chen, S. Albeverio, and S.-M. Fei, Phys. Rev. Lett. **95**, 040504 (2005).
[23] J. I. de Vicente, Phys. Rev. A **75**, 052320 (2007).
[24] H. P. Breuer, J. Phys. A **39**, 11847 (2006).
[25] S. Yu and N.-L. Liu, Phys. Rev. Lett. **95**, 150504 (2005).
[26] O. Gühne, M. Mechler, G. Tóth, and P. Adam, Phys. Rev. A **74**, 010301(R) (2006).
[27] C. Kothe and G. Björk, Phys. Rev. A **75**, 012336 (2007); Z.-W. Wang, Y.-F. Huang, X.-F. Ren, Y.-S. Zhang, and G.-C. Guo, Europhys. Lett. **78**, 40002 (2007).
[28] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, U.K., 1985), Theorem 7.4.9.
[29] M. A. Nielsen, Ph.D. thesis, University of New Mexico, 1998, e-print arXiv:quant-ph/0011036; M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, and A. Hines, Phys. Rev. A **67**, 052301 (2003).
[30] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[31] J. I. de Vicente, Quantum Inf. Comput. **7**, 624 (2007).
[32] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000); M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, *ibid.* **63**, 044304 (2001).
[33] See O. Gühne, P. Hyllus, O. Gittsovich, and J. Eisert, e-print arXiv:quant-ph/0611282v2, Proposition 3.