Minimum-error discrimination of quantum states: Bounds and comparisons

Daowen Qiu[1,2,*] and Lvjun Li[1,†]

[1]Department of Computer Science, Zhongshan University, Guangzhou 510006, People's Republic of China

[2]SQIG–Instituto de Telecomunicações, IST, TULisbon, Avenida Rovisco Pais 1049-001, Lisbon, Portugal

(Received 4 February 2010; published 29 April 2010)

We derive a new bound on the minimum-error probability for ambiguous discrimination and compare the new bound with six other bounds in the literature. Specifically, the main technical contributions are as follows. (1) We obtain a general lower bound on the minimum-error probability for ambiguous discrimination among arbitrary m mixed quantum states with given prior probabilities. We further analyze how this lower bound is attainable by presenting a necessary and sufficient condition related to it. (2) We compare this new lower bound with six other bounds in the literature, in detail. We show that this new bound improves the previous one in the literature and in the equiprobable case; the new bound also improves another one. Moreover, we give an example to show that this new bound is the tightest one for some cases.

DOI: 10.1103/PhysRevA.81.042329 PACS number(s): 03.67.−a, 03.65.Ta

I. INTRODUCTION

A fundamental issue in quantum information science is that nonorthogonal quantum states cannot be perfectly discriminated, and indeed, motivated by the study of quantum communication and quantum cryptography [1], distinguishing quantum states has become a more and more important subject in quantum information theory [2–8]. This problem may be roughly described by the connection between quantum communication and quantum-state discrimination in this manner [2,3,6–8]: Suppose that a transmitter, Alice, wants to convey classical information to a receiver, Bob, using a quantum channel, and Alice represents the message conveyed as a mixed quantum state that, with given prior probabilities, belongs to a finite set of mixed quantum states, say $\{\rho_1,\rho_2,\ldots,\rho_m\}$; then Bob identifies the state by a measurement.

As is known, if the supports of mixed states $\rho_1,\rho_2,\ldots,\rho_m$ are not mutually orthogonal, then Bob cannot reliably identify which state Alice has sent, namely, $\rho_1,\rho_2,\ldots,\rho_m$ can not be faithfully distinguished [2,7,8]. However, it is always possible to discriminate them in a probabilistic means. To date, there have been many interesting results concerning quantum-state discrimination; refer to [3,4], and [6], and references therein. It is worth mentioning that some schemes of quantum-state discrimination have been experimentally realized (e.g., see [9–11] and the detailed review in [6]).

Various strategies have been proposed for distinguishing quantum states [3,4,6], including *ambiguous discrimination*, *unambiguous discrimination*, and a method combining both strategies. Assume that mixed states $\rho_1,\rho_2,\ldots,\rho_m$ have the *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively. An important approach to discriminate them is ambiguous (also called *quantum-state detection*) [2,7,8], which is studied further in this paper, in which an inconclusive outcome is not allowed, and thus error may result. A measurement for discrimination consists of m measurement operators (e.g., positive semidefinite operators) that form a resolution of the identity on the Hilbert space spanned by all eigenvectors corresponding to all nonzero eigenvalues of $\rho_1,\rho_2,\ldots,\rho_m$. Much work has been devoted to devising a measurement maximizing the success probability (i.e., minimizing the error probability) of detecting the states [12–14].

The first important result is the pioneering work by Helstrom [2]—a general expression of the minimum achievable error probability of distinguishing between two mixed quantum states. For the case of more than two quantum states, some necessary and sufficient conditions have been derived for an optimum measurement maximizing the success probability of correct detection [7,8]. However, analytical solutions for an optimum measurement have been obtained only for some special cases (see, e.g., [15–17]).

Regarding the minimum-error probability for ambiguous discrimination among arbitrary m mixed quantum states with given prior probabilities, Hayashi *et al.* [18] gave a lower bound in terms of the individual operator norm. Recently, Qiu [19] obtained a different lower bound by means of pairwise trace distance. When $m = 2$, these two bounds are precisely the well-known Helstrom limit [2]. Later, Montanaro [20] derived another lower bound by virtue of pairwise fidelity. However, when $m = 2$, the lower bound in [20] is smaller than the Helstrom limit. Indeed, it is worth mentioning that, with a lemma [21], we can also obtain a different lower bound represented by the prior probabilities (we review these bounds in detail in Sec. II). Besides this, there also exist other estimates of minimum-error probability [22–26].

In this paper, we derive a new lower bound on the minimum-error probability for ambiguous discrimination between arbitrary m mixed quantum states with given prior probabilities. We show that this bound improves the previous one derived in [19], and in the equiprobable case, the new bound also improves the one derived in [20]. Also, we further present a necessary and sufficient condition to show how this new lower bound is attainable.

The remainder of the paper is organized as follows. In Sec. II, we review six of the existing lower bounds on the minimum-error probability for ambiguous discrimination between arbitrary m mixed states and also give the new bound in this paper, which is derived in the next section. Then, in

*issqdw@mail.sysu.edu.cn

†hnbcllj@163.com

Sec. III, we present the new lower bound on the minimum-error probability for ambiguous discrimination between arbitrary m mixed states, and we give a necessary and sufficient condition to show how this new lower bound is attainable. Furthermore, in Sec. IV, we show that this new bound improves the previous one [19], and in the equiprobable case, the new bound also improves the one derived in [20]. In particular, we try to compare the new bound with these six other bounds reviewed in Sec. II. Finally, some concluding remarks are made in Sec. V.

II. REVIEWING LOWER BOUNDS ON THE MINIMUM-ERROR PROBABILITY

This section reviews some of the existing lower bounds on the minimum-error probability for ambiguous discrimination between arbitrary m mixed states. Also, we present the new bound in this paper, but its proof is deferred to the next section.

Assume that a quantum system is described by a mixed quantum state, say ρ, drawn from a collection $\{\rho_1,\rho_2,\ldots,\rho_m\}$ of mixed quantum states on an n-dimensional complex Hilbert space $\mathcal{H}$, with the *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively. We assume without loss of generality that all eigenvectors of ρ_i, $1\leqslant i\leqslant m$, span $\mathcal{H}$; otherwise we consider the spanned subspace instead of $\mathcal{H}$. A mixed quantum state [27,28] ρ is a positive semidefinite operator with trace 1, denoted $\mathrm{Tr}(\rho)=1$. (Note that a positive semidefinite operator must be a Hermitian operator.) To detect ρ, we need to design a measurement consisting of m positive semidefinite operators, say Π_i, $1\leqslant i\leqslant m$, satisfying the resolution

$$\sum_{i=1}^{m}\Pi_i=I, \tag{1}$$

where I denotes the identity operator on $\mathcal{H}$. By the measurement Π_i, $1\leqslant i\leqslant m$, if the system has been prepared by ρ, then $\mathrm{Tr}(\rho\Pi_i)$ is the probability of deducing the system's being state ρ_i. Therefore, with this measurement, the average probability P of correctly detecting the system's state is as follows:

$$P=\sum_{i=1}^{m}p_i\mathrm{Tr}(\rho_i\Pi_i). \tag{2}$$

The average probability Q of erroneous detection is

$$Q=1-P=1-\sum_{i=1}^{m}p_i\mathrm{Tr}(\rho_i\Pi_i). \tag{3}$$

A main objective is to design an optimum measurement that minimizes the probability of erroneous detection. As mentioned, for the case of $m=2$, the optimum detection problem has been completely solved by Helstrom [4], and the minimum attainable error probability, say Q_E, is, by the Helstrom limit [4],

$$Q_E=\tfrac{1}{2}(1-\mathrm{Tr}|p_2\rho_2-p_1\rho_1|), \tag{4}$$

where $|A|=\sqrt{A^\dagger A}$ for any linear operator A, and $A^\dagger$ denotes the conjugate transpose of A.

For discriminating more than two states, some bounds have been obtained [18–26], and we review six lower bounds [18–23] here. We first give a lower bound, and it follows from the subsequent lemma.

Lemma 1 [21]. If $0\leqslant\lambda_i\leqslant 1$, and $\sum_{i=1}^m\lambda_i\leqslant l$, then $\sum_{i=1}^m p_i\lambda_i\leqslant \mathrm{Pr}(\{p_i\},l)$, where $\{p_1,p_2,\ldots,p_m\}$ is a probability distribution, and $\mathrm{Pr}(\{p_i\},l)$ denotes the sum of the l comparatively larger probabilities of $\{p_1,p_2,\ldots,p_m\}$ [e.g., if $p_{i_1}\geqslant p_{i_2}\geqslant\cdots\geqslant p_{i_m}$ and $l\leqslant m$, then $\mathrm{Pr}(\{p_i\},l)=\sum_{k=1}^{l}p_{i_k}$].

From this lemma it follows a lower bound on the minimum-error probability for ambiguous discrimination between $\{\rho_1,\rho_2,\ldots,\rho_m\}$ with the *a priori* probabilities $p_1,p_2,\ldots,p_m$. We first recall the operator norm and trace norm of operator A. $\|A\|$ denotes the operator norm of A, that is, $\|A\|=\max\{\|A|\psi\rangle\|:|\psi\rangle\in\mathcal{S}\}$, where $\mathcal{S}$ is the set of all unit vectors, that is, $\|A\|$ is the largest singular value of A. $\|A\|_{\mathrm{tr}}=\mathrm{Tr}\sqrt{A^\dagger A}$ denotes the trace norm of A; equivalently, $\|A\|_{\mathrm{tr}}$ is the sum of the singular values of A.

Theorem 2. For any m mixed quantum states $\rho_1,\rho_2,\ldots,\rho_m$ with *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively, then the minimum-error probability Q_E satisfies $Q_E\geqslant L_0$, where

$$L_0=1-\mathrm{Pr}(\{p_i\},d), \tag{5}$$

and d denotes the dimension of the Hilbert space spanned by $\{\rho_i\}$.

Proof. Let P_S denote the optimal correct probability, and let $\mathbb{E}_m$ denote the class of all positive-operator-valued measures (POVMs) of the form $\{E_i:1\leqslant i\leqslant m\}$. Due to

$$\begin{aligned}\sum_{i=1}^{m}\mathrm{Tr}(\rho_iE_i)&\leqslant\sum_{i=1}^{m}\|\rho_i\|\,\|E_i\|_{\mathrm{tr}}=\sum_{i=1}^{m}\|E_i\|_{\mathrm{tr}}\\&=\sum_{i=1}^{m}\mathrm{Tr}(E_i)=\mathrm{Tr}(I)=d,\end{aligned} \tag{6}$$

and with Lemma 1, we have

$$\sum_{i=1}^{m}p_i\mathrm{Tr}(\rho_iE_i)\leqslant\mathrm{Pr}(\{p_i\},d). \tag{7}$$

We thus get

$$P_S=\max_{\{E_j\}\in\mathbb{E}_m}\sum_{i=1}^{m}p_i\mathrm{Tr}(\rho_iE_i)\leqslant\mathrm{Pr}(\{p_i\},d). \tag{8}$$

Therefore, we have

$$Q_E=1-P_S\geqslant 1-\mathrm{Pr}\left(\{p_i\},d\right). \tag{9}$$

The proof is completed. ■

Another lower bound L_1 was given by Hayashi *et al.* [18] in terms of the individual operator norm. That is,

$$L_1=1-d\max_{i=1,\ldots,m}\{||p_i\rho_i||\}, \tag{10}$$

where d, as above, is the dimension of the Hilbert space spanned by $\{\rho_i\}$. It is easily seen that L_1 may be negative for discriminating some states.

Recently, Qiu [19] gave a lower bound L_2 in terms of pairwise trace distance, that is,

$$L_2=\frac{1}{2}\left(1-\frac{1}{m-1}\sum_{1\leqslant i<j\leqslant m}\mathrm{Tr}|p_j\rho_j-p_i\rho_i|\right). \tag{11}$$

Then Montanaro [20] derived a lower bound L_3 in terms of pairwise fidelity, that is,

$$L_3 = \sum_{1\leqslant i<j\leqslant m} p_i p_j F^2(\rho_i,\rho_j), \tag{12}$$

where, also in this paper, $F(\rho_i,\rho_j) = \mathrm{Tr}\sqrt{\sqrt{\rho_i}\rho_j\sqrt{\rho_i}}$ as usual [28].

In this paper, we derive a new lower bound L_4 in terms of trace distance. More exactly,

$$L_4 = 1 - \min_{k=1,\ldots,m}\left\{p_k + \sum_{j\neq k}\mathrm{Tr}(p_j\rho_j - p_k\rho_k)_+\right\}, \tag{13}$$

where $(p_j\rho_j - p_k\rho_k)_+$ denotes the positive part of a spectral decomposition of $p_j\rho_j - p_k\rho_k$. The proof for deriving L_4 is deferred to Sec. III.

In addition, Nagaoka *et al.* [23] gave a two-sided estimate, which is tight within a factor of 2 and includes a lower bound L_5, that is,

$$L_5 = 1 - \mathrm{Tr}\sqrt{\sum_{i=1}^m p_i^2\rho_i^2}. \tag{14}$$

Montanaro [22] derived a lower bound of pure-states discrimination. For discriminating pure states $\{|\psi_i\rangle\}$ with the *a priori* probabilities p_i, the minimum-error probability satisfies

$$Q_E^* \geqslant 1 - \sqrt{\sum_{i=1}^m (\langle\psi_i'|\rho^{-\frac{1}{2}}|\psi_i'\rangle)^2}, \tag{15}$$

where $|\psi_i'\rangle = \sqrt{p_i}|\psi_i\rangle$ and $\rho = \sum_{i=1}^m |\psi_i'\rangle\langle\psi_i'|$. By the following lemma of Tyson [23], a mixed-state lower bound can be obtained from the pure-state lower bound.

Lemma 3 [23]. Take spectral decompositions $\rho_i = \sum_k \lambda_{ik}|\psi_{ik}\rangle\langle\psi_{ik}|$, and consider the pure-state ensemble $\xi^* = \{(|\psi_{ik}\rangle, p_i\lambda_{ik})\}$. Then the minimum-error probability Q_E^* for discriminating ξ^* satisfies

$$Q_E \leqslant Q_E^* \leqslant (2 - Q_E)Q_E. \tag{16}$$

From Lemma 3, we can get

$$Q_E \geqslant 1 - \sqrt{1 - Q_E^*}. \tag{17}$$

So we get a lower bound for discriminating the mixed state $\{\rho_i\}$, that is,

$$Q_E \geqslant 1 - \sqrt[4]{\sum_{i=1}^m \sum_{k=1}^{\mathrm{rank}(\rho_i)} (\langle\psi_{ik}'|\rho^{-\frac{1}{2}}|\psi_{ik}'\rangle)^2}, \tag{18}$$

where $\rho = \sum_i^m p_i\rho_i$, $|\psi_{ik}'\rangle = \sqrt{p_i\lambda_{ik}}|\psi_{ik}\rangle$, and $\rho_i = \sum_{k=1}^{\mathrm{rank}(\rho_i)} \lambda_{ik}|\psi_{ik}\rangle\langle\psi_{ik}|$. We denote this lower bound

$$L_6 = 1 - \sqrt[4]{\sum_{i=1}^m \sum_{k=1}^{\mathrm{rank}(\rho_i)} (\langle\psi_{ik}'|\rho^{-\frac{1}{2}}|\psi_{ik}'\rangle)^2}. \tag{19}$$

III. A NEW LOWER BOUND AND EQUALITY CONDITIONS

In this section, we derive the new lower bound L_4 on the minimum-error discrimination between arbitrary m mixed quantum states, then we give a sufficient and necessary condition to achieve this bound.

The measures (e.g., various trace distances and fidelities) between quantum states are of importance in quantum information [28–30]. Here we first give three useful lemmas concerning the usual trace distance and fidelity. As indicated previously, in this paper, $F(\rho,\sigma) = \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$.

Lemma 4 [28]. Let ρ and σ be two quantum states. Then

$$2[1 - F(\rho,\sigma)] \leqslant \mathrm{Tr}|\rho - \sigma| \leqslant 2\sqrt{1 - F^2(\rho,\sigma)}. \tag{20}$$

Lemma 5 [19]. Let ρ and σ be two positive semidefinite operators. Then

$$\mathrm{Tr}(\rho) + \mathrm{Tr}(\sigma) - 2F(\rho,\sigma) \leqslant \mathrm{Tr}|\rho - \sigma| \leqslant \mathrm{Tr}(\rho) + \mathrm{Tr}(\sigma).$$

In addition, the second equality holds if and only if $\rho\perp\sigma$.

Definition 1. Let A be a self-adjoint matrix. Then the positive part is given by

$$A_+ = \sum_{\lambda_k>0} \lambda_k\Pi_k, \tag{21}$$

where $A = \sum_k \lambda_k\Pi_k$ is a spectral decomposition of A.

Lemma 6. Let E, ρ, and σ be three positive semidefinite matrices, with $E \leqslant I$. Then

$$\mathrm{Tr}[E(\rho - \sigma)] \leqslant \mathrm{Tr}(\rho - \sigma)_+, \tag{22}$$

with equality iff E is of the form

$$E = P^+ + P_2, \tag{23}$$

where P^+ is the projection onto the support of $(\rho - \sigma)_+$, and $0 \leqslant P_2 \leqslant I$ is supported on the kernel of $(\rho - \sigma)$.

Proof. It is obvious that

$$(\rho - \sigma) \leqslant (\rho - \sigma)_+. \tag{24}$$

It follows immediately by the positivity of E (or by Lemma 2 of Yuen-Kennedy-Lax [8]) that

$$\mathrm{Tr}E(\rho - \sigma) \leqslant \mathrm{Tr}E(\rho - \sigma)_+. \tag{25}$$

Since $E \leqslant I$, it similarly follows that

$$\mathrm{Tr}E(\rho - \sigma)_+ \leqslant \mathrm{Tr}(\rho - \sigma)_+, \tag{26}$$

proving (22). The equality condition is left as an exercise for the reader. ∎

The new bound is presented by the following theorem.

Theorem 7. For any m mixed quantum states ρ_1, $\rho_2,\ldots,\rho_m$ with the *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively, then the minimum-error probability Q_E satisfies

$$Q_E \geqslant L_4, \tag{27}$$

where L_4 is given by Eq. (13).

Proof. Let P_S denote the maximum probability and let $\mathbb{E}_m$ denote the class of all POVMs of the form $\{E_i : 1 \leqslant i \leqslant m\}$. Then we have that, for any $k \in \{1,2,\ldots,m\}$,

$$P_S = \max_{\{E_j\}\in\mathbb{E}_m} \sum_{j=1}^{m} \mathrm{Tr}(E_j p_j \rho_j) \tag{28}$$

$$= \max_{\{E_j\}\in\mathbb{E}_m} \left\{ p_k + \sum_{j\neq k} \mathrm{Tr}[E_j(p_j\rho_j - p_k\rho_k)] \right\} \tag{29}$$

$$\leqslant p_k + \sum_{j\neq k} \mathrm{Tr}(p_j\rho_j - p_k\rho_k)_+, \tag{30}$$

where inequality (30) holds by Lemma 6.

Consequently, we get

$$P_S \leqslant \min_{k=1,\ldots,m} \left\{ p_k + \sum_{j\neq k} \mathrm{Tr}(p_j\rho_j - p_k\rho_k)_+ \right\}. \tag{31}$$

Therefore, we conclude that inequality (27) holds by $Q_E = 1 - P_S$. ■

Remark 1. With Lemma 5, $\mathrm{Tr}|p_j\rho_j - p_i\rho_i| \leqslant p_i + p_j$, and the equality holds if and only if $\rho_j \perp \rho_i$. Therefore, in Theorem 7, the upper bound on the probability of correct detection between m mixed quantum states satisfies

$$p_{k_0} + \sum_{j\neq k} \mathrm{Tr}(p_j\rho_j - p_{k_0}\rho_{k_0})_+$$

$$= \frac{1}{2}\left[1 + \sum_{j\neq k_0} \mathrm{Tr}|p_j\rho_j - p_{k_0}\rho_{k_0}| - (m-2)p_{k_0} \right]$$

$$\leqslant \frac{1}{2}\left[1 + \sum_{j\neq k_0} (p_j + p_{k_0}) - (m-2)p_{k_0} \right] = 1. \tag{32}$$

By Lemma 5, we further see that this bound is strictly smaller than 1 usually, unless $\rho_1,\rho_2,\ldots,\rho_m$ are mutually orthogonal.

Remark 2. When $m = 2$, the lower bound in Theorem 7 is precisely $\frac{1}{2}(1 - \mathrm{Tr}|p_2\rho_2 - p_1\rho_1|)$, which is in accord with the well-known Helstrom limit [2]; and indeed, in this case, this bound can always be attained by choosing the optimum POVM: $E_2 = P_{12}^+$ and $E_1 = I - E_2$. Here P_{12}^+ denotes the projective operator onto the subspace spanned by the all eigenvectors corresponding to all positive eigenvalues of $p_2\rho_2 - p_1\rho_1$.

From the proof of Theorem 7, we can obtain a sufficient and necessary condition on the minimum-error probability Q_E attaining the lower bound L_4, which is described by the following theorem.

Theorem 8. Equality is attained in the bound (27) iff for some fixed k, the operators $\{(p_j\rho_j - p_k\rho_k)_+\}_{j\neq k}$ have mutually orthogonal supports.

Proof. Suppose that for some POVM $\{E_k\}$, we have the equality

$$\mathrm{Tr}\left(\sum_k E_k\rho_k\right) = \mathrm{Tr}\left(\rho_k + \sum_{j\neq k} E_j(\rho_j - \rho_k)\right) \tag{33}$$

$$\leqslant \mathrm{Tr}\left(\rho_k + \sum_{j\neq k} (\rho_j - \rho_k)_+\right). \tag{34}$$

Then by Lemma 5,

$$E_j \geqslant \Pi_+(\rho_j - \rho_k), \tag{35}$$

where $\Pi_+(\rho_j - \rho_k)$ is the positive projection onto the positive subspace of $\rho_j - \rho_k$. If the unit vector $|\psi\rangle$ is in the support of $(\rho_{j_0} - \rho_k)_+$, then one has

$$1 = ||\psi\rangle|^2 = \sum_j \langle\psi|E_j|\psi\rangle = 1 + \sum_{j\neq j_0} \langle\psi|E_j|\psi\rangle \geqslant 1. \tag{36}$$

It follows that $\langle\psi|E_j|\psi\rangle = 0$ for all $j \neq j_0$. In particular, the support of E_{j_0} is orthogonal to the supports of the other E_j.

Conversely, if the supports of the other $(\rho_j - \rho_k)_+$ are mutually orthogonal, then the middle term of (34) attains a maximum for the POVM:

$$E_j = \Pi_+(\rho_j - \rho_k), \quad j \neq k, \tag{37}$$

$$E_k = I - \sum_{j\neq k} E_j. \tag{38}$$

In this case, one has equality of all terms in (34). ■

Suppose that $\rho_1,\rho_2,\ldots,\rho_m$ are m mixed quantum states with *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively. The condition for the new bound L_4 being attained can also be presented as follows: there exists $p_{k_0}\rho_{k_0}$ such that $P_{k_0 i}^+ \perp P_{k_0 j}^+$ $(\forall i \neq j)$, where $P_{k_0 t}^+$ denotes the projective operator onto the subspace spanned by all eigenvectors corresponding to all positive eigenvalues of $p_t\rho_t - p_{k_0}\rho_{k_0}$. To make the result more accessible, we give a simple example to explain the condition for the bound's being attained.

For example, let $p_1 = p_2 = p_3 = \frac{1}{3}$, $0 < \gamma < \beta < \alpha < 1$, and $\rho_1 = \alpha|0\rangle\langle 0| + (1-\alpha)|1\rangle\langle 1|$, $\rho_2 = \beta|0\rangle\langle 0| + (1-\beta)|2\rangle\langle 2|$, $\rho_3 = \gamma|0\rangle\langle 0| + (1-\gamma)|3\rangle\langle 3|$. We have $(p_2\rho_2 - p_1\rho_1)_+ = \frac{(1-\beta)}{3}|2\rangle\langle 2|$ (i.e., $P_{12}^+ = |2\rangle\langle 2|$), and $(p_3\rho_3 - p_1\rho_1)_+ = \frac{(1-\gamma)}{3}|3\rangle\langle 3|$ (i.e., $P_{13}^+ = |3\rangle\langle 3|$), which have mutually orthogonal supports. So in this case, the new lower bound is attained. We get

$$L_4 = 1 - \min_{k=1,\ldots,m} \left\{ p_k + \sum_{j\neq k} \mathrm{Tr}(p_j\rho_j - p_k\rho_k)_+ \right\} \tag{39}$$

$$= 1 - \frac{\beta+\gamma}{3}. \tag{40}$$

That is, $Q_E = 1 - [(\beta+\gamma)/3]$.

IV. COMPARISONS BETWEEN DIFFERENT LOWER BOUNDS

In this section, we compare the seven different lower bounds $(L_i, i = 0,1,2,3,4,5,6)$ on the minimum-error probability for discriminating arbitrary m mixed quantum states with the *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively. Also, when discriminating two states, we consider their relation to the Helstrom limit.

First, concerning the relation between L_4 and L_2, we have the following result.

Theorem 9. For any m mixed quantum states $\rho_1,\rho_2,\ldots,\rho_m$ with the *a priori* probabilities $p_1,p_2,\ldots,p_m$, respectively, the two lower bounds L_2 and L_4 on the minimum-error probability for ambiguously discriminating these m states have the following relationship:

$$L_4 \geqslant L_2. \tag{41}$$

Proof. First from Eq. (13) it follows that L_4 is equivalent to

$$\frac{1}{2}\left[1-\min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\mathrm{Tr}|p_j\rho_j-p_k\rho_k|-(m-2)p_k\right\}\right], \tag{42}$$

and

$$L_2=\frac{1}{2}\left(1-\frac{1}{m-1}\sum_{1\leqslant i<j\leqslant m}\mathrm{Tr}|p_j\rho_j-p_i\rho_i|\right). \tag{43}$$

Let

$$\min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\mathrm{Tr}|p_j\rho_j-p_k\rho_k|-(m-2)p_k\right\} = \sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0} \tag{44}$$

for some $k_0\in\{1,2,\ldots,m\}$. Then L_4 equals

$$\frac{1}{2}\left\{1-\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right]\right\}. \tag{45}$$

Therefore,

$$2L_4-2L_2=\frac{1}{m-1}\sum_{1\leqslant i<j\leqslant m}\mathrm{Tr}|p_j\rho_j-p_i\rho_i| -\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right]. \tag{46}$$

Note that

$$\sum_{1\leqslant i<j\leqslant m}\mathrm{Tr}|p_j\rho_j-p_i\rho_i|=\frac{1}{2}\sum_{i=1}^{m}\sum_{j\neq i}\mathrm{Tr}|p_j\rho_j-p_i\rho_i| \tag{47}$$

and

$$\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0} =\frac{1}{m}\sum_{i=1}^{m}\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right].$$

By combining Eqs. (46) and (47) and the preceding equality, we have

$$2L_4-2L_2 =\frac{1}{2(m-1)}\sum_{i=1}^{m}\sum_{j\neq i}\mathrm{Tr}|p_j\rho_j-p_i\rho_i| -\frac{1}{m}\sum_{i=1}^{m}\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right].$$

Furthermore, the above equality can be equivalently written as follows:

$$\begin{aligned}2L_4-2L_2 &=\frac{1}{2(m-1)}\sum_{i=1}^{m}\left[\left(\sum_{j\neq i}\mathrm{Tr}|p_j\rho_j-p_i\rho_i|-(m-2)p_i\right) -\left(\sum_{j\neq k_0}^{m}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right)\right]\\ &\quad+\frac{m-2}{2(m-1)}-\left[\frac{1}{m}-\frac{1}{2(m-1)}\right]\\ &\quad\times\sum_{i=1}^{m}\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right].\end{aligned} \tag{48}$$

With Eq. (44) we know that, for any $i\in\{1,2,\ldots,m\}$,

$$\sum_{j\neq i}\mathrm{Tr}|p_j\rho_j-p_i\rho_i|-(m-2)p_i \geqslant\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}. \tag{49}$$

Note that $(1/m)-\{1/[2(m-1)]\}=(m-2)/2m(m-1)$. Therefore, with Eq. (48) we have

$$2L_4-2L_2\geqslant\frac{m-2}{2(m-1)}-\frac{m-2}{2m(m-1)}\sum_{i=1}^{m} \times\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right] \tag{50}$$

$$=\frac{m-2}{2(m-1)}-\frac{m-2}{2(m-1)} \times\left[\sum_{j\neq k_0}\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|-(m-2)p_{k_0}\right]. \tag{51}$$

With Lemma 5, we know that $\mathrm{Tr}|p_j\rho_j-p_{k_0}\rho_{k_0}|\leqslant p_j+p_{k_0}$. Therefore, according to the inequality (51), we further have

$$2L_4-2L_2\geqslant\frac{m-2}{2(m-1)}-\frac{m-2}{2(m-1)} \times\left[\sum_{j\neq k_0}(p_j+p_{k_0})-(m-2)p_{k_0}\right]=0. \tag{52}$$

Consequently, we conclude that inequality (41) holds and the proof is completed. ■

Indeed, $L_4 > L_2$ is also possible for discriminating some states. We give an example later in this section.

When $m = 2$, we have the following relations between L_2, L_3, L_4 and the Helstrom limit H.

Proposition 10. When $m = 2$,

$$L_4 = L_2 = H \geqslant L_3, \tag{53}$$

where H is the Helstrom limit [2]; that is, $H = \frac{1}{2}(1 - \mathrm{Tr}|p_1\rho_1 - p_2\rho_2|)$.

Here, we need another useful lemma.

Lemma 11. Let ρ_1 and ρ_2 be two mixed states, and $p_1 + p_2 \leqslant 1$ with $p_i \geqslant 0$, $i = 1,2$. Then

$$p_1 + p_2 - 2\sqrt{p_1p_2}F(\rho_1,\rho_2) \leqslant \mathrm{Tr}|p_1\rho_1 - p_2\rho_2| \tag{54}$$
$$\leqslant p_1 + p_2 - 2p_1p_2F^2(\rho_1,\rho_2). \tag{55}$$

Proof. Since $p_1\rho_1$ and $p_2\rho_2$ are positive semidefinite operators and $F(p_1\rho_1, p_2\rho_2) = \sqrt{p_1p_2}F(\rho_1,\rho_2)$, we can directly get the first inequality from Lemma 5.

Now we prove the second inequality. By Uhlmann's theorem [29,30], we let $|\psi_1\rangle$ and $|\psi_2\rangle$ be the purifications of ρ_1 and ρ_2, respectively, such that $F(\rho_1,\rho_2) = |\langle\psi_1|\psi_2\rangle|$. Since the trace distance is nonincreasing under the partial trace [28], we obtain

$$\mathrm{Tr}|p_1\rho_1 - p_2\rho_2| \leqslant \mathrm{Tr}|p_1|\psi_1\rangle\langle\psi_1| - p_2|\psi_2\rangle\langle\psi_2||. \tag{56}$$

Let $\{|\psi_1\rangle, |\psi_1^\perp\rangle\}$ be an orthonormal basis in the subspace spanned by $\{|\psi_1\rangle, |\psi_2\rangle\}$. Then $|\psi_2\rangle$ can be represented as $|\psi_2\rangle = \cos\theta|\psi_1\rangle + \sin\theta|\psi_1^\perp\rangle$. In addition, we have

$$\mathrm{Tr}|p_1|\psi_1\rangle\langle\psi_1| - p_2|\psi_2\rangle\langle\psi_2|| = \mathrm{Tr}\left|\begin{pmatrix} p_1 - p_2\cos^2\theta & -p_2\cos\theta\sin\theta \\ -p_2\cos\theta\sin\theta & -p_2\sin^2\theta \end{pmatrix}\right|. \tag{57}$$

We can calculate the eigenvalues of matrix (57) as

$$\frac{1}{2}\left[p_1 - p_2 \pm \sqrt{p_1^2 + p_2^2 - 2p_1p_2\cos(2\theta)}\right]. \tag{58}$$

Therefore, we have

$$\mathrm{Tr}\,|p_1|\psi_1\rangle\langle\psi_1| - p_2|\psi_2\rangle\langle\psi_2|| = \sqrt{p_1^2 + p_2^2 - 2p_1p_2\cos(2\theta)}. \tag{59}$$

Since

$$2p_1p_2F^2(\rho_1,\rho_2) = 2p_1p_2|\langle\psi_1|\psi_2\rangle|^2 = 2p_1p_2\cos^2\theta,$$

it suffices to show that

$$\sqrt{p_1^2 + p_2^2 - 2p_1p_2\cos(2\theta)} \leqslant p_1 + p_2 - 2p_1p_2\cos^2\theta.$$

That is,

$$p_1^2 + p_2^2 - 2p_1p_2\cos(2\theta) \leqslant (p_1 + p_2 - 2p_1p_2\cos^2\theta)^2,$$

and equivalently,

$$4p_1p_2\cos^2\theta[1 - (p_1 + p_2) + p_1p_2\cos^2\theta] \geqslant 0, \tag{60}$$

which is clearly true. Consequently, we complete the proof. ■

Proof of Proposition 10. It is easy to verify that, when $m = 2$, $L_1 = L_2 = \frac{1}{2}(1 - \mathrm{Tr}|p_1\rho_1 - p_2\rho_2|) = H$, and $L_3 = p_1p_2F^2(\rho_1,\rho_2)$. As a result, to prove inequality (53), we should show that $\frac{1}{2}(1 - \mathrm{Tr}|p_1\rho_1 - p_2\rho_2|) \geqslant p_1p_2F^2(\rho_1,\rho_2)$. Because $p_1 + p_2 = 1$, according to the second inequality in Lemma 11, we easily get the conclusion, and therefore, (53) holds. ■

Remark 3. From the proof of Lemma 11, we know that when $m = 2$, L_3 is smaller than the Helstrom limit unless the mixed states are mutually orthogonal.

Moreover, if we discriminate m equiprobable mixed states, that is, the m mixed states are chosen uniformly at random ($p_i = 1/m$, $i = 1,2,\ldots,m$), then L_3 and L_4 have the following relationship.

Proposition 12. If $p_i = 1/m$ $(i = 1,2,\ldots,m)$, then we have $L_4 \geqslant L_3$.

Proof. If $p_i = 1/m$ $(i = 1,2,\ldots,m)$, we have

$$L_3 = \frac{1}{m^2}\sum_{i<j}F^2(\rho_i,\rho_j), \tag{61}$$

and for any given $k_0 \in \{1,2,\ldots,m\}$, by Eq. (42) we have

$$\begin{aligned} L_4 &= \frac{1}{2}\left[1 - \min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\mathrm{Tr}|p_j\rho_j - p_k\rho_k| - (m-2)p_k\right\}\right] \\ &= \frac{1}{2}\left[\frac{2m-2}{m} - \frac{1}{m}\min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\mathrm{Tr}|\rho_j - \rho_k|\right\}\right] \\ &\geqslant \frac{1}{2}\left[\frac{2m-2}{m} - \frac{1}{m}\sum_{j\neq k_0}\mathrm{Tr}|\rho_j - \rho_{k_0}|\right] \qquad (62) \\ &\geqslant \frac{1}{2}\left[\frac{2m-2}{m} - \frac{2}{m}\sum_{j\neq k_0}\sqrt{1 - F^2(\rho_j,\rho_{k_0})}\right], \qquad (63) \end{aligned}$$

where the last inequality holds by Lemma 4. Thus, we get

$$L_4 \geqslant \frac{1}{2}\left[\frac{2m-2}{m} - \frac{2}{m}\min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\sqrt{1 - F^2(\rho_j,\rho_k)}\right\}\right].$$

Therefore, we have

$$\begin{aligned} 2m^2(L_4 - L_3) &\geqslant 2m^2 - 2m - 2m\min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\sqrt{1 - F^2(\rho_j,\rho_k)}\right\} \\ &\quad - 2\sum_{i<j}F^2(\rho_i,\rho_j) \qquad (64) \\ &= 2m^2 - 2m - 2\sum_{i=1}^{m}\min_{k=1,\ldots,m}\left\{\sum_{j\neq k}\sqrt{1 - F^2(\rho_j,\rho_k)}\right\} \\ &\quad - \sum_{i=1}^{m}\sum_{j\neq i}F^2(\rho_i,\rho_j) \qquad (65) \end{aligned}$$

$$\geqslant 2m^2 - 2m - 2\sum_{i=1}^{m}\sum_{j\neq i}\sqrt{1-F^2(\rho_j,\rho_i)} - \sum_{i=1}^{m}\sum_{j\neq i}F^2(\rho_i,\rho_j) \quad (66)$$

$$= \sum_{i=1}^{m}\sum_{j\neq i}\left(\sqrt{1-F^2(\rho_j,\rho_i)}-1\right)^2 \quad (67)$$

$$\geqslant 0. \quad (68)$$

Thus, we have $L_4 \geqslant L_3$. We complete the proof. ■

Furthermore, even if the prior probabilities are not equal, under some restricted conditions, L_2, L_3, and L_4 also have certain relationships. We present a sufficient condition as follows.

Proposition 13. Let $a_i = \sum_{j\neq i} p_i p_j F^2(\rho_i,\rho_j)$. Then L_2, L_3, and L_4 have the following relationship: for any $m \geqslant 2$,

$$L_2 \geqslant \frac{1}{m-1}L_3, \quad (69)$$

and when $\max_{i=1,\ldots,m}\{a_i\} \geqslant \frac{1}{2}\sum_{i=1}^{m} a_i$, we have

$$L_4 \geqslant L_3. \quad (70)$$

Proof. By Lemma 11, we have

$$L_2 = \frac{1}{2}\left(1 - \frac{1}{m-1}\sum_{1\leqslant i<j\leqslant m}\mathrm{Tr}|p_j\rho_j - p_i\rho_i|\right) \quad (71)$$

$$\geqslant \frac{1}{2}\left\{1 - \frac{1}{m-1}\sum_{1\leqslant i<j\leqslant m}\left[p_i+p_j-2p_ip_jF^2(\rho_i,\rho_j)\right]\right\} \quad (72)$$

$$= \frac{1}{m-1}L_3. \quad (73)$$

For any given $k_0 = 1,\ldots,m$, by Eq. (42) we have

$$L_4 \geqslant \frac{1}{2}\left\{1 - \left[\sum_{j\neq k_0}\mathrm{Tr}\left|p_j\rho_j - p_{k_0}\rho_{k_0}\right| - (m-2)p_{k_0}\right]\right\} \quad (74)$$

$$= \frac{1}{2} - \frac{1}{2}\sum_{j\neq k_0}\mathrm{Tr}\left|p_j\rho_j - p_{k_0}\rho_{k_0}\right| + \frac{m-2}{2}p_{k_0} \quad (75)$$

$$\geqslant \frac{1}{2} - \frac{1}{2}\sum_{j\neq k_0}\left[p_{k_0} + p_j - 2p_{k_0}p_jF^2\left(\rho_{k_0},\rho_j\right)\right] + \frac{m-2}{2}p_{k_0} \quad (76)$$

$$= \sum_{j\neq k_0} p_{k_0}p_jF^2\left(\rho_{k_0},\rho_j\right). \quad (77)$$

So we have

$$L_4 \geqslant \max_{k=1,\ldots,m}\left\{\sum_{j\neq k}p_kp_jF^2(\rho_k,\rho_j)\right\}. \quad (78)$$

Moreover, we have

$$L_3 = \sum_{1\leqslant i<j\leqslant m} p_ip_jF^2(\rho_i,\rho_j) \quad (79)$$

$$= \frac{1}{2}\sum_{i=1}^{m}\sum_{j\neq i}p_ip_jF^2(\rho_i,\rho_j). \quad (80)$$

Let $a_i = \sum_{j\neq i} p_ip_jF^2(\rho_i,\rho_j)$. Then we get

$$L_4 - L_3 \geqslant \max_{i=1,\ldots,m}\{a_i\} - \frac{1}{2}\sum_{i=1}^{m}a_i. \quad (81)$$

If $\max_{i=1,\ldots,m}\{a_i\} - \frac{1}{2}\sum_{i=1}^{m}a_i \geqslant 0$, then $L_4 \geqslant L_3$. We complete the proof. ■

Although the bound L_5 is tight within a factor of 2, for some cases, the new bound is tighter than L_5 and becomes the tightest one in the seven bounds, which is equal to the minimum-error probability. We give an example as follows.

Example 1. Let $p_1 = p_2 = p_3 = \frac{1}{3}$, and $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, $\rho_2 = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|2\rangle\langle 2|$, $\rho_3 = \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|3\rangle\langle 3|$. Then we can work out the seven lower bounds directly, as $L_0 = 0$, $L_1 = 0$, $L_2 = \frac{5}{36}$, $L_3 = \frac{1}{24}$, $L_4 = \frac{7}{36}$, $L_5 = \frac{13-\sqrt{61}}{36}$, and $L_6 = 1 - 4\sqrt{\frac{10}{13}}$. Hence, $L_4 > L_5 > L_2 > L_6 > L_3 > L_1 = L_0$. Indeed, in this example, the operators $(p_2\rho_2 - p_1\rho_1)_+$ and $(p_3\rho_3 - p_1\rho_1)_+$ have mutually orthogonal supports. So the minimum-error probability $Q_E = L_4 = \frac{7}{36}$.

However, even under the same condition when the new bound is tight, there exist examples to show that the new bound is not strictly better than other bounds.

Example 2. Let $p_1 = p_2 = p_3 = \frac{1}{3}$, and $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, $\rho_2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|$, $\rho_3 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|3\rangle\langle 3|$. We get $L_4 = \frac{1}{3}$. In this example, the operators $(p_2\rho_2 - p_1\rho_1)_+ = \frac{1}{6}|1\rangle\langle 1|$ and $(p_3\rho_3 - p_1\rho_1)_+ = \frac{1}{6}|3\rangle\langle 3|$ have mutually orthogonal supports. So according to Theorem 8, the new bound is tight (i.e., the minimum-error probability $Q_E = L_4 = \frac{1}{3}$). Also, we can get $L_1 = \frac{1}{3} = L_4$. That is, even in the condition when the new bound is tight, the new bound is as good as L_1 but not strictly better than existing bounds.

Therefore, in the light of these two examples, we conclude that, even under the condition when the new bound is tight, different examples show that $L_4 > L_1$ and $L_4 = L_1$ hold, respectively.

To sum up, when $m = 2$, we have $L_4 = L_2 = H \geqslant L_3$ ($\geqslant$ can be strict for some states), and for any m states, $L_4 \geqslant L_2$ always holds ($\geqslant$ can be strict for some states). For the equiprobable case (the prior probabilities are equivalent), $L_4 \geqslant L_3$ always holds. In some cases, the new bound L_4 is the tightest one in the seven bounds.

V. CONCLUDING REMARKS

Quantum-state discrimination is an intriguing issue in quantum information processing [1–7]. In this paper, we have reviewed a number of lower bounds on the minimum-error probability for ambiguous discrimination between arbitrary m quantum mixed states. In particular, we have derived a new lower bound on the minimum-error probability and presented a sufficient and necessary condition for achieving this bound.

Also, we have proved that our bound improves the previous one obtained in [19], and in the equiprobable case, the new bound also improves the one derived in [20]. In addition, we have compared the new bound with six of the previous bounds, by a series of propositions and examples.

From Examples IV and IV, we know that, under the same condition when the new bound L_4 is tight, different examples show the possibility of $L_4 > L_1$ and $L_4 = L_1$. Thus a natural question is whether or not there exists a condition such that the new bound L_4 is always strictly better than the six other bounds. A further problem worthy of consideration is how to calculate the minimum-error probability for ambiguous discrimination between arbitrary m quantum mixed states with the prior probabilities, respectively, and devise an optimum measurement correspondingly. In particular, we would consider the appropriate application of these bounds presented in this paper in quantum communication [21]. Indeed, it is worth mentioning that quantum-state discrimination has already been applied to quantum encoding [31].

ACKNOWLEDGMENTS

The authors are grateful to the referee for invaluable suggestions that helped us improve the quality of the paper. This work was supported in part by the National Natural Science Foundation (Grants No. 60573006 and No. 60873055), the Research Foundation for the Doctoral Program of Higher School of Ministry of Education (Grant No. 20050558015), the Program for New Century Excellent Talents in University (NCET) of China, and a project of the SQIG at IT, funded by FCT and EU FEDER Project Nos. Quantlog POCI/MAT/55796/2004 and QSec PTDC/EIA/67661/2006, IT Project QuantTel, NoE Euro-NF, and the SQIG LAP initiative.

[1] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[3] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[4] J. A. Bergou, U. Herzog, and M. Hillery, *Quantum State Estimation*, Lecture Notes in Physics, Vol. 649 (Springer, Berlin, 2004), p. 417.
[5] A. Chefles, *Quantum State Estimation*, Lecture Notes in Physics, Vol. 649 (Springer, Berlin, 2004), p. 467.
[6] S. M. Barnett and S. Croke, Adv. Opt. Photonics **1**, 238 (2009).
[7] A. S. Holevo, J. Multivar. Anal. **3**, 337 (1973).
[8] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **21**, 125 (1975).
[9] S. M. Barnett and E. Riis, J. Mod. Opt. **44**, 1061 (1997).
[10] R. B. M. Clarke, V. M. Kendon, A. Chefles, S. M. Barnett, E. Riis, and M. Sasaki, Phys. Rev. A **64**, 012303 (2001).
[11] M. Mohseni, A. M. Steinberg, and J. A. Bergou, Phys. Rev. Lett. **93**, 200403 (2004).
[12] M. Osaki, M. Ban, and O. Hirota, Phys. Rev. A **54**, 1691 (1996).
[13] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[14] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theory **50**, 1198 (2004).
[15] S. M. Barnett, Phys. Rev. A **64**, 030303(R) (2001).
[16] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter, Phys. Rev. A **65**, 052308 (2002).
[17] C.-L. Chou and L. Y. Hsu, Phys. Rev. A **68**, 042305 (2003).
[18] M. Hayashi, A. Kawachi, and H. Kobayashi, Quantum Inf. Comput. **8**, 0345 (2008).
[19] D. W. Qiu, Phys. Rev. A **77**, 012328 (2008).
[20] A. Montanaro, *IEEE Information Theory Workshop, ITW'08* (IEEE, Piscataway, NJ, 2008), p. 378.
[21] A. Nayak and J. Salzman, J. ACM **53**, 184 (2006).
[22] A. Montanaro, Commun. Math. Phys. **273**, 619 (2007).
[23] J. Tyson, J. Math. Phys. **50**, 032106 (2009); e-print arXiv:0907.3386; T. Ogawa and H. Nagaoka, IEEE Trans. Inf. Theory **45**, 2486 (1999).
[24] W. Hwang and J. Bae, e-print arXiv:0909.1149v2.
[25] H. Barnum and E. Knill, J. Math. Phys. **43**, 2097 (2002).
[26] P. Hayden, D. Leung, and G. Smith, Phys. Rev. A **71**, 062339 (2005).
[27] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1986).
[28] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[29] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[30] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[31] N. Elron and Y. C. Eldar, IEEE Trans. Inf. Theory **53**, 1900 (2007).