Unambiguous discrimination between quantum mixed states

Yuan Feng,[1,*] Runyao Duan,[1,†] and Mingsheng Ying[1,‡]

[1] *State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology Tsinghua University, Beijing, China, 100084*

(Dated: March 27, 2014)

We prove that the states secretly chosen from a mixed state set can be perfectly discriminated if and only if these states are orthogonal. The sufficient and necessary condition when nonorthogonal quantum mixed states can be unambiguously discriminated is also presented. Furthermore, we derive a series of lower bounds on the inconclusive probability of unambiguous discrimination of states from a mixed state set with *a prior* probabilities.

PACS numbers: 03.67.-a,03.67.Mn,03.65.Ud

Quantum state discrimination is an essential problem in quantum information theory. Perfect discrimination among nonorthogonal pure states is, however, forbidden by the laws of quantum mechanics. Nonetheless, if a non-zero probability of inconclusive answer is allowed, one can distinguish with certainty linearly independent pure states. This strategy is usually called *unambiguous discrimination*. Unambiguous discrimination among two equally probable nonorthogonal quantum pure states was originally addressed by Ivanovic [1], and then Dieks [2] and Peres [3]. Jaeger and Shimony [4] extended their result to the case of two nonorthogonal pure states with unequal priori probabilities. Chefles [5] showed that n quantum pure states can be unambiguously discriminated if and only if they are linearly independent. For the general case of unambiguous discrimination between n pure states with *a prior* probabilities, it was shown in [6] and [7] that the problem of optimal discrimination, in the sense that the success probability is maximized, or equivalently, the inconclusive probability is minimized, can be reduced to a semidefinite programming (SDP) problem, which has only numerical solution in mathematics. On the other hand, Zhang *et al* [8] and Feng *et al* [9] derived two lower bounds on the inconclusive probability of unambiguous discrimination among n pure states.

Somewhat surprisingly, it is only recently that the problem of unambiguous discrimination between mixed states is considered. In Ref. [10], the optimal unambiguous discrimination between a pure state and a mixed state with rank 2 was examined. Rudolph *et al* [11] derived a lower bound and an upper bound on the maximal probability of successful discrimination of two mixed states. Raynal *et al* [12] presented two reduction theorems to reduce the optimal unambiguous discrimination of two mixed states to that of other two mixed states which have the same rank. In the general case of n mixed state discrimination, Fiurasek and Jezek [13] and Eldar [14] gave some sufficient and necessary conditions on the optimal unambiguous discrimination and some numerical methods were discussed.

In this paper, we consider first the distinguishability of any mixed state set. We prove that any state chosen from a mixed state set can be perfectly discriminated if and only if the set are orthogonal, in the sense that any state in the set has support orthogonal to those of the others. For the case of nonorthogonal mixed state set, the sufficient and necessary condition of when states from it can be unambiguously discriminated is that any state in the set has the support space not totally included in the supports of the others. Furthermore, we consider the problem of discriminating unambiguously of n mixed states with *a prior* probabilities and present a series lower bounds on the inconclusive probability.

Suppose a quantum system is prepared in a state secretly drawn from a known set $\rho_1, \dots, \rho_n$, where each ρ_i is a mixed state in the Hilbert space $\mathcal{H}$. The task of discrimination is to obtain as much information about the identification of the state as possible. In what follows, by perfect discrimination we mean that one can always get the correct answer while by unambiguous discrimination we mean that except a maybe nonzero inconclusive probability, one can identify the state without error. It is obvious that perfect discrimination is necessarily an unambiguous one, but the reverse is not true in general. To unambiguously discriminate $\rho_1, \dots, \rho_n$, one can construct a most general positive-operator valued measurement (POVM) comprising $n+1$ elements $\Pi_0, \Pi_1, \dots, \Pi_n$ such that

$$\Pi_i \geq 0, \quad i = 0, 1, \dots, n$$

$$\sum_{i=0}^{n} \Pi_i = I \tag{1}$$

where I denotes the identity matrix in $\mathcal{H}$. Each POVM element Π_i, $i = 1, \dots, n$ corresponds to identification of the corresponding state ρ_i, while Π_0 corresponds to the inconclusive answer. For the sake of simplicity, we often specify only $\Pi_1, \dots, \Pi_n$ for a POVM since the left element Π_0 is uniquely determined by $\Pi_0 = I - \sum_{i=1}^n \Pi_i$. It is then straightforward that a POVM $\Pi_1, \dots, \Pi_n$, $\sum_{i=1}^n \Pi_i \leq I$, can perfectly discriminate $\rho_1, \dots, \rho_n$ if and only if

$$\mathrm{Tr}(\rho_i \Pi_j) = \delta_{ij}$$

*Electronic address: fengy99g@mails.tsinghua.edu.cn
†Electronic address: dry02@mails.tsinghua.edu.cn
‡Electronic address: yingmsh@tsinghua.edu.cn

while can unambiguously discriminate $\rho_1, \ldots, \rho_n$ if and only if

$$\mathrm{Tr}(\rho_i \Pi_j) = p_i \delta_{ij}$$

for some $p_i > 0$, where $i, j = 1, \ldots, n$.

Since the intersection of the kernels of all ρ_i, $i = 1, \ldots, n$, is not useful for the purpose of unambiguous discrimination, sometimes we can assume without loss of generality that each Π_i, $i = 1, \ldots, n$, is in $\mathrm{supp}(\rho_1, \ldots, \rho_n)$. Here $\mathrm{supp}(\rho_1, \ldots, \rho_n)$ is defined by the Hilbert space spanned by eigenvectors of the matrices $\rho_1, \ldots, \rho_n$ with nonzero corresponding eigenvalues.

The following lemma is a necessary condition of a POVM to unambiguously discriminate a given mixed state set.

Lemma 1 *Suppose $\Pi_1, \ldots, \Pi_n$ are POVM elements and $\sum_i \Pi_i \leq I$. If for any i, Π_i can unambiguously discriminate ρ_i, then $\Pi_j \rho_i = 0$ for any $i \neq j$.*

Proof. Suppose for any i, Π_i can unambiguously discriminate ρ_i, then we have $\mathrm{Tr}(\Pi_j \rho_i) = p_i \delta_{ij}$ for some $p_i > 0$. Let

$$\rho_i = \sum_{k=1}^{n_i} r_i^k |\psi_i^k\rangle\langle\psi_i^k| \tag{2}$$

for some $r_i^k > 0$ be the spectrum decomposition of ρ_i, then for any $i \neq j$

$$0 = \mathrm{Tr}(\Pi_j \rho_i) = \sum_{k=1}^{n_i} r_i^k \langle\psi_i^k|\Pi_j|\psi_i^k\rangle \tag{3}$$

and $\langle\psi_i^k|\Pi_j|\psi_i^k\rangle = 0$ for $k = 1, \ldots, n_i$ from the fact $r_i^k > 0$. That implies $\Pi_j|\psi_i^k\rangle = 0$ and so $\Pi_j \rho_i = 0$. ■

It is well known that perfect pure state discrimination is possible if and only if the states to be discriminated are orthogonal to each other. In the case of mixed state, we have a similar result as the following theorem.

Theorem 1 *The quantum mixed states $\rho_1, \rho_2, \ldots, \rho_n$ can be perfectly discriminated if and only if they are orthogonal, that is, $\rho_i \rho_j = \delta_{ij} \rho_i^2$.*

Proof. If $\rho_i \rho_j = \delta_{ij} \rho_i^2$, then $\mathrm{supp}(\rho_i) \perp \mathrm{supp}(\rho_j)$ for any $i \neq j$. We choose Π_i as the projector onto $\mathrm{supp}(\rho_i)$. Obviously $\sum_i \Pi_i = I_s$ and $\mathrm{Tr}(\Pi_i \rho_j) = \delta_{ij}$, where I_s is the identity matrix in $\mathrm{supp}(\rho_1, \ldots, \rho_n)$. That indicates $\Pi_1, \ldots, \Pi_n$ can perfectly discriminate $\rho_1, \ldots, \rho_n$.

Conversely, if $\rho_1, \rho_2, \ldots, \rho_n$ can be discriminated perfectly, then there exist POVM elements $\Pi_1, \ldots, \Pi_n$, $\sum_k \Pi_k = I$, such that for any $i = 1, \ldots, n$, Π_i can perfectly (so unambiguously) discriminate ρ_i. From Lemma 1, we have $\Pi_j \rho_i = 0$ for any $i \neq j$. So $\rho_i \rho_j = \rho_i (\sum_k \Pi_k) \rho_j = \delta_{ij} \rho_i^2$. ■

The above theorem gives us a sufficient and necessary condition when mixed states can be discriminated perfectly. That is, they must be orthogonal to each other. In the case when the states are nonorthogonal, a strategy is, as in pure state situation, unambiguous discrimination. While a set of pure states can be unambiguously discriminated if and only if they are linearly independent [5], the unambiguous discrimination between mixed states has a stronger requirement, as the following theorem indicates.

Theorem 2 *The quantum mixed states $\rho_1, \ldots, \rho_n$ can be unambiguously discriminated if and only if for any $i = 1, \ldots, n$, $\mathrm{supp}(S) \neq \mathrm{supp}(S_i)$, where $S = \{\rho_1, \ldots, \rho_n\}$ and $S_i = S \backslash \{\rho_i\}$.*

Proof. "$\Longrightarrow$". Suppose $\rho_1, \ldots, \rho_n$ can be unambiguously discriminated, then there exist POVM elements $\Pi_1, \ldots, \Pi_n$ such that $\sum_i \Pi_i \leq I$ and $\mathrm{Tr}(\Pi_i \rho_j) = p_i \delta_{ij}$ for some $p_i > 0$. Let $|\psi_i^k\rangle, k = 1, \ldots, n_i$, be the eigenvectors of ρ_i with the corresponding eigenvalues larger than 0. Then there exists $1 \leq h_i \leq n_i$ such that $\langle\psi_i^{h_i}|\Pi_i|\psi_i^{h_i}\rangle > 0$ and from Lemma 1, for any $1 \leq j \leq n_i$, $\langle\psi_i^j|\Pi_k|\psi_i^j\rangle = 0$ provided that $i \neq k$.

In what follows, we prove that for any $i = 1, \ldots, n$, $|\psi_i^{h_i}\rangle$ cannot be written as a linear combination of the states $|\psi_k^j\rangle$ for $k \neq i$ and $j = 1, \ldots, n_k$, that will imply the result $\mathrm{supp}(S_i) \neq \mathrm{supp}(S)$. Suppose

$$|\psi_i^{h_i}\rangle = \sum_{k \neq i, j} a_{k,j}^i |\psi_k^j\rangle$$

for some $a_{k,j}^i$, then

$$\Pi_i |\psi_i^{h_i}\rangle = \sum_{k \neq i, j} a_{k,j}^i \Pi_i |\psi_k^j\rangle = 0, \tag{4}$$

which contradicts with $\langle\psi_i^{h_i}|\Pi_i|\psi_i^{h_i}\rangle > 0$.

"$\Longleftarrow$". Suppose $\mathrm{supp}(S) \neq \mathrm{supp}(S_i)$, then $\mathrm{supp}(\rho_i) \not\subseteq \mathrm{supp}(S_i)$. It follows that there exists a state $|\phi_i\rangle$ such that $|\phi_i\rangle \not\perp \mathrm{supp}(\rho_i)$ but $|\phi_i\rangle \perp \mathrm{supp}(S_i)$. That is $\langle\phi_i|\rho_i|\phi_i\rangle > 0$ but $\langle\phi_i|\rho_k|\phi_i\rangle = 0$ for any $k \neq i$. Let $\Pi_i = q_i|\phi_i\rangle\langle\phi_i|$, where q_i is sufficient small but positive such that $\sum_{i=1}^n \Pi_i \leq I$, we can check easily that the POVM elements $\Pi_1, \ldots, \Pi_n$ can unambiguously discriminate ρ_i with a positive probability $p_i = q_i \langle\phi_i|\rho_i|\phi_i\rangle > 0$ for any $i = 1, \ldots, n$. ■

When $\rho_1, \ldots, \rho_n$ are all pure states, the requirement of them to be unambiguously distinguishable presented in the above theorem is exactly that they should be linearly independent, just as we all know. This is because if $\rho_i = |\psi_i\rangle\langle\psi_i|$ for some state $|\psi_i\rangle$ then $\mathrm{supp}(S) \neq \mathrm{supp}(S_i)$ for any i if and only if $|\psi_1\rangle, \ldots, |\psi_n\rangle$ are linearly independent.

In general, however, the requirement of $\rho_1, \ldots, \rho_n$ to be unambiguously distinguishable is more strict than just linear independence. To see this, for any $i = 1, \ldots, n$, suppose $\mathrm{supp}(S) \neq \mathrm{supp}(S_i)$, we show ρ_i cannot be written as a linear combination of ρ_j, where $j \neq i$. In fact, if $\rho_i = \sum_{j \neq i} a_j^i \rho_j$ for some a_j^i, let $|\phi_i\rangle$ be a state orthogonal to $\mathrm{supp}(S_i)$ but not orthogonal to $\mathrm{supp}(\rho_i)$, then

$$0 < \langle\phi_i|\rho_i|\phi_i\rangle = \sum_{j \neq i} a_i^j \langle\phi_i|\rho_j|\phi_i\rangle = 0.$$

This contradiction indicates that $\rho_1,\ldots,\rho_n$ are linearly independent. The converse, however, does not necessarily hold. That is, the linear independence of $\rho_1,\ldots,\rho_n$ cannot guarantee that $\mathrm{supp}(S)\neq\mathrm{supp}(S_i)$. To see this, let us give a simple example. Suppose ρ_1 and ρ_2 are two different density matrices with rank m in an m-dimensional Hilbert space. It is obvious that ρ_1 and ρ_2 are linearly independent but $\mathrm{supp}(\rho_1)=\mathrm{supp}(\rho_2)=\mathrm{supp}(\rho_1,\rho_2)$. So in general the linear independence of certain mixed states cannot ensure the existence of a POVM to unambiguously discriminate between them.

We now turn to consider the problem of unambiguously discriminating between n quantum mixed states with a prior probabilities. The aim is to optimize the discrimination by choosing appropriate measurements to maximize the success probability, or equivalently, minimize the inconclusive probability. For the general case of unambiguous discrimination between n pure states, the optimization problem can be reduced to a semidefinite problem [6], which has no analytic solution. So the bound on the success (or inconclusive) probability for any unambiguous discrimination process becomes very important. A lot of works such as Ref. [8] and Ref. [9] dedicate to this field. In the following, we derive a lower bound on the inconclusive probability of unambiguous discrimination between n mixed states using a method similar to that in Ref. [9].

Theorem 3 *Suppose a quantum system is prepared in one of the n mixed states $\rho_1,\ldots,\rho_n$ with a prior probabilities $\eta_1,\ldots,\eta_n$. Then a lower bound on the inconclusive probability P_0 of unambiguous discrimination between these states is*

$$P_0 \geq \sqrt{\frac{n}{n-1}\sum_{i\neq j}\eta_i\eta_j F(\rho_i,\rho_j)^2}$$

where $F(\rho_i,\rho_j)$ is the fidelity of ρ_i and ρ_j.

Proof. For any POVM elements $\Pi_1,\ldots,\Pi_n$, $\sum_i \Pi_i\leq I$, which can unambiguously discriminate $\rho_1,\ldots,\rho_n$, we have $\mathrm{Tr}(\Pi_i\rho_j)=p_i\delta_{ij}$ for $i,j=1,\ldots,n$. Define $\Pi_0=I-\sum_{i=1}^n\Pi_i\geq 0$, then $P_0=\sum_i\eta_i\mathrm{Tr}(\Pi_0\rho_i)$. So

$$P_0^2=\sum_i\eta_i^2(\mathrm{Tr}(\Pi_0\rho_i))^2+\sum_{i\neq j}\eta_i\eta_j\mathrm{Tr}(\Pi_0\rho_i)\mathrm{Tr}(\Pi_0\rho_j). \tag{5}$$

By Cauchy inequality, we have

$$\sum_i\eta_i^2(\mathrm{Tr}(\Pi_0\rho_i))^2\geq\frac{1}{n-1}\sum_{i\neq j}\eta_i\eta_j\mathrm{Tr}(\Pi_0\rho_i)\mathrm{Tr}(\Pi_0\rho_j). \tag{6}$$

Substituting Eq.(6) into Eq.(5) we have

$$P_0^2\geq\frac{n}{n-1}\sum_{i\neq j}\eta_i\eta_j\mathrm{Tr}(\Pi_0\rho_i)\mathrm{Tr}(\Pi_0\rho_j). \tag{7}$$

Furthermore, using Cauchy inequality again, we have

$$\begin{aligned}
&\mathrm{Tr}(\Pi_0\rho_i)\mathrm{Tr}(\Pi_0\rho_j)\\
&=\mathrm{Tr}(U\sqrt{\rho_i}\sqrt{\Pi_0}\sqrt{\Pi_0}\sqrt{\rho_i}U^\dagger)\mathrm{Tr}(\sqrt{\rho_j}\sqrt{\Pi_0}\sqrt{\Pi_0}\sqrt{\rho_j})\\
&\geq(\mathrm{Tr}(U\sqrt{\rho_i}\Pi_0\sqrt{\rho_j}))^2\\
&=(\mathrm{Tr}(U\sqrt{\rho_i}(I-\textstyle\sum_{k=1}^n\Pi_k)\sqrt{\rho_j}))^2
\end{aligned} \tag{8}$$

for any unitary matrix U. From Lemma 1, we have $\sqrt{\rho_i}\Pi_k\sqrt{\rho_j}=0$ for any $i\neq j$ and $k=1,\ldots,n$. Notice also that

$$F(\rho_i,\rho_j)=\max_U\mathrm{Tr}(U\sqrt{\rho_i}\sqrt{\rho_j})$$

where the maximum is taken over all unitary matrix U. It follows that for any $i\neq j$,

$$\mathrm{Tr}(\Pi_0\rho_i)\mathrm{Tr}(\Pi_0\rho_j)\geq F(\rho_i,\rho_j)^2 \tag{9}$$

Taking Eq.(9) back into Eq.(7) we derive the lower bound on P_0 as

$$P_0\geq\sqrt{\frac{n}{n-1}\sum_{i\neq j}\eta_i\eta_j F(\rho_i,\rho_j)^2}. \tag{10}$$

That completes the proof of this theorem. ■

When $n=2$, the lower bound we presented above reduces to $P_0\geq 2\sqrt{\eta_1\eta_2}F(\rho_1,\rho_2)$, which partially coincides with the bound given in [11]. On the other hand, when $\rho_1,\ldots,\rho_n$ are all pure states, then the lower bound reduces to the one derived in Ref. [9].

What we would like to point out here is that from the proof of the above theorem, we can derive a series of lower bounds on the inconclusive probability. In fact, if let

$$A_k=\sum_i\eta_i^{2k}(\mathrm{Tr}(\Pi_0\rho_i))^{2k}$$

and

$$B_k=\sum_{i\neq j}\eta_i^k\eta_j^k(\mathrm{Tr}(\Pi_0\rho_i))^k(\mathrm{Tr}(\Pi_0\rho_j))^k$$

then by Cauchy inequality, we have $A_k\geq B_k/(n-1)$. Using these notations, the key steps Eq.(5)-(7) in the proof of the above theorem can be reexpressed as

$$P_0^2=A_1+B_1\geq\frac{n}{n-1}B_1 \tag{11}$$

which implies the lower bound

$$P_0\geq P_0^{(1)}\doteq\sqrt{\frac{n}{n-1}C_1} \tag{12}$$

as in Eq.(10), where C_k is defined by

$$C_k=\sum_{i\neq j}\eta_i^k\eta_j^k F(\rho_i,\rho_j)^{2k}$$

Now, if we notice the fact that $A_k^2 = A_{2k} + B_{2k}$, then we can first consider the term A_1 and derive that $A_1 = \sqrt{A_2 + B_2}$, so we can rewrite Eq.(11) as

$$P_0^2 = \sqrt{A_2 + B_2} + B_1 \geq \sqrt{\frac{n}{n-1} B_2} + B_1.$$

which implies another lower bound

$$P_0 \geq P_0^{(2)} \doteq \sqrt{C_1 + \sqrt{\frac{n}{n-1} C_2}}. \quad (13)$$

One can easily prove that the bound presented in Eq.(13) is better than that in Eq.(12) by Cauchy inequality.

Similarly, we can derive a series of lower bounds on the inconclusive probability of unambiguous discrimination between n mixed states as follows

$$P_0 \geq P_0^{(k)} \doteq \sqrt{C_1 + \sqrt{\ldots + \sqrt{\frac{n}{n-1} C_k}}}. \quad (14)$$

We can also prove that $P_0^{(1)} \leq P_0^{(2)} \leq \ldots$, that means when k increases, the lower bounds become better and better in the sense that they are closer and closer to the real optimal inconclusive probability. On the other hand, since the increasing sequence $\{P_0^{(k)}, k = 1, 2, \ldots\}$ has an upper bound 1, they definitely converge at a limit $P_0^{(\infty)}$, which is the best lower bound we can derive using this method.

To summarize, we prove that any state chosen from a mixed state set can be perfectly discriminated if and only if the set are orthogonal. For the case of nonorthogonal mixed state set, the sufficient and necessary condition of when states from it can be unambiguously discriminated is that any state in the set has the support space not totally included in the supports of the others. We consider also the problem of discriminating unambiguously of n mixed states with *a prior* probabilities and present a series of lower bounds on the inconclusive probability.

Acknowledgement: The authors thank S. Y. Zhang for useful discussion in this field. In pure state case, he pointed out a result similar to the series of lower bounds presented in this paper. This work was supported by National Foundation of Natural Sciences of China (Grant No: 60273003), National Key Project for Fundamental Research of China (Grant No: 1998030905).

[1] I.D. Ivanovic, Phys. Lett. A 123, 257 (1987).
[2] D. Dieks, Phys. Lett. A 126, 303 (1988).
[3] A. Peres, Phys. Lett. A 128, 19 (1988).
[4] G. Jaeger, A. Shimony, Phys. Lett. A 197, 83(1995).
[5] A. Chefles, Phys. Lett. A 239, 339(1998).
[6] X. M. Sun, S. Y. Zhang, Y. Feng, M. S. Ying, Phys. Rev. A 65, 044306(2002).
[7] Y. C. Eldar, IEEE Trans. Infom. Theory, Vol 49, No. 2, 2003.
[8] S. Y. Zhang, Y. Feng, X. M. Sun, M. S. Ying, Phys. Rev. A 64, 062103(2001).
[9] Y. Feng, S. Y. Zhang, R. Y. Duan, and M. S. Ying, Phys. Rev. A 66, 062313 (2002).
[10] Y. Sun, J.A. Bergou, and M. Hillery, Phys. Rev. A 66, 032315 (2002).
[11] T. Rudolph, R. W. Spekkens, P. S. Turner, Phys. Rev. A 68, 010301(R)(2003).
[12] P. Raynal, N. Lutkenhaus, S. J. van Enk, Phys. Rev. A 68, 022308 (2003).
[13] J. Fiurasek and M. Jezek, Phys. Rev. A 67, 012321 (2003).
[14] Y. C. Eldar, Phys. Rev. A 67, 042309 (2003).