A lower bound on the probability of error in quantum state discrimination

Ashley Montanaro[1]

[1]Department of Computer Science
University of Bristol
Bristol, UK

9th May 2008

University of Bristol

QICS

Introduction

We consider the quantum analogue of hypothesis testing:
quantum state discrimination.

Introduction

We consider the quantum analogue of hypothesis testing: quantum state discrimination.

Problem

Given an unknown state $\rho_?$ picked from an ensemble $\mathcal{E} = \{\rho_i\}$ of quantum states, with a priori probabilities p_i, how hard is it to determine which state $\rho_?$ is?

Introduction

We consider the quantum analogue of hypothesis testing: quantum state discrimination.

Problem

Given an unknown state $\rho_?$ picked from an ensemble $\mathcal{E} = \{\rho_i\}$ of quantum states, with a priori probabilities p_i, how hard is it to determine which state $\rho_?$ is?

Formally: let $M = \{\mu_i\}$ be a quantum measurement (POVM), i.e. $\mu_i \geqslant 0$, $\sum_i \mu_i = I$. Define the probability of error

$$P_E(M, \mathcal{E}) = \sum_{i \neq j} p_j \operatorname{tr}(\mu_i \rho_j)$$

Then what is

$$P_E(\mathcal{E}) = \min_M P_E(M, \mathcal{E})?$$

Previous work

Pioneering work by Holevo and Helstrom in 1970s gives exact solution of problem for 2 states ($\mathcal{E} = \{\rho_0, \rho_1\}$, $p_0 = p$, $p_1 = (1 - p)$):

$$P_E(\mathcal{E}) = \frac{1}{2} - \frac{1}{2} \|p\rho_0 - (1-p)\rho_1\|_1$$

(note: p-norms $\|\rho\|_p = \left(\sum_i \sigma_i(\rho)^p\right)^{1/p}$, $\sigma_i(\rho)$ = i'th singular value of ρ)

Previous work

Pioneering work by Holevo and Helstrom in 1970s gives exact solution of problem for 2 states ($\mathcal{E} = \{\rho_0, \rho_1\}$, $p_0 = p$, $p_1 = (1 - p)$):

$$P_E(\mathcal{E}) = \frac{1}{2} - \frac{1}{2} \| p\rho_0 - (1-p)\rho_1 \|_1$$

(note: p-norms $\|\rho\|_p = \left(\sum_i \sigma_i(\rho)^p\right)^{1/p}$, $\sigma_i(\rho)$ = i'th singular value of ρ)

But for more than 2 states, no exact solution is known.

Previous work

Pioneering work by Holevo and Helstrom in 1970s gives exact solution of problem for 2 states ($\mathcal{E} = \{\rho_0, \rho_1\}$, $p_0 = p$, $p_1 = (1-p)$):

$$P_E(\mathcal{E}) = \frac{1}{2} - \frac{1}{2}\|p\rho_0 - (1-p)\rho_1\|_1$$

(note: p-norms $\|\rho\|_p = \left(\sum_i \sigma_i(\rho)^p\right)^{1/p}$, $\sigma_i(\rho)$ = i'th singular value of ρ)

But for more than 2 states, no exact solution is known.

So we concentrate on finding bounds on the probability of error.

Previous work

A useful upper bound [Barnum and Knill '02]:

$$P_E(\mathcal{E}) \leqslant 2 \sum_{i>j} \sqrt{p_i p_j} \sqrt{F(\rho_i, \rho_j)}$$

(has found applications in quantum algorithms; note fidelity $F(\rho_i, \rho_j) = \|\sqrt{\rho_i}\sqrt{\rho_j}\|_1^2$)

Previous work

A useful upper bound [Barnum and Knill '02]:

$$P_E(\mathcal{E}) \leqslant 2 \sum_{i>j} \sqrt{p_i p_j} \sqrt{F(\rho_i, \rho_j)}$$

(has found applications in quantum algorithms; note fidelity $F(\rho_i, \rho_j) = \|\sqrt{\rho_i}\sqrt{\rho_j}\|_1^2$)

This bound relates the pairwise (local) distinguishability of a set of states to their global distinguishability.

Could we find a similar lower bound?

Previous work

A useful upper bound [Barnum and Knill '02]:

$$P_E(\mathcal{E}) \leqslant 2 \sum_{i>j} \sqrt{p_i p_j} \sqrt{F(\rho_i, \rho_j)}$$

(has found applications in quantum algorithms; note fidelity $F(\rho_i, \rho_j) = \|\sqrt{\rho_i}\sqrt{\rho_j}\|_1^2$)

This bound relates the pairwise (local) distinguishability of a set of states to their global distinguishability.

Could we find a similar lower bound?

Potential applications:

- Security proofs in quantum cryptography
- Lower bounds in quantum query complexity

Lower bounds

Some recently developed lower bounds:

- A bound based only on the individual states [Hayashi et al '08]:

$$P_E(\mathcal{E}) \geqslant 1 - n \max_i p_i \|\rho_i\|_\infty$$

(gives nothing when any of the states are pure)

Lower bounds

Some recently developed lower bounds:

- A bound based only on the individual states [Hayashi et al '08]:

$$P_E(\mathcal{E}) \geqslant 1 - n \max_i p_i \|\rho_i\|_\infty$$

(gives nothing when any of the states are pure)

- A recent bound in terms of the trace distance [Qiu '08]:

$$P_E(\mathcal{E}) \geqslant \frac{1}{2}\left(1 - \frac{1}{n-1}\sum_{i>j} \|p_i\rho_i - p_j\rho_j\|_1\right)$$

(n = number of states)

The new lower bound

Theorem

Let $\mathcal{E}$ be an ensemble of quantum states $\{\rho_i\}$ with a priori probabilities $\{p_i\}$. Then

$$P_E(\mathcal{E}) \geqslant \sum_{i>j} p_i p_j F(\rho_i, \rho_j).$$

The new lower bound

Theorem

Let $\mathcal{E}$ be an ensemble of quantum states $\{\rho_i\}$ with a priori probabilities $\{p_i\}$. Then

$$P_E(\mathcal{E}) \geqslant \sum_{i>j} p_i p_j F(\rho_i, \rho_j).$$

Note:

- ...the similarity to $P_E(\mathcal{E}) \leqslant 2\sum_{i>j} \sqrt{p_i p_j}\sqrt{F(\rho_i, \rho_j)}$.
- ...it's easy to use this bound in a multiple-copy scenario.

Proving the lower bound

The bound is based on matrix inequalities. We need some definitions:

Proving the lower bound

The bound is based on matrix inequalities. We need some definitions:

- Decompose $p_i\rho_i = \sum_j |e_{ij}\rangle\langle e_{ij}|$, assume ρ_i is d-dimensional and write

$$S_i = (|e_{i1}\rangle \cdots |e_{id}\rangle)\,, S = (S_1 \cdots S_n)$$

Proving the lower bound

The bound is based on matrix inequalities. We need some definitions:

- Decompose $p_i \rho_i = \sum_j |e_{ij}\rangle\langle e_{ij}|$, assume ρ_i is d-dimensional and write

$$S_i = (|e_{i1}\rangle \cdots |e_{id}\rangle)\,, S = (S_1 \cdots S_n)$$

- Similarly, decompose $\mu_i = \sum_j |f_{ij}\rangle\langle f_{ij}|$ and write

$$N_i = (|f_{i1}\rangle \cdots |f_{id}\rangle)\,, N = (N_1 \cdots N_n)$$

Proving the lower bound

The bound is based on matrix inequalities. We need some definitions:

- Decompose $p_i \rho_i = \sum_j |e_{ij}\rangle\langle e_{ij}|$, assume ρ_i is d-dimensional and write

$$S_i = (|e_{i1}\rangle \cdots |e_{id}\rangle)\,, S = (S_1 \cdots S_n)$$

- Similarly, decompose $\mu_i = \sum_j |f_{ij}\rangle\langle f_{ij}|$ and write

$$N_i = (|f_{i1}\rangle \cdots |f_{id}\rangle)\,, N = (N_1 \cdots N_n)$$

- Define the block matrix $A = N^\dagger S$ (so $A_{ij} = N_i^\dagger S_j$)

Proof outline

We will prove the following.

$$\begin{aligned} P_E(M, \mathcal{E}) &= \sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i>j} \|(A^\dagger A)_{ij}\|_1^2 \\ &= \sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j) \end{aligned}$$

Proof outline

We will prove the following.

$$
\begin{aligned}
P_E(M, \mathcal{E}) &= \sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i>j} \|(A^\dagger A)_{ij}\|_1^2 \\
&= \sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j)
\end{aligned}
$$

The red equality follows from:

$$
\sum_i \mu_i = I
$$

Proof outline

We will prove the following.

$$\begin{aligned} P_E(M, \mathcal{E}) &= \sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i>j} \|(A^\dagger A)_{ij}\|_1^2 \\ &= \sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j) \end{aligned}$$

The red equality follows from:

$$\sum_i \mu_i = I \Rightarrow NN^\dagger = I$$

Proof outline

We will prove the following.

$$
\begin{aligned}
P_E(M, \mathcal{E}) &= \sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i>j} \|(A^\dagger A)_{ij}\|_1^2 \\
&= \sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j)
\end{aligned}
$$

The red equality follows from:

$$
\sum_i \mu_i = I \Rightarrow NN^\dagger = I \Rightarrow A^\dagger A = S^\dagger NN^\dagger S = S^\dagger S
$$

The first equality

We want to show that

$$P_E(M, \mathcal{E}) = \sum_{i \neq j} \|A_{ij}\|_2^2$$

The first equality

We want to show that

$$P_E(M, \mathcal{E}) = \sum_{i \neq j} \|A_{ij}\|_2^2$$

This is immediate:

$$\|A_{ij}\|_2^2 = \mathrm{tr}((N_i^\dagger S_j)(S_j^\dagger N_i))$$

The first equality

We want to show that

$$P_E(M, \mathcal{E}) = \sum_{i \neq j} \|A_{ij}\|_2^2$$

This is immediate:

$$\|A_{ij}\|_2^2 = \mathrm{tr}((N_i^\dagger S_j)(S_j^\dagger N_i)) = \mathrm{tr}((N_i N_i^\dagger)(S_j S_j^\dagger))$$

The first equality

We want to show that

$$P_E(M, \mathcal{E}) = \sum_{i \neq j} \|A_{ij}\|_2^2$$

This is immediate:

$$\|A_{ij}\|_2^2 = \mathrm{tr}((N_i^\dagger S_j)(S_j^\dagger N_i)) = \mathrm{tr}((N_i N_i^\dagger)(S_j S_j^\dagger)) = p_j \, \mathrm{tr}(\mu_i \rho_j)$$

The inequality

We want to show that

$$\sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i > j} \|(A^\dagger A)_{ij}\|_1^2$$

The inequality

We want to show that

$$\sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i > j} \|(A^\dagger A)_{ij}\|_1^2$$

Will follow from the following inequality:

$$\sum_{i > 1} \|(A^\dagger A)_{1i}\|_1^2 \leqslant \sum_{i > 1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

The inequality

We want to show that

$$\sum_{i \neq j} \|A_{ij}\|_2^2 \geqslant \sum_{i > j} \|(A^\dagger A)_{ij}\|_1^2$$

Will follow from the following inequality:

$$\sum_{i>1} \|(A^\dagger A)_{1i}\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

First step: can show that

$$\sum_{i>1} \|(A^\dagger A)_{1i}\|_1^2 \leqslant \left\| \Big((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \Big) \right\|_1^2$$

(proof: by a majorisation argument)

A block matrix inequality

We want to show that

$$\left\| \begin{pmatrix} (A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \end{pmatrix} \right\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

A block matrix inequality

We want to show that

$$\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

Group A into "super-blocks":

$$A = \begin{pmatrix} \begin{pmatrix} A_{11} \end{pmatrix} & \begin{pmatrix} A_{12} & \dots & A_{1n} \end{pmatrix} \\ \begin{pmatrix} A_{21} \\ \vdots \\ A_{n2} \end{pmatrix} & \begin{pmatrix} A_{22} & \dots & A_{2n} \\ \vdots & \ddots & \vdots \\ A_{n2} & \dots & A_{nn} \end{pmatrix} \end{pmatrix}$$

A block matrix inequality (2)

We want to show that

$$\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

Define a new 2×2 "super-block matrix" B by padding each of these "super-blocks" in A with 0's so that each super-block is square and the same size. Then

$$\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 = \|B_{11}^\dagger B_{12} + B_{21}^\dagger B_{22}\|_1^2$$

A block matrix inequality (2)

We want to show that

$$\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

Define a new 2×2 "super-block matrix" B by padding each of these "super-blocks" in A with 0's so that each super-block is square and the same size. Then

$$\begin{aligned} \left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 &= \|B_{11}^\dagger B_{12} + B_{21}^\dagger B_{22}\|_1^2 \\ &\leqslant (\|B_{11}\|_2^2 + \|B_{22}\|_2^2)(\|B_{12}\|_2^2 + \|B_{21}\|_2^2) \end{aligned}$$

A block matrix inequality (2)

We want to show that

$$\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

Define a new 2×2 "super-block matrix" B by padding each of these "super-blocks" in A with 0's so that each super-block is square and the same size. Then

$$\begin{aligned}
\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 &= \|B_{11}^\dagger B_{12} + B_{21}^\dagger B_{22}\|_1^2 \\
&\leqslant (\|B_{11}\|_2^2 + \|B_{22}\|_2^2)(\|B_{12}\|_2^2 + \|B_{21}\|_2^2) \\
&\leqslant \|B_{12}\|_2^2 + \|B_{21}\|_2^2
\end{aligned}$$

A block matrix inequality (2)

We want to show that

$$\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 \leqslant \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2$$

Define a new 2×2 "super-block matrix" B by padding each of these "super-blocks" in A with 0's so that each super-block is square and the same size. Then

$$\begin{aligned}
\left\| \left((A^\dagger A)_{12} \cdots (A^\dagger A)_{1n} \right) \right\|_1^2 &= \|B_{11}^\dagger B_{12} + B_{21}^\dagger B_{22}\|_1^2 \\
&\leqslant (\|B_{11}\|_2^2 + \|B_{22}\|_2^2)(\|B_{12}\|_2^2 + \|B_{21}\|_2^2) \\
&\leqslant \|B_{12}\|_2^2 + \|B_{21}\|_2^2 \\
&= \sum_{i>1} \|A_{1i}\|_2^2 + \|A_{i1}\|_2^2
\end{aligned}$$

Getting the fidelities from $S^\dagger S$

We want to show the final equality

$$\sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j)$$

Getting the fidelities from $S^\dagger S$

We want to show the final equality

$$\sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j)$$

It is immediate that $S_i S_i^\dagger = p_i \rho_i$, so by the polar decomposition, for some unitary U

$$S_i = \sqrt{p_i \rho_i} U$$

Getting the fidelities from $S^\dagger S$

We want to show the final equality

$$\sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j)$$

It is immediate that $S_i S_i^\dagger = p_i \rho_i$, so by the polar decomposition, for some unitary U

$$S_i = \sqrt{p_i \rho_i} U$$

Implies that in terms of the blocks of S,

$$\|S_i^\dagger S_j\|_1^2 = \|U^\dagger \sqrt{p_i \rho_i} \sqrt{p_j \rho_j} V\|_1^2$$

Getting the fidelities from $S^\dagger S$

We want to show the final equality

$$\sum_{i>j} \|(S^\dagger S)_{ij}\|_1^2 = \sum_{i>j} p_i p_j F(\rho_i, \rho_j)$$

It is immediate that $S_i S_i^\dagger = p_i \rho_i$, so by the polar decomposition, for some unitary U

$$S_i = \sqrt{p_i \rho_i} U$$

Implies that in terms of the blocks of S,

$$\|S_i^\dagger S_j\|_1^2 = \|U^\dagger \sqrt{p_i \rho_i} \sqrt{p_j \rho_j} V\|_1^2 = p_i p_j \|\sqrt{\rho_i} \sqrt{\rho_j}\|_1^2 = p_i p_j F(\rho_i, \rho_j)$$

and the proof is complete.

Tightness

Even for an ensemble of 2 states, this bound is not always tight (i.e. does not reduce to the Holevo-Helstrom bound).

Tightness

Even for an ensemble of 2 states, this bound is not always tight (i.e. does not reduce to the Holevo-Helstrom bound).
Consider an ensemble $\mathcal{E} = \{\rho_1, \rho_2\}$ where $\rho_1 = \rho_2$, $p_1 = p$, $p_2 = 1 - p$. Then

$$P_E(\mathcal{E}) = \frac{1}{2} - \frac{1}{2}\|(p - (1-p))\rho\|_1 = \frac{1}{2} - |p - \frac{1}{2}|$$

but the bound here guarantees only

$$P_E(\mathcal{E}) \geqslant p(1-p)$$

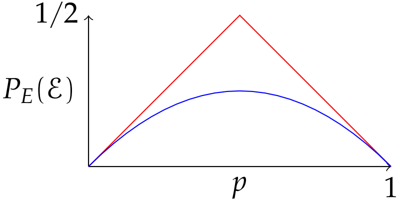
Tightness

Even for an ensemble of 2 states, this bound is not always tight (i.e. does not reduce to the Holevo-Helstrom bound).
Consider an ensemble $\mathcal{E} = \{\rho_1, \rho_2\}$ where $\rho_1 = \rho_2$, $p_1 = p$, $p_2 = 1 - p$. Then

$$P_E(\mathcal{E}) = \frac{1}{2} - \frac{1}{2}\|(p - (1-p))\rho\|_1 = \frac{1}{2} - |p - \frac{1}{2}|$$

but the bound here guarantees only

$$P_E(\mathcal{E}) \geqslant p(1-p)$$



Holevo-Helstrom bound

New bound

Summary

$$P_E(\mathcal{E}) \geqslant \sum_{i>j} p_i p_j F(\rho_i, \rho_j).$$

- We've seen a new lower bound on the probability of error in quantum state discrimination.
- It can be thought of as a converse of an upper bound of Barnum and Knill.
- It's comparable to a recent bound of Qiu.

Summary

$$P_E(\mathcal{E}) \geqslant \sum_{i>j} p_i p_j F(\rho_i, \rho_j).$$

- We've seen a new lower bound on the probability of error in quantum state discrimination.
- It can be thought of as a converse of an upper bound of Barnum and Knill.
- It's comparable to a recent bound of Qiu.

Applications?

Summary

$$P_E(\mathcal{E}) \geqslant \sum_{i>j} p_i p_j F(\rho_i, \rho_j).$$

- We've seen a new lower bound on the probability of error in quantum state discrimination.
- It can be thought of as a converse of an upper bound of Barnum and Knill.
- It's comparable to a recent bound of Qiu.

Applications?

Further reading: arXiv:0711.2012.

Summary

$$P_E(\mathcal{E}) \geqslant \sum_{i>j} p_i p_j F(\rho_i, \rho_j).$$

- We've seen a new lower bound on the probability of error in quantum state discrimination.
- It can be thought of as a converse of an upper bound of Barnum and Knill.
- It's comparable to a recent bound of Qiu.

Applications?

Further reading: arXiv:0711.2012.

Thanks for your time!