Quantum state discrimination

I. DISCRIMINATING BETWEEN PAIRS OF STATES

Definition 1 *Let* X *be a register with alphabet* Σ. *Let* Y *be a classical register with alphabet* $\{0,1\}$. *Alice prepares the following classical-quantum state* $\sigma \in \mathsf{D}(\mathcal{Y} \otimes \mathcal{X})$ *with* $\rho_0, \rho_1 \in \mathsf{D}(\mathcal{X})$.

$$\sigma = \lambda E_{0,0} \otimes \rho_0 + (1-\lambda) E_{1,1} \otimes \rho_1 \tag{1}$$

send X *to Bob. Then Bob guesses the state of* Y *according to the result of a measurement.*

A. Classical states discrimination

Consider the classical case that ρ_i is the probability state of X referring to $p_i \in \mathcal{P}(\Sigma)$, $(i = 0,1)$. That is

$$\sigma = \sum_{a\in\Sigma} \lambda p_0(a) E_{0,0} \otimes E_{a,a} + (1-\lambda) p_1(a) E_{1,1} \otimes E_{a,a} \tag{2}$$

It is easy to see that $\Pr(\mathsf{X} = a) = \lambda p_0(a) + (1-\lambda) p_1(a)$. We have

$$\Pr(\mathsf{Y} = 0 | \mathsf{X} = a) = \frac{\lambda p_0(a)}{\lambda p_0(a) + (1-\lambda) p_1(a)} \tag{3}$$

$$\Pr(\mathsf{Y} = 1 | \mathsf{X} = a) = \frac{(1-\lambda) p_1(a)}{\lambda p_0(a) + (1-\lambda) p_1(a)} \tag{4}$$

If the measurement tells that $X = a$, then the probability Bob is correct with the best strategy is given by

$$\frac{\max\{\lambda p_0(a), (1-\lambda) p_1(a)\}}{\lambda p_0(a) + (1-\lambda) p_1(a)} = \frac{1}{2} + \frac{|\lambda p_0(a) - (1-\lambda) p_1(a)|}{2(\lambda p_0(a) + (1-\lambda) p_1(a))} \tag{5}$$

Thus the probability Bob is correct is given by

$$\frac{1}{2} + \frac{1}{2} \sum_{a\in\Sigma} |\lambda p_0(a) - (1-\lambda) p_1(a)| = \frac{1}{2} + \frac{1}{2} \|\rho_0 - \rho_1\|_1 \tag{6}$$

B. Quantum state discrimination

Suppose Bob use a measurement $\mu : \{0,1\} \to \mathsf{Pos}(\mathcal{X})$ and take the outcome of the measurement as the strategy. Let Φ_μ be the quantum-to-classical channel corresponding to μ

$$\begin{aligned}\Phi_\mu(\sigma) = {} & \lambda \langle \mu(0), \rho_0 \rangle E_{0,0} \otimes E_{0,0} \\ & + \lambda \langle \mu(1), \rho_0 \rangle E_{0,0} \otimes E_{1,1} \\ & + (1-\lambda) \langle \mu(0), \rho_1 \rangle E_{1,1} \otimes E_{0,0} \\ & + (1-\lambda) \langle \mu(1), \rho_1 \rangle E_{1,1} \otimes E_{1,1}\end{aligned}$$

Then the probability he is correct is

$$\lambda \langle \mu(0), \rho_0 \rangle + (1-\lambda) \langle \mu(1), \rho_1 \rangle \tag{7}$$

Lemma 1 $u \in \mathbb{C}^\Sigma$ *and* $\{P_a : a \in \Sigma\} \subset \mathsf{Pos}(\mathcal{X})$ *be a collection of positive semidefinite operators. It holds that*

$$\left\| \sum_{a\in\Sigma} u(a) P_a \right\| \leq \|u\| \left\| \sum_{a\in\Sigma} P_a \right\| \tag{8}$$

Proof. Define $A \in \mathsf{Lin}(\mathcal{X}, \mathcal{X} \otimes \mathbb{C}^\Sigma)$

$$A = \sum_{a\in\Sigma} \sqrt{P_a} \otimes e_a \tag{9}$$

$$\begin{aligned}
\left\| \sum_{a\in\Sigma} u(a) P_a \right\| &= \left\| \sum_{a\in\Sigma} u(a) A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a}) A \right\| \\
&\leq \|A^*\| \left\| \sum_{a\in\Sigma} u(a) E_{a,a} \right\| \|A\| \\
&= \|u\| \|A\|^2 \\
&= \|u\| \|A^* A\| \\
&= \|u\| \left\| \sum_{a\in\Sigma} P_a \right\|
\end{aligned}$$

■

Theorem 1 *(Holevo-Helstrom theorem) Let $\mathcal{X}$ be a complex Euclidean space, let $\rho_0, \rho_1 \in \mathsf{D}(X)$ be density operators, and let $\lambda \in [0,1]$. For every choice of a measurement $\mu : \{0,1\} \to \mathsf{Pos}(\mathcal{X})$, it holds that*

$$\lambda\langle \mu(0), \rho_0\rangle + (1-\lambda)\langle \mu(1), \rho_1\rangle \leq \frac{1}{2} + \frac{1}{2}\|\lambda\rho_0 - (1-\lambda)\rho_1\|_1 \tag{10}$$

Moreover, there exists a projective measurement for which equality is achieved.

Proof. Let $X = \lambda\rho_0 - (1-\lambda)\rho_1$.

$$\lambda\langle \mu(0), \rho_0\rangle + (1-\lambda)\langle \mu(1), \rho_1\rangle = \frac{1}{2} + \frac{1}{2}\langle \mu(0) - \mu(1), X\rangle \tag{11}$$

We know that

$$\langle \mu(0) - \mu(1), X\rangle \leq \|\mu(0) - \mu(1)\| \|X\|_1 \leq \|X\|_1 \tag{12}$$

To achieve the equality, consider thw Jordan-Hahn decomposition

$$X = P - Q \tag{13}$$

Then define

$$\mu(0) = \Pi_{\mathsf{im}(P)} \qquad \mu(1) = \Pi_{\mathsf{im}(Q)} \tag{14}$$

It holds that

$$\langle \mu(0) - \mu(1), X\rangle = \mathrm{Tr}(P) + \mathrm{Tr}(Q) = \|X\|_1 \tag{15}$$

■

Theorem 2 *Let $\mu : \Sigma \to \mathsf{Pos}(\mathcal{X})$ be a measurement, and let $X \in \mathsf{Lin}(\mathcal{X})$ be an operator. Let Φ_μ be the quantum-to-classical channel corresponding to μ. Then*

$$\|\Phi_\mu(X)\|_1 \leq \|X\|_1 \tag{16}$$

Proof.

$$\begin{aligned}\|\Phi_\mu(X)\|_1 &= \sum_{a\in\Sigma} |\langle \mu(a), X\rangle| \\ &= \sum_{a\in\Sigma} u(a)\langle \mu(a), X\rangle \\ &= \left\langle \sum_{a\in\Sigma} u(a)\mu(a), X \right\rangle \\ &\leq \left\| \sum_{a\in\Sigma} u(a)\mu(a) \right\| \|X\|_1 \\ &\leq \|X\|_1\end{aligned}$$

where $u(a)$ are the phase factors. ■

Definition 2 *Let X be a register and let Y be a register having classical state set $\{0,1\}$. The register Y is to be viewed as a classical register, while X is an arbitrary register. Also let $\mathcal{C}_0, \mathcal{C}_1 \subset \mathsf{D}(\mathcal{X})$ be nonempty, convex sets of states, and let $\lambda \in [0,1]$ be a real number. The sets $\mathcal{C}_0$ and $\mathcal{C}_1$, as well as the number λ, are assumed to be known to both Alice and Bob. Alice uses arbitrary states $\rho_0 \in \mathcal{C}_1, \rho_1 \in \mathcal{C}_2$ to prepare a state*

$$\sigma = \lambda E_{0,0} \otimes \rho_0 + (1-\lambda) E_{1,1} \otimes \rho_1 \tag{17}$$

and send it to Bob. Then Bob guesses the state of Y according to the result of a measurement.

Theorem 3 *Let $\mathcal{C}_0, \mathcal{C}_1 \subset \mathsf{D}(\mathcal{X})$ be nonempty, convex sets, and let $\lambda \in [0,1]$. It holds that*

$$\sup_{\mu} \inf_{\rho_0,\rho_1} (\lambda\langle \mu(0), \rho_0\rangle + (1-\lambda)\langle \mu(1), \rho_1\rangle) = \inf_{\rho_0,\rho_1} \sup_{\mu} (\lambda\langle \mu(0), \rho_0\rangle + (1-\lambda)\langle \mu(1), \rho_1\rangle) \tag{18}$$

$$= \frac{1}{2} + \frac{1}{2} \inf_{\rho_0,\rho_1} \|\lambda\rho_0 + (1-\lambda)\rho_1\|_1 \tag{19}$$

II. DISCRIMINATING QUANTUM STATES OF AN ENSEMBLE

Definition 3 *Let X be a register. Let Y be a classical register with alphabet Σ. Let $\eta : \Sigma \to \mathsf{Pos}(\mathcal{X})$ be an ensemble of states.*

Alice prepares the pair (Y, X) in the classical-quantum state

$$\sigma = \sum_{a\in\Sigma} E_{a,a} \otimes \eta(a) \tag{20}$$

and send it to Bob. Then Bob guesses the state of Y according to the result of a measurement.

The probability Bob is correct:

$$\sum_{a\in\Sigma} \langle \mu(a), \eta(a)\rangle \tag{21}$$

To optimize the probability, consider a more general problem: let $\phi : \Sigma \to \mathsf{Herm}(\mathcal{X})$. Consider a maximization of the quantity

$$\sum_{a\in\Sigma} \langle \mu(a), \phi(a)\rangle \tag{22}$$

over all measurements μ.

A semidefinite program for optimal measurements

For any choice of a function $\phi : \Sigma \to \mathsf{Herm}(\mathcal{X})$, define

$$\operatorname{opt}(\phi) = \max_{\mu} \sum_{a\in\Sigma} \langle \mu(a), \phi(a)\rangle \tag{23}$$

There is no closed-form expression that is known to represent the value $\operatorname{opt}(\phi)$ for an arbitrary choice of a function $\phi : \Sigma \to \mathsf{Herm}(\mathcal{X})$.

Definition 4 *Let $P, Q \in \mathsf{Pos}(\mathcal{X})$, the fidelity is defined as*

$$\mathrm{F}(P,Q) = \|\sqrt{P}\sqrt{Q}\|_1 = \mathrm{Tr}\left(\sqrt{\sqrt{Q}P\sqrt{Q}}\right) \tag{24}$$

Property 1 *The following facts hold:*

1. F *is continuous at* (P,Q)
2. $\mathrm{F}(P,Q) = \mathrm{F}(Q,P)$
3. $\mathrm{F}(\lambda P,Q) = \mathrm{F}(P,\lambda Q) = \sqrt{\lambda}\,\mathrm{F}(P,Q)$
4. $\mathrm{F}(P,Q) = \mathrm{F}(\Pi_{\mathsf{im}(Q)}P\Pi_{\mathsf{im}(Q)},Q) = \mathrm{F}(P,\Pi_{\mathsf{im}(P)}Q\Pi_{\mathsf{im}(P)})$
5. $\mathrm{F}(P,Q) \geq 0$ *with equality iff* $PQ = 0$
   Proof. $\|\sqrt{P}\sqrt{Q}\|_1 \geq 0$ *with equality iff* $\sqrt{P}\sqrt{Q} = 0$*, which is equivalent to* $PQ = 0$.
6. $\mathrm{F}(P,Q)^2 \leq \mathrm{Tr}(P)\,\mathrm{Tr}(Q)$ *with equality iff P and Q are linearly dependent.*
   Proof.
   $$\|\sqrt{P}\sqrt{Q}\|_1^2 = |\langle U, \sqrt{P}\sqrt{Q}\rangle|^2 \tag{25}$$
7. $V \in \mathsf{U}(\mathcal{X},\mathcal{Y})$, $\mathrm{F}(P,Q) = \mathrm{F}(VPV^*, VQV^*)$
8. $F(P, vv^*) = \sqrt{v^*Pv}$
9. $F(P, QPQ) = \langle P, Q\rangle$
10. $\rho \in \mathsf{D}(\mathcal{X})$, $P \leq \mathbb{1}_{\mathcal{X}}$, $\langle P,\rho\rangle > 0$
    $$\mathrm{F}\left(\rho, \frac{\sqrt{P}\rho\sqrt{P}}{\langle P,\rho\rangle}\right) \geq \sqrt{\langle P,\rho\rangle} \tag{26}$$
11. $\mathrm{F}(P_0 \otimes P_1, Q_0 \otimes Q_1) = \mathrm{F}(P_0,Q_0)\,\mathrm{F}(P_1,Q_1)$
12. $$\mathrm{F}(P,Q) = \max\left\{|\,\mathrm{Tr}(X)| : X \in \mathsf{Lin}(\mathcal{X}), \begin{bmatrix} P & X \\ X^* & Q \end{bmatrix} \in \mathsf{Pos}(\mathcal{X}\oplus\mathcal{X})\right\} \tag{27}$$

III. CHANNEL DISCRIMINATION

Bob prepares a state $\sigma \in \mathsf{D}(\mathcal{X}\otimes\mathcal{W})$. Then Alice prepare channel Φ_0 or Φ_1 on system $\mathcal{X}$.

$$\rho_0 = (\Phi_0 \otimes \mathbb{1}_{\mathsf{Lin}(\mathcal{W})})\sigma \qquad \rho_1 = (\Phi_1 \otimes \mathbb{1}_{\mathsf{Lin}(\mathcal{W})})\sigma \tag{28}$$

with probability λ and $1-\lambda$.

Then Bob can distinguish the two states with probability

$$\frac{1}{2} + \frac{1}{2}\|\lambda\rho_0 + (1-\lambda)\rho_1\|_1 \tag{29}$$

Definition 5 *The induced trace norm*

$$\|\Phi\|_1 = \max\{\|\Phi(X)\|_1 : X \in \mathsf{Lin}(\mathcal{X}), \|X\|_1 \leq 1\} \tag{30}$$

Theorem 4 *Let $\Phi \in \mathsf{Transf}(\mathcal{X},\mathcal{Y})$ be a positive and trace-presearving map, then $\|\Phi\|_1 = 1$.*

Property 2 *1.*

$$\|\Psi\Phi\|_1 \leq \|\Psi\|_1\|\Phi\|_1 \tag{31}$$

2.

$$\|\Psi_1\Psi_0 - \Phi_1\Phi_0\|_1 \leq \|\Psi_1 - \Phi_1\|_1\|\Psi_0 - \Phi_0\|_1 \tag{32}$$

$$\left\|\left|\sum_{a\in\Sigma}\right|\right\| \tag{33}$$