QIC 820 / CO781 / CO486 / CS 867

Lecture notes for Oct 24, 2023

Last time: applications of SDP, strong duality & complementary slackness
for optimal state discrimination

Helstrom's theorem *
Fidelity & Alberti's theorem *

proved earlier
alternative proofs here

Today:

Uhlmann's theorem *
Several properties of fidelity *

Completely bounded / diamond norm for channels

SDP for diamond norm

Very briefly in class, Read exercise: chapter 20 in LN 2011

<u>Rederiving Uhlmann's theorem from SDP:</u>

Let $P, Q \in \mathrm{Pos}(\mathcal{X})$, uu^* a fixed purification of P, $u \in \mathcal{X} \otimes \mathcal{Y}$
$\dim(\mathcal{Y}) \geq \dim(\mathcal{X})$

Consider the following SDP's :

$$\alpha = \sup \langle W, uu^* \rangle \qquad\qquad \beta = \inf \langle Q, Z \rangle$$
$$\text{s.t. } \mathrm{Tr}_{\mathcal{Y}}(W) = Q \qquad\qquad \text{s.t. } Z \otimes \mathbb{1}_{\mathcal{Y}} \geq uu^*$$
$$W \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \qquad\qquad Z \in \mathrm{Herm}(\mathcal{X})$$

- Claim 1 : these are primal-dual pair, easily verified by noting :

  W : primal variable
  $A = uu^*$, $B = Q$
  $\Phi = \mathrm{Tr}_{\mathcal{Y}} \in C(\mathcal{X} \otimes \mathcal{Y}, \mathcal{X})$
  $\Phi^*(Z) = Z \otimes \mathbb{1}_{\mathcal{Y}}$ (derived before)

- Claim 2 : $\beta = F(P, Q)^2$

Pf: (a) Rephrasing the dual constraints. Let Z be dual feasible.

Note $Z \geq 0$ . . Let $Z = \sum_i \lambda_i |e_i\rangle\langle e_i|$, $\lambda_i > 0$
be spec decomp.

$$\text{Let } Z^{-\frac{1}{2}} = \sum_i \lambda_i^{-\frac{1}{2}} |e_i\rangle\langle e_i| \quad (\text{pseudo-inverse})$$
$$\Pi_Z = \sum_i |e_i\rangle\langle e_i|$$

Now $Z \otimes \mathbb{1}_{\mathcal{Y}} \geq uu^* \iff \Pi_Z \otimes \mathbb{1}_{\mathcal{Y}} \geq (Z^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathcal{Y}}) uu^* (Z^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathcal{Y}})$

$$\iff \| (Z^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathcal{Y}}) uu^* (Z^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathcal{Y}}) \|_\infty \leq 1$$
$$\|$$
$$\mathrm{tr}\, (Z^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathcal{Y}}) uu^* (Z^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathcal{Y}})$$

(because matrix is rank 1 !!)

$$\mathrm{tr}\,(Z^{-\frac{1}{2}} \otimes \mathbb{1}_Y)\, uu^* \,(Z^{-\frac{1}{2}} \otimes \mathbb{1}_Y)$$

$$= \mathrm{tr}\left[(Z^{-1} \otimes \mathbb{1}_Y)\, uu^*\right]$$

$$= \langle Z^{-1}, \mathrm{Tr}_Y\, uu^* \rangle \qquad \text{(proved earlier in course)}$$

$$= \langle Z^{-1}, P \rangle \qquad \text{(u purifies P)}$$

$$\therefore\ \beta = \inf \langle Q, Z \rangle \quad \text{s.t. } \langle Z^{-1}, P\rangle \leq 1,\quad Z \geq 0$$

ⓑ We can restrict the feasible set to $\langle Z^{-1}, P\rangle = 1$

Since if $\langle Z^{-1}, P\rangle = \lambda < 1$

$(Z\lambda)$ is feasible : $Z\lambda \geq 0$

$$\langle (Z\lambda)^{-1}, P\rangle = \lambda^{-1}\langle Z^{-1}, P\rangle = 1$$

$\langle Q, Z\lambda\rangle = \lambda\langle Q, Z\rangle \leq \langle Q, Z\rangle$ $\therefore$ λZ is better than Z.

$$\therefore\ \beta = \inf \langle Q, Z\rangle \quad \text{s.t. } \langle Z^{-1}, P\rangle = 1,\quad Z \geq 0$$

Note this is a different SDP with the same value.

ⓒ Finally : $\beta = \inf\limits_{Z \geq 0} \langle Q, Z\rangle \langle P, Z^{-1}\rangle$

by multiplying $1 = \langle P, Z^{-1}\rangle$ to objective function and noting that it's now scale invariant so we drop $1 = \langle P, Z^{-1}\rangle$ constraint.

$$= \inf_{Z > 0} \underbrace{\langle Q, Z\rangle}_{= \lim\limits_{\varepsilon \to 0} \langle Q, Z + \varepsilon \mathbb{1}\rangle} \underbrace{\langle P, Z^{-1}\rangle}$$

initially, $Z \otimes \mathbb{1}_Y \geq uu^*$, $Z \geq 0$

$\therefore \langle I - \Pi_Z, P\rangle = 0$, preserved when Z rescaled

$= F(P, Q)^2$ (by Alberti) $\quad \therefore \lim\limits_{\varepsilon \to 0} \langle P, (Z + I\varepsilon)^{-1}\rangle = \langle P, Z\rangle$.

Alternatively, take $P \in \mathrm{Pd}(X)$ then $Z \in \mathrm{Pd}(X)$ use continuity of $F(Q, P)$

- Claim 3 : original dual strictly feasible.

  take $Z = \|u\|^2 \times 2 \times \mathbb{1}_X$, then $Z \otimes \mathbb{1}_Y > uu^*$

  β bounded since primal SDP is feasible, with $W = Q \otimes \frac{\mathbb{1}_Y}{\dim Y}$.

  By Slater's Thm for the dual, $\alpha = \beta$ and α can be attained.

$$\therefore \ F(P,Q)^2 = \max_{W \text{ extension of } Q} \langle W, uu^* \rangle$$

$$= \max_{W \text{ purifies } Q} \langle W, uu^* \rangle$$

which is Uhlmann's Thm.

fixed purification of P.

purifies W from the previous line

Application: proving properties of $\| \|_1$ & F using SDP.

- Monotonicity: If $\Phi \in C(\mathcal{X}, \mathcal{Y})$ (TP & CP), and $P, Q \in \mathrm{Pos}(\mathcal{X})$, then

(1) $\| P - Q \|_1 \geq \| \Phi(P) - \Phi(Q) \|_1$

(2) $F(\Phi(P), \Phi(Q)) \geq F(P, Q)$

Pf: For (1): $\| \Phi(P) - \Phi(Q) \|_1 \frac{1}{4} + \frac{1}{2}$

$$= \sup \tfrac{1}{2} \langle M, \Phi(P) \rangle + \tfrac{1}{2} \langle M', \Phi(Q) \rangle$$

s.t. $M + M' = \mathbb{1}$

$M, M' \geq 0$

$$= \sup \tfrac{1}{2} \langle \Phi^*(M), P \rangle + \tfrac{1}{2} \langle \Phi^*(M'), Q \rangle$$

$M + M' = \mathbb{1} \Rightarrow \Phi^*(M) + \Phi^*(M') = \mathbb{1}$ (Φ TP $\Leftrightarrow$ Φ^* unital)

$M, M' \geq 0 \Rightarrow \Phi^*(M), \Phi^*(M') \geq 0$ (only need positivity)

$\therefore$ $\Phi^*(M), \Phi^*(M')$ feasible for the SDP for $\| P - Q \|_1 \frac{1}{4} + \frac{1}{2}$

$\leq \| P - Q \|_1 \frac{1}{4} + \frac{1}{2}$

For (2): $F(P, Q) = \max \frac{1}{2} \mathrm{Tr}(X) + \frac{1}{2} \mathrm{Tr}(X^*)$

s.t. $\begin{bmatrix} P & X \\ X^* & Q \end{bmatrix} \geq 0$

$\because$ Φ completely positive, $I_{\mathbb{C}^2} \otimes \Phi \left(\begin{bmatrix} P & X \\ X^* & Q \end{bmatrix} \right) \geq 0$

$$\| \qquad \begin{bmatrix} \Phi(P) & \Phi(X) \\ \Phi(X^*) & \Phi(Q) \end{bmatrix}$$

$\therefore$ $\Phi(X)$ is feasible for the SDP for $F(\Phi(P), \Phi(Q))$.

Φ TP $\Rightarrow$ $\frac{1}{2}(\mathrm{Tr}(X) + \mathrm{Tr}(X^*)) = \frac{1}{2} \mathrm{Tr}(\Phi(X) + \mathrm{Tr}\, \Phi(X^*))$ $\therefore$ $F(P, Q) \geq F(\Phi(P), \Phi(Q))$

- Joint Concavity:

Let $(p_1, \dots, p_n)$ be a prob vector, $P_i, Q_i \in \mathrm{Pos}(X)$, $i = 1 \dots n$

Then $F\left(\underline{\sum_i p_i P_i}, \underline{\sum_i p_i Q_i} \right) \geq \sum_i p_i \, F(P_i, Q_i)$

intuition: mixing reduces distinguishability

Pf: For each i, let X_i optimizes $F(P_i, Q_i) = \max \frac{1}{2} \mathrm{tr}(X_i) + \frac{1}{2} \mathrm{tr}(X_i^*)$

$$\text{s.t.} \begin{bmatrix} P_i & X_i \\ X_i^* & Q_i \end{bmatrix} \geq 0$$

So $\begin{bmatrix} \sum_i p_i P_i & \sum_i p_i X_i \\ \sum_i p_i X_i^* & \sum_i p_i Q_i \end{bmatrix} \geq 0$

So $X = \sum_i p_i X_i$ feasible for $F\left(\sum_i p_i P_i, \sum_i p_i Q_i \right)$

$$\therefore F\left(\sum_i p_i P_i, \sum_i p_i Q_i \right) \geq \frac{1}{2} \mathrm{tr}\, X + \frac{1}{2} \mathrm{tr}\, X^* \qquad (X \text{ feasible})$$

$$= \frac{1}{2} \sum_i p_i \, \mathrm{tr}\, X_i + \frac{1}{2} \sum_i p_i \, \mathrm{tr}\, X_i^* \qquad (\text{sub } X = \sum_i p_i X_i)$$

$$= \sum_i p_i \, F(P_i, Q_i) \qquad (\text{optimality of } X_i \text{ for } F(P_i, Q_i)).$$

LN 2011, cp 20. Completely-bounded trace norm

Recall if state ρ_0 is given wp λ, ρ_1 wp $1-\lambda$ $\Big\}$ state ρ_i

and meas (μ_0, μ_1) applied with outcome K,

then $\text{prob}(K=i) = \lambda \langle \mu_0, \rho_0 \rangle + (1-\lambda) \langle \mu_1, \rho_1 \rangle$

$\downarrow$ max over μ_0, μ_1

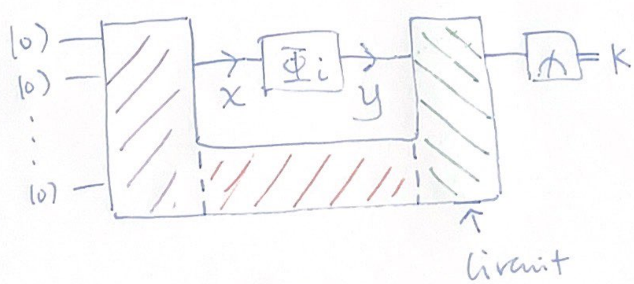
$$= \frac{1}{2} + \frac{1}{2} \| \lambda \rho_0 - (1-\lambda) \rho_1 \|_1$$

Instead, if channels Φ_0 is given wp λ, Φ_1 wp $1-\lambda$ $\Big\}$ channel $\Phi_i \in C(\mathcal{X}, \mathcal{Y})$

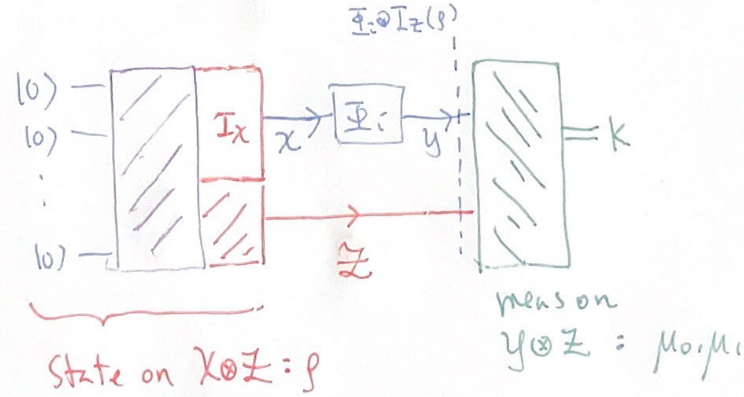
what is the "sup" prob to identify i?

(1) The procedure to find i cannot depend on i (except the one black-box use of Φ_i)

(2) The final step is a measurement with outcome $K \in \{0, 1\}$.



$\|$



③ $\max_{\mu_0,\mu_1} \text{Prob}(K=i) = \frac{1}{2} + \frac{1}{2} \| \lambda\, \Phi_0 \otimes I_Z(\rho) - (1-\lambda)\, \Phi_1 \otimes I_Z(\rho) \|_1$

$= \frac{1}{2} + \frac{1}{2} \| (\lambda \Phi_0 - (1-\lambda) \Phi_1) \otimes I_Z(\rho) \|_1$

Best prob $(K=i)$

$= \sup_{Z} \max_{\rho \in D(X \otimes Z)} \max_{\mu_0,\mu_1} \text{Prob}(K=i) = \frac{1}{2} + \frac{1}{2} ||| \lambda \Phi_0 - (1-\lambda) \Phi_1 |||_1$

where $||| \Phi |||_1 := \sup_{Z} \max_{\rho \in D(X \otimes Z)} \| \Phi \otimes I_Z(\rho) \|_1$

is the completely-bounded trace-norm of Φ.

④ By expanding Z to purify ρ, WLOG, $\rho = uu^*$.

⑤ If $\Phi_0, \Phi_1 \in T(X,Y)$ instead of $C(X,Y)$

max is over $\rho = uv^*$, $u, v \in X \otimes Z$.

⑥ $\sup_{Z}$ can be replaced by $Z \sim X$!! (Lemma 20.2, Thm 20.3)

⑦ Thm 20.5 : if Φ Hermiticity-preserving, optimal $\rho = uu^*$.

⑧ Thm 20.4 : If $\Phi_i \in T(X_i, Y_i)$

then $||| \Phi_1 \otimes \Phi_2 |||_1 = ||| \Phi_1 |||_1 \cdot ||| \Phi_2 |||_2$

⑨ Sys Z is NECESSARY !!

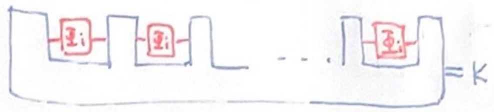
See Example 20.1 for the near max difference of prob $(K=i)$ with /without Z.

See arXiv/quant-ph/0307104, Thm II.2 and Eq (33)

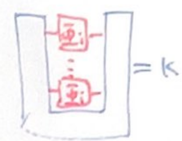
Very diff examples

(10) If one is given $n > 1$ uses of the unknown channel Φ_i,

the best distinguishing circuit is:



corresponds to



The best prob $(k = i)$ is NOT necessarily related to $||| \lambda \Phi_0^{\otimes n} - (1-\lambda) \Phi_1^{\otimes n} |||_1$

See arXiv: 0909.0256 for explicit example, and more app of SDP!!