Lecture 16

Quantum Chernoff bound

Asymptotic limit of symmetric hypothesis testing

It is intuitive that error prob. should generally decrease as more copies of state are available

i.e. ρ or σ vs.

$\rho^{\otimes 2}$ or $\sigma^{\otimes 2}$ vs.

$\rho^{\otimes 3}$ or $\sigma^{\otimes 3}$ etc.

- It generally happens that decay rate of error prob. is exponential in n:

$$p^*_{err}(\lambda, \rho^{\otimes n}, \sigma^{\otimes n}) \approx 2^{-n\,\xi(\rho,\sigma)}$$

where ξ is a function of ρ & σ (not of λ)

Theorem:

$$\lim_{n\to\infty} -\frac{1}{n}\log_2 p^*_{err}(\lambda, \rho^{\otimes n}, \sigma^{\otimes n})$$
$$= C(\rho\|\sigma)$$
$$:= \sup_{s\in(0,1)}\left(-\log_2 \mathrm{Tr}[\rho^s\sigma^{1-s}]\right)$$

Helpful lemma:

$$\frac{1}{2}\left(\mathrm{Tr}[A+B] - \|A-B\|_1\right) \leq \mathrm{Tr}[A^sB^{1-s}]$$

$\forall$ PSD A & B & $s\in(0,1)$

Set $\Delta = A - B$

& set Δ_+ & Δ_- to be positive & negative parts of Δ

(i.e. $\Delta_+, \Delta_- \geq 0$, $\Delta = \Delta_+ - \Delta_-$ & $\Delta_+ \Delta_- = 0$)

$$|\Delta| = |\Delta_+ - \Delta_-| = \Delta_+ + \Delta_-$$

Then $\|A-B\|_1 = \|\Delta\|_1 = \mathrm{Tr}[\Delta_+] + \mathrm{Tr}[\Delta_-]$

Also
$$A+B = A-B+2B = \Delta_+ - \Delta_- + 2B$$

$$\Rightarrow \frac{1}{2}\left(\mathrm{Tr}[A+B] - \|A-B\|_1\right) = \mathrm{Tr}[B] - \mathrm{Tr}[\Delta_-]$$

suffices to prove

$$\mathrm{Tr}[B] - \mathrm{Tr}[\Delta_-] \leq \mathrm{Tr}[A^s B^{1-s}] \quad \forall s \in (0,1)$$

$B + \Delta_+ \geq B$ (b/c $\Delta_+ \geq 0$)

Since $A - B = \Delta_+ - \Delta_-$,

$$A + \Delta_- = B + \Delta_+ \geq B$$

$$\Rightarrow \quad B^s \leq (A + \Delta_-)^s$$ for $s \in (0,1)$ (x^s op. monotone)

then

$$Tr[B] - Tr[A^s B^{1-s}]$$

$$= Tr[(B^s - A^s) B^{1-s}]$$

$$\leq Tr[((A+\Delta_-)^s - A^s) B^{1-s}]$$

$$\leq Tr[((A+\Delta_-)^s - A^s) (A+\Delta_-)^{1-s}]$$

$$= Tr[A] + Tr[\Delta_-] - Tr[A^s (A+\Delta_-)^{1-s}]$$

$$\leq Tr[A] + Tr[\Delta_-] - Tr[A]$$

$$= Tr[\Delta_-]$$ end of proof

We can use this lemma to prove one part of the q. Chernoff bound

Pick $A = \lambda\rho^{\otimes n}$ & $B = (1-\lambda)\sigma^{\otimes n}$ to find that

$$
\begin{aligned}
&p^*_{err}(\lambda, \rho^{\otimes n}, \sigma^{\otimes n}) \\
&= \frac{1}{2}\left(1 - \|\lambda\rho^{\otimes n} - (1-\lambda)\sigma^{\otimes n}\|_1\right) \\
&\leq \mathrm{Tr}\left[(\lambda\rho^{\otimes n})^s \left((1-\lambda)\sigma^{\otimes n}\right)^{1-s}\right] \\
&= \lambda^s(1-\lambda)^{1-s} \; \mathrm{Tr}\left[(\rho^s)^{\otimes n}(\sigma^{1-s})^{\otimes n}\right] \\
&= \lambda^s(1-\lambda)^{1-s} \left(\mathrm{Tr}[\rho^s\sigma^{1-s}]\right)^n \\
&\leq \left(\mathrm{Tr}[\rho^s\sigma^{1-s}]\right)^n \quad \forall s \in (0,1)
\end{aligned}
$$

Take $-\log$, divide by n, to get

$$
\frac{-\log p^*_{err}}{n} \geq -\log \mathrm{Tr}[\rho^s\sigma^{1-s}] \quad \forall s \in (0,1)
$$

$$\Rightarrow \lim_{n\to\infty} \frac{1}{n}\left(-\log p_{err}^{*}\right) \geq C(\rho\|\sigma)$$

For the other inequality, see the book.

Now consider asymmetric setting of hypothesis testing