Notes on asymptotics of quantum hypothesis testing

Anna Jenčová*

1 Preliminaries

Let $\mathcal{H}$ be a finite dimensional Hilbert space.

1.1 Pinching

Let $A \in B(\mathcal{H})$ be self-djoint, with spectral decomposition $A = \sum_i \lambda_i P_i$. We will need the pinching map $B(\mathcal{H}) \to B(\mathcal{H})$, defined as

$$\mathcal{E}_A(X) = \sum_i P_i X P_i.$$

Then A is a cp unital map. Moreover, $\mathcal{E}_A(X)$ commutes with X and we have the pinching inequality [**?**]

$$\mathcal{E}_A(X) \leq |\mathrm{spec}(A)| X, \qquad X \geq 0. \tag{1}$$

1.2 Relative entropies

Let ρ and σ be density operators. The (Umegaki) relative entropy is defined as

$$D(\rho\|\sigma) := \begin{cases} \mathrm{Tr}\,[\rho(\log\rho - \log\sigma)], & \mathrm{supp}(\rho) \leq \mathrm{supp}(\sigma) \\ \infty, & \text{otherwise.} \end{cases}$$

The standard Rényi relative entropy for $\alpha \in [0,1] \setminus \{1\}$ is defined as

$$D_\alpha(\rho\|\sigma) := \begin{cases} \dfrac{1}{\alpha-1} \log \mathrm{Tr}\,[\rho^\alpha \sigma^{1-\alpha}], & \mathrm{supp}(\rho) \leq \mathrm{supp}(\sigma) \text{ or } \alpha \in (0,1) \\ \infty, & \text{otherwise.} \end{cases}$$

The sandwiched Rényi relative entropy for $\alpha \in [1/2, \infty] \setminus \{1\}$ is defined as

$$\hat{D}_\alpha(\rho\|\sigma) := \begin{cases} \dfrac{1}{\alpha-1} \log \mathrm{Tr}\,[\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}], & \mathrm{supp}(\rho) \leq \mathrm{supp}(\sigma) \text{ or } \alpha \in [1/2, 1) \\ \infty, & \text{otherwise.} \end{cases}$$

*Mathematical Institute, Slovak Academy of Sciences, Štefánikova 49, 814 73 Bratislava, Slovakia, jenca@mat.savba.sk

1.3 The function ϕ

We assume $\mathrm{supp}(\rho) \leq \mathrm{supp}(\sigma)$**, so that** $D(\rho\|\sigma) < \infty$**.**

Let us define

$$\phi(s) = \log \mathrm{Tr}\,[\rho^{1-s}\sigma^s], \qquad s \in \mathbb{R}.$$

Then ϕ is a convex and smooth function, with derivative

$$\phi'(s) = (\mathrm{Tr}\,[\rho^{1-s}\sigma^s])^{-1}\mathrm{Tr}\,[\rho^{1-s}\sigma^s(\log\sigma - \log\rho),$$

[**?** , Exercise 3.5] In particular, $\phi'(0) = -D(\rho\|\sigma)$ and $\phi'(1) = D(\sigma\|\rho)$.

Lemma 1. *Put*

$$\psi(\lambda) = \inf_{s\in[0,1]} \lambda s + \phi(s), \qquad \lambda \in \mathbb{R}.$$

Then

$$\psi(\lambda) = \begin{cases} 0 & \lambda \geq -\phi'(0) = D(\rho\|\sigma) \\ < 0 & \lambda < D(\rho\|\sigma) \\ \lambda & \lambda \leq -\phi'(1) = -D(\sigma\|\rho). \end{cases}$$

Proof. By convexity, the derivative $\phi'(s)$ is nondecreasing. It follows that if $\lambda \geq -\phi'(0)$, then

$$\frac{d}{ds}(\lambda s + \phi(s)) = \lambda + \phi'(s) \geq -\phi'(0) + \phi'(s) \geq 0,$$

so that the function $s \mapsto \lambda s + \phi(s)$ is nondecreasing, so that the infimum is attained at $s = 0$. Similarly, if $\lambda \leq -\phi'(1)$, then the infimum is attained at $s = 1$ and hence $\psi(\lambda) = \lambda$. Let now $\lambda < -\phi'(0)$, then we see that the function $s \mapsto \lambda s + \phi(s)$ is strictly decreasing at $s = 0$, so that we must have $\psi(\lambda) < 0$.

□

We define

$$\psi^*(\lambda) = \inf_{t\in[-1,0]} t\lambda + \phi(t).$$

Again, if $\lambda > D(\rho\|\sigma) = -\phi'(0)$, then $t \mapsto t\lambda + \phi(t)$ is strictly increasing at $t = 0$, which implies that $\phi^*(\lambda) < 0$.

1.4 Inequalities

We have two basic inequalities. For $A, B \geq 0$, let $\{A \geq B\}$ be the sum of eigenprojections of $A - B$ corresponding to nonnegative eigenvalues, similarly $\{A \leq B\}$, $\{A > B\}$ etc. Then

Lemma 2 (Quantum Neyman-Pearson)**.** *We have*

$$\min_{0\leq T\leq I} \mathrm{Tr}\,[A(I-T)] + \mathrm{Tr}\,[BT] = \mathrm{Tr}\,[A\{A \leq B\}] + \mathrm{Tr}\,[B\{A > B\}].$$

Lemma 3 (Audenaert et al)**.** *We have for any* $s \in [0,1]$*,*

$$\mathrm{Tr}\,[A\{A \leq B\}] + \mathrm{Tr}\,[B\{A > B\}] \leq \mathrm{Tr}\,[A^{1-s}B^s].$$

These statements hold in the von Neumann algebra case as well.

2 QHT

Let ρ, σ be a pair of density matrices. We test the hypothesis $H_0 = \rho$ against the alternative $H_1 = \sigma$. A test is given by an operator $0 \le T \le I$, corresponding to accepring H_0. The two error probabilities are

$$\alpha(T) = \mathrm{Tr}\,[(I-T)\rho], \qquad \beta(T) = \mathrm{Tr}\,[T\sigma].$$

We will consider the asymptotic behaviour of the error probabilities

$$\alpha_n(T_n) = \mathrm{Tr}\,[(I-T_n)\rho_n], \qquad \beta_n(T_n) = \mathrm{Tr}\,[T_n\sigma_n]$$

in testing $H_0 = \rho_n := \rho^{\otimes n}$ against $H_1 = \sigma_n := \sigma^{\otimes n}$.

2.1 Quantum Stein's lemma

We assume $\mathrm{supp}(\rho) \le \mathrm{supp}(\sigma)$**, so that** $D(\rho\|\sigma) < \infty$**.**

Let $\lambda \in \mathbb{R}$ and let $S_n := \{\rho^{\otimes n} > e^{n\lambda}\sigma^{\otimes n}\}$. Then using Lemma 3 (Audenaert) with $A = \rho^{\otimes n}$ and $B = e^{\lambda n}\sigma^{\otimes n}$, we get for any $s \in [0,1]$

$$\alpha_n(S_n) + e^{n\lambda}\beta_n(S_n) \le \mathrm{Tr}\, e^{n\lambda s}[(\rho^{\otimes n})^{1-s}(\sigma^{\otimes n})^s] = e^{n\lambda s}(\mathrm{Tr}\,[\rho^{1-s}\sigma^s])^n = e^{n(\lambda s + \phi(s))}. \tag{2}$$

Hence by taking the infimum over $s \in [0,1]$,

$$\alpha_n(S_n) \le e^{n\psi(\lambda)}, \qquad \beta_n(S_n) \le e^{n(-\lambda+\psi(\lambda))} \tag{3}$$

On the other hand, put $p_n = \mathrm{Tr}\,[\rho^{\otimes n}S_n]$ and $q_n = \mathrm{Tr}\,[\sigma^{\otimes n}S_n]$. Then $p_n \ge e^{n\lambda}q_n$ and therefore $p_n^t \le e^{n\lambda t}q_n^t$ for for any $t \in [-1,0]$. We get

$$\begin{aligned} 1 - \alpha_n(S_n) &= p_n \le e^{n\lambda t}p_n^{1-t}q_n^t \le e^{n\lambda t}(p_n^{1-t}q_n^t + (1-p_n)^{1-t}(1-q_n)^t) \le e^{n\lambda t}\mathrm{Tr}\,[(\rho^{\otimes n})^{1-t}(\sigma^{\otimes n})^t] \\ &= e^{n(\lambda t + \phi(t))} \end{aligned}$$

for all $t \in [-1,0]$. It follows that for any test T_n, we have

$$\begin{aligned} 1 - \alpha_n(T_n) &= \mathrm{Tr}\,[\rho^{\otimes n}T_n] = \mathrm{Tr}\,[(\rho^{\otimes n} - e^{\lambda n}\sigma^{\otimes n})T_n] + e^{\lambda n}\beta_n(T_n) \le \mathrm{Tr}\,[(\rho^{\otimes n} - e^{\lambda n}\sigma^{\otimes n})S_n] + e^{\lambda n}\beta_n(T_n) \\ &\le 1 - \alpha_n(S_n) + e^{\lambda n}\beta_n(T_n) \le e^{n(\lambda t + \phi(t))} + e^{\lambda n}\beta_n(T_n) \end{aligned}$$

and hence

$$\beta_n(T_n) \ge e^{-n\lambda}(1 - \alpha_n(T_n) - e^{n\psi^*(\lambda)}) \tag{4}$$

Lemma 4 (Quantum Stein's lemma)**.** *[**? ?**] For all $\epsilon \in (0,1)$, we have*

$$\lim_{n\to\infty} -\frac{1}{n}\log\beta_n(\epsilon) = D(\rho\|\sigma).$$

Proof. Let $\lambda < D(\rho\|\sigma)$, then by Lemma 1, $\psi(\lambda) < 0$, so that in this case (3), $\alpha_n(S_n) \to 0$ and

$$-\frac{1}{n}\log\beta_n(S_n) \ge \lambda - \psi(\lambda) > \lambda.$$

For $\epsilon \in (0,1)$ we have $\alpha_n(S_n) \le \epsilon$ for large enough n, so that $\beta_n(\epsilon) \le \beta_n(S_n)$. It follows that

$$\liminf_n -\frac{1}{n}\log\beta_n(\epsilon) \ge -\frac{1}{n}\log\beta_n(S_n) \ge \lambda.$$

Conversely, by (4) we have for any sequence of tests such that $\alpha_n(T_n) \leq \epsilon$ that

$$\beta_n(T_n) \geq e^{-n\lambda}(1 - \epsilon - e^{n\psi^*(\lambda)}).$$

Since $\psi^*(\lambda) < 0$ for $\lambda > D(\rho\|\sigma)$, this implies that, for such λ,

$$\limsup_n -\frac{1}{n}\beta_n(\epsilon) \leq \lambda.$$

Chooseng any $\delta > 0$, we obtain

$$D(\rho\|\sigma) - \delta \leq \liminf_n -\frac{1}{n}\beta_n(\epsilon) \leq \limsup_n -\frac{1}{n}\beta_n(\epsilon) \leq D(\rho\|\sigma) + \delta.$$

Since δ was arbitrary, this implies the statement.

$\square$

The following quantum Stein's lemma describes the situation when the error of the first kind is constrained by some $\epsilon > 0$. In this case, the optimal value of the second kind error

$$\beta_n(\epsilon) := \min_{0 \leq T_n \leq I} \{\beta_n(T_n) \mid \alpha_n(T_n) \leq \epsilon\}, \qquad \epsilon > 0$$

converges to zero exponetially fast, that is, $\beta_n(\epsilon) \sim e^{-nr}$. The lemma shows that for any $\epsilon > 0$, the error exponent r is given by the relative entropy