Recoverability of quantum channels via hypothesis testing

Anna Jenčová

Mathematical Institute, Slovak Academy of Sciences, Bratislava, Slovakia

ILAS 2023

Recoverability

Recoverability = possibility to reverse the action of a quantum channel on a set of states

- exactly (sufficiency, reversibility) or approximately
- characterized by preservation (or decrease) of some important quantities of quantum information theory.

This talk: quantities related to hypothesis testing

Quantum relative entropy

$\mathcal{H}$ a Hilbert space, $\mathcal{T}(\mathcal{H})$ trace class, $\mathcal{S}(\mathcal{H})$ density operators

Relative entropy: For $\rho, \sigma \in \mathcal{S}(\mathcal{H})$

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

Data processing inequality (DPI)

$$D(\Phi(\rho)\|\Phi(\sigma)) \leq D(\rho\|\sigma)$$

for any quantum channel $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ (CPTP map)

Equality in DPI

Theorem (Petz, 1986, 1988)

Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, $D(\rho\|\sigma) < \infty$. Then

$$D(\Phi(\rho)\|\Phi(\sigma)) = D(\rho\|\sigma)$$

if and only if there is a recovery channel Ψ:

$$\Psi \circ \Phi(\rho) = \rho, \qquad \Psi \circ \Phi(\sigma) = \sigma.$$

In this case, Φ is sufficient for $\{\rho, \sigma\}$ (related to classical sufficient statistics).

Universal recovery channel

- Petz recovery map: $\Phi_\sigma : \mathcal{T}(\mathrm{supp}(\Phi(\sigma))) \to \mathcal{T}(\mathcal{H})$,

$$\Phi_\sigma(\cdot) = \sigma^{1/2}\Phi^*(\Phi(\sigma)^{-1/2} \cdot \Phi(\sigma)^{-1/2})\sigma^{1/2}$$

- Φ_σ is a channel, $\Phi_\sigma \circ \Phi(\sigma) = \sigma$.

Theorem (Petz, 1986, 1988)

Let $\rho \in \mathcal{S}(\mathcal{H})$, $D(\rho\|\sigma) < \infty$. We have

$$D(\Phi(\rho)\|\Phi(\sigma)) = D(\rho\|\sigma) \iff \Phi_\sigma \circ \Phi(\rho) = \rho.$$

Structure of sufficient channels

Assume that σ is faithful ($\mathrm{supp}(\sigma) = I$).

- The set

$$\mathcal{C} = \{\Psi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H}) \text{ channel}, \; \Psi(\rho) = \rho, \Psi(\sigma) = \sigma\}$$

  is a convex, closed semigroup.

- By mean ergodic theorem: there is some $E \in \mathcal{C}$, such that

$$E \circ \Phi = \Phi \circ E = E, \qquad \forall \Phi \in \mathcal{C}.$$

- The adjoint E^* is a conditional expectation on $B(\mathcal{H})$: the range of E^* is a subalgebra and we have

$$E^*(E^*(X)YE^*(Z)) = E^*(X)E^*(Y)E^*(Z), \quad X, Y, Z \in B(\mathcal{H}).$$

Luczak, 2014

Structure of sufficient channels

$\mathcal{M}_{\rho,\sigma} := E^*(B(\mathcal{H}))$ is the minimal sufficient subalgebra

There are (up to a unitary):

- a decomposition $\mathcal{H} = \bigoplus_n \mathcal{H}_n^L \otimes \mathcal{H}_n^R$ such that

$$\mathcal{M}_{\rho,\sigma} = \bigoplus_n B(\mathcal{H}_n^L) \otimes I_{\mathcal{H}_n^R},$$

- states $\sigma_n^R \in \mathcal{S}(\mathcal{H}_n^R)$, $\sigma_n^L, \rho_n^L \in \mathcal{S}(\mathcal{H}_n^L)$ and (discrete) probability distributions $p = \{p_n\}$, $q = \{q_n\}$ such that

$$\rho = \bigoplus_n p_n(\rho_n^L \otimes \sigma_n^R), \qquad \sigma = \bigoplus_n q_n(\sigma_n^L \otimes \sigma_n^R)$$

- the pair $\{p, q\}$ the classical part of $\{\rho, \sigma\}$.

Structure of sufficient channels

Theorem

Φ is sufficient with respect to $\{\rho, \sigma\}$ if and only if

- $\mathcal{M}_{\rho,\sigma} \simeq \mathcal{M}_{\Phi(\rho),\Phi(\sigma)}$
- the restriction $\Phi^*|_{\mathcal{M}_{\Phi(\rho),\Phi(\sigma)}}$ is an isomorphism onto $\mathcal{M}_{\rho,\sigma}$.

In that case, for any recovery channel Ψ,

$$\Psi^*|_{\mathcal{M}_{\rho,\sigma}} = (\Phi^*|_{\mathcal{M}_{\Phi(\rho),\Phi(\sigma)}})^{-1}.$$

This is a strong condition on the structure of the channel.

Recoverability (approximate version)

Theorem (Fawzi, Renner 2015; Wilde 2015; Junge et al. 2018)

There exists a channel $\Phi_\sigma^u : \mathcal{T}(\mathcal{K}) \to \mathcal{T}(\mathcal{H})$ such that $\Phi_\sigma^u \circ \Phi(\sigma) = \sigma$ and for any $\rho \in \mathcal{S}(\mathcal{H})$,

$$\begin{aligned} D(\rho\|\sigma) &\geq D(\Phi(\rho)\|\Phi(\sigma)) - 2\log F(\rho, \Phi_\sigma^u \circ \Phi(\rho)) \\ &\geq D(\Phi(\rho)\|\Phi(\sigma)) + \frac{1}{4}\|\rho - \Phi_\sigma^u \circ \Phi(\rho)\|_1^2. \end{aligned}$$

The universal recovery channel Φ_σ^u can be chosen as

$$\Phi_\sigma^u(\cdot) = \int_{-\infty}^{\infty} \sigma^{-it}\Phi_\sigma(\Phi(\sigma)^{it} \cdot \Phi(\sigma)^{-it})\sigma^{it} \frac{\pi}{\cosh(2\pi t) + 1} dt.$$

Other characterization of sufficiency (recoverability)

Equality in DPI and recoverability were studied for other quantities:

- standard f-divergences
- max (min) f-divergences
- optimized f-divergences
- standard (Petz) Rényi divergences
- sandwiched Rényi divergences
- quantum Fisher information

We are interested in quantities related to quantum hypothesis testing (state discrimination).

AJ, Petz 2006; Hiai et al. 2010; AJ 2012; Luczak 2014; Hiai, Mosonyi 2016; AJ 2018; Carlen, Vershynina 2020; Gao, Wilde 2020; Hiai 2021, Gao et al 2023,...

Quantum hypothesis testing

Suppose $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ are given, one of them is the true state:

- we test the hypothesis $H_0 = \sigma$ against $H_1 = \rho$
- a test: an effect $0 \leq T \leq I$,

$$\mathrm{Tr}\,[T\omega] - \text{probability of rejecting } H_0 \text{ in the state } \omega$$

- error probabilities:

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

- Bayes error probabilities for $\lambda \in [0, 1]$:

$$P_e(\lambda, \sigma, \rho, T) := \lambda\alpha(T) + (1 - \lambda)\beta(T)$$

Quantum Neyman-Pearson lemma

Put $P_{s,\pm} := \mathrm{supp}((\rho - s\sigma)_\pm)$, $P_{s,0} := I - P_{s,+} - P_{s,-}$.

A test T is Bayes optimal for $\lambda \in (0,1)$ if and only if

$$T = P_{s,+} + X, \quad 0 \le X \le P_{s,0}, \qquad s = \frac{\lambda}{1-\lambda}$$

and then

$$\begin{aligned} P_e(\lambda, \sigma, \rho) &:= \min_{0 \le T \le I} P_e(\lambda, \sigma, \rho, T) \\ &= (1-\lambda)(1 - \mathrm{Tr}\left[(\rho - s\sigma)_+\right]) \\ &= (1-\lambda)(s - \mathrm{Tr}\left[(\rho - s\sigma)_-\right]) \\ &= \frac{1}{2}(1 - (1-\lambda)\|\rho - s\sigma\|_1). \end{aligned}$$

Data processing inequalities

We clearly have for any quantum channel Φ and $\lambda \in [0, 1]$:

$$P_e(\lambda, \Phi(\sigma), \Phi(\rho)) \geq P_e(\lambda, \sigma, \rho),$$

or equivalently, for any $s \in \mathbb{R}$:

$$\|\Phi(\rho) - s\Phi(\sigma)\|_1 \leq \|\rho - s\sigma\|_1;$$

$$\mathrm{Tr}\left[(\Phi(\rho) - s\Phi(\sigma))_+\right] \leq \mathrm{Tr}\left[(\rho - s\sigma)_+\right];$$

$$\mathrm{Tr}\left[(\Phi(\rho) - s\Phi(\sigma))_-\right] \leq \mathrm{Tr}\left[(\rho - s\sigma)_-\right].$$

Equality in DPI

The following are equivalent:

- $P_e(\lambda, \Phi(\sigma), \Phi(\rho)) = P_e(\lambda, \sigma, \rho)$, $\lambda \in [0, 1]$;
- $\|\Phi(\rho) - s\Phi(\sigma)\|_1 = \|\rho - s\sigma\|_1$, $s \in \mathbb{R}$;
- $\mathrm{Tr}\left[(\Phi(\rho) - s\Phi(\sigma))_+\right] = \mathrm{Tr}\left[(\rho - s\sigma)_+\right]$, $s \in \mathbb{R}$;
- $\mathrm{Tr}\left[(\Phi(\rho) - s\Phi(\sigma))_-\right] = \mathrm{Tr}\left[(\rho - s\sigma)_-\right]$, $s \in \mathbb{R}$;
- $\Phi^*(Q_{s,+}) = P_{s,+}$, $s \in \mathbb{R}$;
- $\Phi^*(Q_{s,-}) = P_{s,-}$, $s \in \mathbb{R}$.

$$(\ Q_{s,\pm} = \mathrm{supp}((\Phi(\rho) - s\Phi(\sigma))_\pm))$$

- sufficiency/recoverability?

Previous results on equality in DPI

More assumptions are needed:

- equality in DPI for all pairs in a larger set of states,
- or for $\Phi^{\otimes n}$, $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, for all $n \in \mathbb{N}$,
- Φ has commutative range.

For the asymptotic case (quantities related to error exponents):

- equality in DPI for Chernoff or Hoeffding distances implies sufficiency of the channel

Recoverability (approximate case): no results

Blume-Kohout et al., 2010; Ticozzi & Viola, 2010; AJ, 2010, 2012; Luczak, 2015

An integral formula for relative entropy

Theorem (Frenkel, arxiv:2208.12194)

For any $\rho, \sigma \in \mathcal{S}(\mathcal{H})$:

$$D(\rho\|\sigma) = \int_{-\infty}^{\infty} \frac{dt}{|t|(1-t)^2} \operatorname{Tr}\left[((1-t)\rho + t\sigma)_-\right]$$

- proved for $\dim(\mathcal{H}) < \infty$
- extends to infinite dimensions.

An integral formula for relative entropy

A slight reformulation:

For $\mu, \lambda \geq 0$ such that $\mu\sigma \leq \rho \leq \lambda\sigma$:

$$D(\rho\|\sigma) = \int_{\mu}^{\lambda} \frac{ds}{s} \operatorname{Tr}\left[(\rho - s\sigma)_{-}\right] + \log(\lambda) + 1 - \lambda$$

- we may always put $\mu = 0$,
- if $\dim(\mathcal{H}) < \infty$: if such λ does not exist, then $D(\rho\|\sigma) = \infty$,
- in general:

$$D(\rho\|\sigma) = \lim_{\lambda \searrow 0} D(\rho\|\lambda\rho + (1-\lambda)\sigma)$$

Sufficient channels via hypothesis testing

Theorem

Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ be any states, $\sigma_0 = \frac{1}{2}(\rho + \sigma)$, Φ a channel.

The following are equivalent:

- $P_e(\lambda, \Phi(\sigma), \Phi(\rho)) = P_e(\lambda, \sigma, \rho)$, $\lambda \in [0, 1]$;
- $\|\Phi(\rho) - s\Phi(\sigma)\|_1 = \|\rho - s\sigma\|_1$, $s \in \mathbb{R}$;
- $D(\rho\|\sigma_0) = D(\Phi(\rho), \Phi(\sigma_0))$;
- $\Phi^u_{\sigma_0} \circ \Phi(\rho) = \rho$;
- Φ is sufficient with respect to $\{\rho, \sigma\}$.

Recoverability via hypothesis testing

We will need a further assumption on ρ, σ:

$$D_H(\rho\|\sigma) := \inf\{\frac{\lambda}{\mu},\ \lambda, \mu > 0, \mu\sigma \leq \rho \leq \lambda\sigma\} < \infty$$

- D_H is the Hilbert projective metric,
- $D_H(\rho\|\sigma) = D_{\max}(\rho\|\sigma) + D_{\max}(\sigma\|\rho)$,
- if $\dim(\mathcal{H}) < \infty$, the assumption is equivalent to

$$\mathrm{supp}(\rho) = \mathrm{supp}(\sigma),$$

- if $\dim(\mathcal{H}) = \infty$: a much stronger assumption.

Recoverability via hypothesis testing

Theorem

Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, Φ a channel. If there is some $\epsilon \geq 0$ such that

$$\|\Phi(\rho) - s\Phi(\sigma)\|_1 \geq \|\rho - s\sigma\|_1 - \epsilon, \qquad \forall s \geq 0,$$

then

$$\|\Phi_\sigma^u \circ \Phi(\rho) - \rho\|_1 \leq \sqrt{2\epsilon} D_H(\rho, \sigma)^{1/2}.$$

Compatible channels

The channels

$$\Phi_1 : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K}_1), \qquad \Phi_2 : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K}_2)$$

are compatible if there is a joint channel

$$\Lambda : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K}_1 \otimes \mathcal{K}_2)$$

such that

$$\Phi_1 = \mathrm{Tr}_{\mathcal{K}_2} \circ \Lambda, \qquad \Phi_2 = \mathrm{Tr}_{\mathcal{K}_1} \circ \Lambda.$$

Sufficiency and compatibility of channels

Theorem

Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ with $\{p, q\}$ - the classical part of $\{\rho, \sigma\}$.

- If Φ_1 and Φ_2 are compatible channels and Φ_1 is sufficient for $\{\rho, \sigma\}$, then there are some states τ_n such that

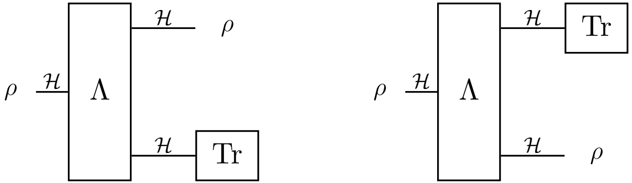
$$\Phi_2(\rho) = \sum_n p_n \tau_n, \qquad \Phi_2(\sigma) = \sum_n q_n \tau_n.$$

- If the above condition holds for any channel compatible with Φ_1, then Φ_1 is sufficient for $\{\rho, \sigma\}$.

cf. Kaniowski et al, 2015; Kuramochi, 2018

Broadcasting

A broadcasting channel: for $\rho \in \mathcal{S}(\mathcal{H})$



- no-broadcasting:

$$\mathrm{Tr}_2 \circ \Lambda(\rho) = \mathrm{Tr}_1 \circ \Lambda(\rho) = \rho \text{ for all } \rho \text{ is impossible}$$

- restricted to $\rho \in \mathcal{S} \subset \mathcal{S}(\mathcal{H})$:

$$\text{broadcasting is possible} \iff \mathcal{S} \text{ is commutative.}$$

Broadcasting and distinguishability

Put $\mathcal{S} = \{\rho, \sigma\}$ and require that for all $\lambda \in [0,1]$,

$$\begin{aligned} P_e(\lambda, \mathrm{Tr}_1 \circ \Lambda(\rho), \mathrm{Tr}_1 \circ \Lambda(\sigma)) &= P_e(\lambda, \mathrm{Tr}_2 \circ \Lambda(\rho), \mathrm{Tr}_2 \circ \Lambda(\sigma)) \\ &= P_e(\lambda, \rho, \sigma). \end{aligned}$$

- possible only if ρ and σ commute
- If $P_e(\lambda, \mathrm{Tr}_2 \circ \Lambda(\rho), \mathrm{Tr}_2 \circ \Lambda(\sigma)) = P_e(\lambda, \rho, \sigma)$ for all λ, then

  $$P_e(\lambda, \mathrm{Tr}_1 \circ \Lambda(\rho), \mathrm{Tr}_1 \circ \Lambda(\sigma)) \geq P_e(\lambda, p, q), \quad \forall \lambda \in [0,1],$$

  $\{p, q\}$ is the classical part of $\{\rho, \sigma\}$.