

On Composite Quantum Hypothesis Testing

Mario Berta (Department of Computing)

with Fernando Brandão and Christoph Hirche – arXiv:1709.07268

Overview

- 1 Introduction
 - 2 Composite Hypothesis Testing
 - 3 Proof Idea
 - 4 Examples
 - 5 Conclusion
-

Introduction: Hypothesis Testing

- Discriminate between two sequences of quantum states ρ_n, σ_n on $\mathcal{H}^{\otimes n}$ – **null and alternative hypothesis** – with two outcome POVM $\{M_n, (1 - M_n)\}$. M_n is associated with accepting ρ_n and $(1 - M_n)$ with accepting σ_n .
- This leads to **two types of errors**

$$\alpha_n(M_n) := \text{Tr} [\rho_n(1 - M_n)] \text{ Type 1 error} \quad \beta_n(M_n) := \text{Tr} [\sigma_n M_n] \text{ Type 2 error.}$$

- Symmetric setting for $\rho_n = \rho^{\otimes n}, \sigma_n = \sigma^{\otimes n}$ with

$$\xi_n(\rho, \sigma) := \inf_{0 \leq M_n \leq 1} \frac{\alpha_n(M_n)}{2} + \frac{\beta_n(M_n)}{2}$$

leads to

Quantum Chernoff bound [Audenaert *et al.*, PRL 07]

$$\xi(\rho, \sigma) := \lim_{n \rightarrow \infty} -\frac{\log \xi_n(\rho, \sigma)}{n} = -\log \min_{0 \leq s \leq 1} \text{Tr} [\rho^s \sigma^{1-s}].$$

Introduction: Asymmetric Hypothesis Testing

- Same two type of errors $\alpha_n(M_n), \beta_n(M_n)$ and $\rho_n = \rho^{\otimes n}, \sigma_n = \sigma^{\otimes n}$ but **asymmetric** setting with

$$\beta_\varepsilon^n(\rho, \sigma) := \inf_{0 \leq M_n \leq 1} \{ \beta_n(M_n) \mid \alpha_n(M_n) \leq \varepsilon \}.$$

leads to **asymptotic error exponent**

Quantum Stein's lemma [Hiai and Petz, CMP 91]

$$\beta(\rho, \sigma) := \lim_{\substack{n \rightarrow \infty \\ \varepsilon \rightarrow 0}} - \frac{\log \beta_\varepsilon^n(\rho, \sigma)}{n} = D(\rho \parallel \sigma) := \text{Tr} [\rho (\log \rho - \log \sigma)].$$

- **Note:** this led to the definition of the **quantum relative entropy** $D(\rho \parallel \sigma)$.
- **Motivation:** fundamental task in **quantum statistics** + underlying technical core problem for many applications in QIT as, e.g., quantum channel coding, quantum illumination, quantum reading, etc. [very many references].

Composite Hypothesis Testing: Setup

- **Composite** null and alternative hypotheses

$$\mathcal{S}_n := \left\{ \underbrace{\int \rho^{\otimes n} d\nu}_{=: \rho_n(\nu)} \mid \rho \in \mathcal{S} \right\} \quad \text{vs.} \quad \mathcal{T}_n := \left\{ \underbrace{\int \sigma^{\otimes n} d\mu}_{=: \sigma_n(\mu)} \mid \sigma \in \mathcal{T} \right\}$$

with \mathcal{S}, \mathcal{T} sets of quantum states and ν, μ measures on \mathcal{S}, \mathcal{T} , resp.

- For the **asymmetric setting** we define

$$\beta_\varepsilon^n(\mathcal{S}, \mathcal{T}) := \inf_{0 \leq M_n \leq 1} \left\{ \underbrace{\sup_{\mu \in \mathcal{T}} \text{Tr} [M_n \sigma_n(\mu)]}_{=: \beta_n(M_n)} \mid \underbrace{\sup_{\nu \in \mathcal{S}} \text{Tr} [(1 - M_n) \rho_n(\nu)]}_{=: \alpha_n(M_n)} \leq \varepsilon \right\}.$$

- This leads to the definition of the **composite asymptotic error exponent**

$$\beta(\mathcal{S}, \mathcal{T}) := \lim_{\substack{n \rightarrow \infty \\ \varepsilon \rightarrow 0}} - \frac{\log \beta_\varepsilon^n(\mathcal{S}, \mathcal{T})}{n}.$$

Composite Hypothesis Testing: Classical Case

- If all involved quantum states pairwise commute (**classical setting** – probability distributions P, Q) we have

Composite Stein's lemma [Levitin and Merhav, IEEE 02]

$$\beta(S, \mathcal{T}) = \inf_{P \in S} \inf_{Q \in \mathcal{T}} \beta(P, Q) = \inf_{P \in S} \inf_{Q \in \mathcal{T}} D(P \| Q) \text{ with Kulback-Leibler divergence.}$$

- **Question:** does this hold in the general non-commutative case as well? Yes, if $\mathcal{T} = \{\sigma\}$, i.e., only composite null hypothesis [Hayashi, JPA 02].
- Some related cases are understood as well [Brandão and Plenio, CMP 10] + [Hayashi and Tomamichel, JMP 16]. However, the general case remained open – see also [Bjelaković *et al.*, CMP 05].
- **Motivation:** fundamental task in **quantum statistics**, composite version of applications in QIT (e.g., network quantum Shannon theory).

Composite Hypothesis Testing: Quantum Case

- Our main result is **regularized formula**

Composite quantum Stein's lemma [this talk]

$$\beta(\mathcal{S}, \mathcal{T}) = \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\substack{\rho \in \mathcal{S} \\ \mu \in \mathcal{T}}} D \left(\rho^{\otimes n} \left\| \int \sigma^{\otimes n} d\mu(\sigma) \right. \right) \neq \inf_{\substack{\rho \in \mathcal{S} \\ \sigma \in \mathcal{T}}} D(\rho \|\sigma) \text{ in general.}$$

- Hence, in general $D(\rho^{\otimes n} \|\int \sigma^{\otimes n} d\mu(\sigma)) \not\leq n \cdot \inf_{\sigma \in \mathcal{T}} D(\rho \|\sigma)$.
- **Converse:** $\beta(\mathcal{S}, \mathcal{T}) \leq \text{RHS}$ based on MONO of quantum relative entropy under quantum channels [Hiai and Petz, CMP 91].
- **Achievability:** $\beta(\mathcal{S}, \mathcal{T}) \geq \text{RHS}$ via
 - ① measure: post-measurement probability distributions
 - ② apply classical composite Stein's lemma
 - ③ mathematical properties of quantum entropy
- **Regularization:** examples + novel quantum entropy inequalities.

Proof Idea: Classical Strategy

$$\beta(\mathcal{S}, \mathcal{T}) := \lim_{\varepsilon \rightarrow 0} \lim_{n \rightarrow \infty} -\frac{\log \beta_{\varepsilon}^n(\mathcal{S}, \mathcal{T})}{n}$$

- For $n \in \mathbb{N}$, $\varepsilon \in (0, 1)$, and POVM \mathcal{N}_n with $P_n := \mathcal{N}_n(\rho^{\otimes n})$, $Q_n := \mathcal{N}_n(\sigma^{\otimes n})$ composite Stein's lemma for probability distributions gives achievability bound

$$-\log \beta_{\varepsilon}^n(\mathcal{S}, \mathcal{T}) \geq \inf_{\substack{\rho \in \mathcal{S} \\ \sigma \in \mathcal{T}}} D(\mathcal{N}_n(\rho^{\otimes n}) \| \mathcal{N}_n(\sigma^{\otimes n})) \geq \inf_{\substack{\nu \in \mathcal{S} \\ \mu \in \mathcal{T}}} D(\mathcal{N}_n(\rho_n(\nu)) \| \mathcal{N}_n(\sigma_n(\mu))).$$

- Optimizing over all POVM \mathcal{N}_n we find the **measured relative entropy** $D_{\mathcal{N}}(\rho \| \sigma)$ as introduced by [Donald, CMP 86]

$$\begin{aligned} -\frac{\log \beta_{\varepsilon}^n(\mathcal{S}, \mathcal{T})}{n} &\geq \frac{1}{n} \sup_{\mathcal{N}_n} \inf_{\substack{\nu \in \mathcal{S} \\ \mu \in \mathcal{T}}} D(\mathcal{N}_n(\rho_n(\nu)) \| \mathcal{N}_n(\sigma_n(\mu))) \\ &\stackrel{\text{minimax}}{=} \frac{1}{n} \inf_{\substack{\nu \in \mathcal{S} \\ \mu \in \mathcal{T}}} \sup_{\mathcal{N}_n} D(\mathcal{N}_n(\rho_n(\nu)) \| \mathcal{N}_n(\sigma_n(\mu))). \end{aligned}$$

$\underbrace{\hspace{15em}}_{=: D_{\mathcal{N}}(\rho_n(\nu) \| \sigma_n(\mu))}$

Proof Idea: Properties of Quantum Entropy

- Hence, so far we have

$$\beta(\mathcal{S}, \mathcal{T}) \geq \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\substack{\nu \in \mathcal{S} \\ \mu \in \mathcal{T}}} D_{\mathcal{N}}(\rho_n(\nu) \| \sigma_n(\mu))$$

and it remains to prove that asymptotically

$$\frac{1}{n} \inf_{\substack{\nu \in \mathcal{S} \\ \mu \in \mathcal{T}}} D_{\mathcal{N}}(\rho_n(\nu) \| \sigma_n(\mu)) \stackrel{(i)}{\geq} \frac{1}{n} \inf_{\substack{\nu \in \mathcal{S} \\ \mu \in \mathcal{T}}} D(\rho_n(\nu) \| \sigma_n(\mu)) \stackrel{(ii)}{\geq} \frac{1}{n} \inf_{\substack{\rho \in \mathcal{S} \\ \mu \in \mathcal{T}}} D(\rho^{\otimes n} \| \sigma_n(\mu)).$$

- Using **asymptotic spectral pinching** [Hayashi, JPA 02] + [Sutter *et al.*, CMP 17] it can be shown

$$D_{\mathcal{N}}(\rho \| \sigma) \geq D(\rho \| \sigma) - \log |\text{spec}(\sigma)| \quad \left(\text{MONO: } D_{\mathcal{N}}(\rho \| \sigma) \leq D(\rho \| \sigma) \right).$$

However, since $\sigma_n(\mu) = \int \sigma^{\otimes n} d\mu(\sigma)$ is permutation invariant, we have by **Schur-Weyl duality** $|\text{spec}(\sigma_n(\mu))| \leq \text{poly}(n)$ and step (i) follows.

- Step (ii) is deduced from the **quasi-convexity** of the von Neumann entropy. □

Composite quantum Stein's lemma [this talk]

$$\beta(\mathcal{S}, \mathcal{T}) = \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\substack{\rho \in \mathcal{S} \\ \mu \in \mathcal{T}}} D \left(\rho^{\otimes n} \left\| \int \sigma^{\otimes n} d\mu(\sigma) \right. \right) \neq \inf_{\substack{\rho \in \mathcal{S} \\ \sigma \in \mathcal{T}}} D(\rho \|\sigma) \text{ in general.}$$

- When do we get **single-letter formula**? From [Hayashi, JPA 02] we have

$$\beta(\mathcal{S}, \mathcal{T} = \{\sigma\}) = \inf_{\rho \in \mathcal{S}} D(\rho \|\sigma).$$

- An example for composite alternative hypotheses: **relative entropy of coherence** [Baumgratz *et al.*, PRL 14]

$$D_C(\rho) := \inf_{\sigma \in \mathcal{C}} D(\rho \|\sigma) \text{ for set of states } \mathcal{C} \text{ diagonal in a fixed basis } \{|c\rangle\}.$$

Examples: Relative Entropy of Coherence

- **Goal:** discrimination problem with asymptotic error exponent given by the relative entropy of coherence

$$D_{\mathcal{C}}(\rho) := \inf_{\sigma \in \mathcal{C}} D(\rho \parallel \sigma) \text{ for set of states } \mathcal{C} \text{ diagonal in a fixed basis } \{|c\rangle\}.$$

Null hypothesis: the fixed states $\rho^{\otimes n}$

Alternative hypothesis: convex sets of iid coherent states $\mathcal{C}_n := \left\{ \int \sigma^{\otimes n} d\mu(\sigma) \mid \sigma \in \mathcal{C} \right\}$

$$\beta(\{\rho\}, \mathcal{C}) = \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\mu \in \mathcal{C}} D\left(\rho^{\otimes n} \parallel \int \sigma^{\otimes n} d\mu(\sigma)\right) = D_{\mathcal{C}}(\rho).$$

- More examples possible, e.g., **quantum mutual information** for product state testing (cf. [Hayashi and Tomamichel, JMP 16]).

Examples: Regularization and Entropy Inequalities I

- **Goal:** give discrimination problem such that

$$\lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\substack{\rho \in \mathcal{S} \\ \mu \in \mathcal{T}}} D \left(\rho^{\otimes n} \left\| \int \sigma^{\otimes n} d\mu(\sigma) \right. \right) \neq \inf_{\substack{\rho \in \mathcal{S} \\ \sigma \in \mathcal{T}}} D(\rho \|\sigma)$$

- **Quantum Markov** testing (see also [Cooney et al., PRA 16])

Null hypothesis: the fixed state $\rho_{ABC}^{\otimes n}$

Alternative hypothesis: the convex sets of quantum Markov iid states

$$\mathcal{R}_n := \left\{ \int ((\mathcal{I}_A \otimes \mathcal{R}_{C \rightarrow BC})(\rho_{AC}))^{\otimes n} d\mu(\mathcal{R}) \right\} \text{ with } \mathcal{R}_{C \rightarrow BC} \text{ local quantum channels}$$

- For this example we claim that our formula **does not become single-letter**

$$\begin{aligned} \beta(\{\rho_{ABC}\}, \mathcal{R}) &= \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\mu \in \mathcal{R}} D \left(\rho_{ABC}^{\otimes n} \left\| \int ((\mathcal{I}_A \otimes \mathcal{R}_{C \rightarrow BC})(\rho_{AC}))^{\otimes n} d\mu(\mathcal{R}) \right. \right) \\ &\neq \inf_{\mathcal{R}} D(\rho_{ABC} \|\mathcal{R}_{C \rightarrow BC}(\rho_{AC})). \end{aligned}$$

Examples: Regularization and Entropy Inequalities II

$$\lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\mu \in \mathcal{R}} D \left(\rho_{ABC}^{\otimes n} \left\| \int ((\mathcal{I}_A \otimes \mathcal{R}_{C \rightarrow BC})(\rho_{AC}))^{\otimes n} d\mu(\mathcal{R}) \right. \right) \\ \not\geq \inf_{\mathcal{R}} D(\rho_{ABC} \| (\mathcal{I}_A \otimes \mathcal{R}_{C \rightarrow BC})(\rho_{AC})).$$

- We show improved lower bound on **quantum conditional mutual information (CQMI)** [Sutter *et al.*, CMP 17], relaxed to (see also [Brandão *et al.*, PRL 15])

$$I(A : B|C)_\rho := D(\rho_{ABC} \| \rho_A \otimes \rho_{BC}) - D(\rho_{AC} \| \rho_A \otimes \rho_C) \\ \geq \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\mu \in \mathcal{R}} D \left(\rho_{ABC}^{\otimes n} \left\| \int ((\mathcal{I}_A \otimes \mathcal{R}_{C \rightarrow BC})(\rho_{AC}))^{\otimes n} d\mu(\mathcal{R}) \right. \right).$$

- However, [Fazwi and Fawzi, arXiv 17] give explicit quantum state ρ_{ABC} with

$$I(A : B|C)_\rho \not\geq \inf_{\mathcal{R}} D(\rho_{ABC} \| (\mathcal{I}_A \otimes \mathcal{R}_{C \rightarrow BC})(\rho_{AC})). \quad \square$$

- **Note:** use of additive CQMI nicely allows to circumvent asymptotics.

Composite quantum Stein's lemma [this talk]

$$\beta(\mathcal{S}, \mathcal{T}) = \lim_{n \rightarrow \infty} \frac{1}{n} \inf_{\substack{\rho \in \mathcal{S} \\ \mu \in \mathcal{T}}} D \left(\rho^{\otimes n} \left\| \int \sigma^{\otimes n} d\mu(\sigma) \right. \right) \neq \inf_{\substack{\rho \in \mathcal{S} \\ \sigma \in \mathcal{T}}} D(\rho \parallel \sigma) \text{ in general.}$$

- **Single-letter examples** possible, even with refinements: Hoeffding bound, strong converse exponent, second-order expansion as in [Hayashi and Tomamichel, JMP 16] + [Tomamichel and Hayashi, arXiv 15].
- Symmetric setting: open question about **composite quantum Chernoff bound**

$$\xi(\rho, \sigma) = -\log \min_{0 \leq s \leq 1} \text{Tr} [\rho^s \sigma^{1-s}] \Rightarrow \xi(\mathcal{S}, \mathcal{T}) \stackrel{?}{=} \inf_{\substack{\rho \in \mathcal{S} \\ \sigma \in \mathcal{T}}} \xi(\rho, \sigma)$$

only known up to a factor of two [Audenaert and Mosonyi, JMP 14].

- Applications in QIT, e.g., **network quantum Shannon theory** [Qi *et al.*, arXiv 17]?

Extra: Entropy inequalities

CQMI bounds [Junge *et al.*, arXiv 15], [Sutter *et al.*, CMP 17], [this talk]

For any quantum state ρ_{ABC} the CQMI is lower bounded by the incomparable bounds

$$\begin{aligned} I(A : B|C)_\rho &\geq - \int \beta_0(t) \log \left\| \sqrt{\rho_{ABC}} \sqrt{\sigma_{ABC}^{[t]}} \right\|_1^2 dt \\ I(A : B|C)_\rho &\geq D_{\mathcal{N}} \left(\rho_{ABC} \left\| \int \beta_0(t) \sigma_{ABC}^{[t]} dt \right. \right) \\ I(A : B|C)_\rho &\geq \limsup_{n \rightarrow \infty} \frac{1}{n} D \left(\rho_{ABC}^{\otimes n} \left\| \int \beta_0(t) \left(\sigma_{ABC}^{[t]} \right)^{\otimes n} dt \right. \right), \end{aligned}$$

where $\beta_0(t) := \frac{\pi}{2} (\cosh(\pi t) + 1)^{-1}$ is a universal probability distribution and

$$\sigma_{ABC}^{[t]} := \left(\mathcal{I}_A \otimes R_{C \rightarrow BC}^{[t]} \right) (\rho_{AC}) \text{ with } R_{C \rightarrow BC}^{[t]}(\cdot) := \rho_{BC}^{\frac{1+it}{2}} \left(\rho_C^{\frac{-1-it}{2}} (\cdot) \rho_C^{\frac{-1+it}{2}} \right) \rho_{BC}^{\frac{1-it}{2}}$$

are rotated Petz local recovery quantum channels.