On a gap in the proof of the generalised quantum Stein's lemma and its consequences for the reversibility of quantum resources

Mario Berta

AWS Center for Quantum Computing
Imperial College London

Based on

- **On composite quantum hypothesis testing**

  B., Brandão, Hirche
  Communications in Mathematical Physics 385, 55 (2021)

- **On a gap in the proof of the generalised quantum Stein's lemma and its consequences for the reversibility of quantum resources**

  B., Brandão, Gour, Lami, Plenio, Regula, Tomamichel
  arXiv:2205.02813 (2022)

Outline

- Quantum hypothesis testing
- Quantum resource theories
- Asymptotic reversibility?
- Proof techniques
- Conclusion

Quantum hypothesis testing

Symmetric quantum hypothesis testing

- Two sequences ρ_n, σ_n on $H^{\otimes n}$, discriminate them with two outcome POVM $\{M_n, (1 - M_n)\}$
- Two types of errors:

$$\alpha^n(M_n) \coloneqq Tr[\rho_n(1 - M_n)] \text{ Type 1} \quad \text{and} \quad \beta^n(M_n) \coloneqq Tr[\sigma_n M_n] \text{ Type 2}$$

- Asymptotic independent and identically distributed (IID) for $\rho_n = \rho^{\otimes n}, \sigma_n = \sigma_n^{\otimes n}$
- Symmetric setting

$$\xi(\rho^{\otimes n}, \sigma^{\otimes n}) \coloneqq \inf_{0 \le M_n \le 1} \frac{\alpha^n(M_n)}{2} + \frac{\beta^n(M_n)}{2}$$

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

$$\xi(\rho, \sigma) \coloneqq \lim_{n \to \infty} -\frac{\log \xi(\rho^{\otimes}, \sigma^{\otimes n})}{n} = -\log \min_{0 \le s \le 1} Tr[\rho^s \sigma^{1-s}]$$

Asymmetric quantum hypothesis testing

- Asymptotic IID $\rho_n = \rho^{\otimes n}, \sigma_n = \sigma_n^{\otimes n}$ asymmetric setting

$$\beta_\varepsilon\left(\rho^{\otimes n}, \sigma^{\otimes n}\right) := \inf_{0 \leq M_n \leq 1} \{\beta^n(M_n) \colon \alpha^n(M_n) \leq \varepsilon\}$$

gives quantum Stein's lemma [Hiai & Petz, CMP 91]

$$\beta(\rho, \sigma) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} -\frac{\log \beta_\varepsilon\left(\rho^{\otimes n}, \sigma^{\otimes n}\right)}{n} = D(\rho || \sigma) := Tr[\rho(\log \rho - \log \sigma)]$$

- Fundamental tasks in quantum statistics, underlying much of quantum information theory
- What about composite hypotheses? That is,

$$\rho^{\otimes n} \text{ with } \rho \in T \qquad \text{versus} \qquad \sigma^{\otimes n} \text{ with } \sigma \in S?$$

Composite hypothesis testing

- Asymptotic IID $\rho^{\otimes n}$ with $\rho \in T$ verus $\sigma^{\otimes n}$ with $\sigma \in S$, asymmetric setting

$$\beta_\varepsilon(T^n, S^n) \coloneqq \inf_{0 \le M_n \le 1} \{\sup_{\sigma \in S} Tr\left[M_n \sigma^{\otimes n}\right] : \sup_{\rho \in T} Tr\left[(1 - M_n)\rho^{\otimes n}\right] \le \varepsilon\}$$

- Thought-after characterization

$$\beta(T, S) \coloneqq \lim_{\varepsilon \to 0} \lim_{n \to \infty} -\frac{\log \beta_\varepsilon(T^n, S^n)}{n} = ?$$

- For $\rho \in T, \sigma \in S$ pairwise commuting, composite Stein's lemma [Levitan & Merhav, IEEE 02]

$$\beta(T, S) = \inf_{P \in T} \inf_{Q \in S} \beta(P, Q) = \inf_{P \in T} \inf_{Q \in S} D_{KL}(P||Q) \text{ with } D_{KL}(P||Q) \coloneqq \sum_x p_x \log \frac{p_x}{q_x}$$

  for eigendistributions P, Q in common eigenbasis of ρ, σ

- What about fully quantum version?

Composite quantum hypothesis testing

- Partial results for special cases:

  [Hayashi, JPA 02], [Bjelaković *et al.*, CMP 05], [Brandão & Plenio, CMP 10], [Hayashi & Tomamichel, JMP 16], etc.

- Composite quantum Stein's lemma for T, S convex [B. et al., CMP 21]

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

  see also [Mosonyi *et al.*, arXiv 21], as one does not have the quantum entropy inequality

$$D\left(\rho^{\otimes n} \parallel \int \sigma^{\otimes n} d\mu(\sigma)\right) \ngeq n \cdot \inf_{\sigma\in S} D(\rho||\sigma)$$

- Nevertheless, various examples of interest do become single-letter anyway

Quantum resource theories

Resource theory of entanglement

- All also works for general resource theories (under suitable axiom set)
- Free states are separable states on $H_{AB} \coloneqq H_A \otimes H_B$, that is, convex hull of product states

$$S_{A:B} \coloneqq conv\{|\psi_A\rangle\langle\psi_A| \otimes |\phi\rangle\langle\phi|_B : |\psi\rangle_A \in H_A, |\phi\rangle_B \in H_B\}$$

+ all other states are entangled (i.e., resourceful)

- Unit is ebit $\Phi_{AB} \coloneqq |\Phi\rangle\langle\Phi|_{AB}$ with $|\Phi\rangle_{AB} \coloneqq \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
- Entanglement measure: $R_S(\rho_{AB}) \coloneqq \{s \geq 0: \frac{\rho_{AB}+s\sigma_{AB}}{1+s} \in S_{A:B}\}$ global resource robustness
- Free operations for transformations $\rho_{AB} \to \omega_{AB}$? The largest meaningful such set is given by δ-non-entangling operations

$$NE_{\delta(A:B\to A':B')} \coloneqq \{\Lambda \in CPTP(AB \to A'B'): R_S\big(\Lambda(\sigma_{AB})\big) \leq \delta \ \forall \sigma_{AB} \in S_{A:B}\}$$

Asymptotic resource theory of entanglement

- Distillable entanglement under asymptotically non-entangling operations (ANE):

$$E_D^{ANE}(\rho) := \sup_{(k_n),(\delta_n)} \{\liminf_{n\to\infty} \frac{k_n}{n} : \lim_{n\to\infty} \min_{\Lambda \in NE_{\delta_n}} ||\Lambda(\rho^{\otimes n}) - \Phi^{\otimes k_n}||_1 = 0, \lim_{n\to\infty} \delta_n = 0\}$$

- Entanglement cost under ANE:

$$E_C^{ANE}(\rho) := \inf_{(k_n),(\delta_n)} \{\limsup_{n\to\infty} \frac{k_n}{n} : \lim_{n\to\infty} \min_{\Lambda \in NE_{\delta_n}} ||\Lambda(\Phi^{\otimes k_n}) - \rho^{\otimes n}||_1 = 0, \lim_{n\to\infty} \delta_n = 0\}$$

- Asymptotic transformation rate $\rho_{AB} \to \omega_{AB}$ under ANE:

$$R^{ANE}(\rho \to \omega) := \sup_{(k_n),(\delta_n)} \{\liminf_{n\to\infty} \frac{k_n}{n} : \lim_{n\to\infty} \min_{\Lambda \in NE_{\delta_n}} ||\Lambda(\rho^{\otimes n}) - \omega^{\otimes k_n}||_1 = 0, \lim_{n\to\infty} \delta_n = 0\}$$

aws

- **Asymptotic reversibility?**

Asymptotic characterization of entanglement

- Asymptotically reversible under ANE?

$R^{ANE}(\rho \to \omega) \cdot R^{ANE}(\omega \to \rho) = 1$ or in other words $E_D^{ANE}(\rho) = E_C^{ANE}(\rho)$?

- Entanglement cost [Brandão & Plenio, CMP 10], [Datta, IEEE 09]

$$E_C^{ANE}(\rho) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \min_{\sigma^n \in S^n} D_{\max}^{\varepsilon}(\rho^{\otimes n} || \sigma^n) = \lim_{n \to \infty} \frac{1}{n} \min_{\sigma^n \in S^n} D(\rho^{\otimes n} || \sigma^n) \neq \min_{\sigma \in S} D(\rho || \sigma)$$

- Distillable entanglement [Brandão & Plenio, CMP 10]

$$E_D^{ANE}(\rho) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} -\frac{1}{n} \log \beta_\varepsilon(\rho^{\otimes n}, S^n)$$

for the hypothesis testing $\beta_\varepsilon(\rho^{\otimes n}, S^n) \coloneqq \inf_{0 \le M_n \le 1} \{ \sup_{\sigma^n \in S^n} Tr[M_n \sigma^n] \colon Tr[(1 - M_n)\rho^{\otimes n}] \le \varepsilon \}$

- Composite quantum hypothesis testing question $-\frac{1}{n} \log \beta_\varepsilon(\rho^{\otimes n}, S^n) \to \frac{1}{n} \min_{\sigma^n \in S^n} D(\rho^{\otimes n} || \sigma^n)$?

Reduction to hypothesis testing

- Question if $E_D^{ANE}(\rho) = E_C^{ANE}(\rho)$ reduces to composite quantum hypothesis question

$$-\frac{1}{n}\log\beta_\varepsilon(\rho, S^n) \rightarrow \frac{1}{n}\min_{\sigma^n \in S^n} D(\rho^{\otimes n}||\sigma^n)?$$

- Converse direction by standard arguments [Brandão & Plenio, CMP 10]:

$$\lim_{\varepsilon\rightarrow 0}\lim_{n\rightarrow\infty} -\frac{1}{n}\log\beta_\varepsilon(\rho, S^n) \leq \lim_{n\rightarrow\infty}\frac{1}{n}\min_{\sigma^n\in S^n} D(\rho^{\otimes n}||\sigma^n)$$

- [B. *et al.*, arXiv 22] recently found that achievability direction " $\geq$ " remains open
- Setting: $T^n = \{\rho^{\otimes n}\}$ singleton, but separable set $S^n \equiv S_{A^n:B^n} \equiv S_{(A_1\cdots A_n:B_1\cdots B_n)}$ is not IID and could be entangled across different A_i's and B_i's, resp.
- Results from [B. et al., CMP 21] do not directly apply!

What can be shown?

- Pseudo-entanglement theory:

$\bar{S}_{A^n:B^n} \coloneqq conv\{\bigotimes_{j=1}^{n} \sigma_{A_jB_j}^{(j)} : \sigma_{A_jB_j}^{(j)} \in S_{A_jB_j} \forall j\}$ separable across the partition $A_1 : \cdots : A_n : B_1 : \cdots B_n$

and combination of [Brandão *et al.*, IEEE 20], [B. et al., CMP 21] gives

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\log\beta_\varepsilon\left(\rho^{\otimes n}, \bar{S}^n\right) = \lim_{n\to\infty}\frac{1}{n}\min_{\sigma^n\in\bar{S}^n} D(\rho^{\otimes n}||\sigma^n)$$

- Pseudo-entanglement in blocks $A^k := A_1 \cdots A_k, B^k \coloneqq B_1 \cdots B_k$ with $\bar{S}^k_{A^n:B^n}$ [B. *et al.*, arXiv 22]

$$\lim_{k\to\infty}\lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{nk}\min_{\sigma^{nk}\in\bar{S}^{n,k}}\log\beta_\varepsilon\left(\rho^{\otimes nk}, \sigma^{nk}\right) = \lim_{n\to\infty}\frac{1}{n}\min_{\sigma^n\in S^n} D(\rho^{\otimes n}||\sigma^n)$$

- Remains open if $\lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\min_{\sigma^n\in S^n}\log\beta_\varepsilon\left(\rho^{\otimes n}, \sigma^n\right) \geq \lim_{n\to\infty}\frac{1}{n}\min_{\sigma^n\in S^n} D(\rho^{\otimes n}||\sigma^n)$?

- **Proof techniques:**
  Universal hypothesis tests

1) via Petz-Rényi divergences?

2) via measured divergence?

3) via max-relative entropy?

1) Universal hypothesis tests via Petz-Rényi divergences

- Sion minimax + Audenaert inequality for $s \in (0,1)$ gives [Audenaert *et al.*, CMP 08]

$$-\frac{1}{n}\log \beta_\varepsilon\left(\rho^{\otimes n}, S^n\right) = -\frac{1}{n}\sup_{\sigma^n \in S^n}\ \inf_{0 \le M_n \le 1, Tr\left[M_n \rho^{\otimes n}\right] \ge 1-\varepsilon} \log Tr[M_n \sigma^n] \ge \frac{1}{n}\inf_{\sigma^n \in S^n} D_s(\rho^{\otimes n}||\sigma^n) - \frac{1}{n}\cdot\frac{s}{1-s}\log\frac{1}{\varepsilon}$$

  for the additive $D_s(\rho||\sigma) := \frac{1}{s-1}\log Tr[\rho^s \sigma^{1-s}]$ with $\lim_{s \to 1} D_s(\rho||\sigma) = D(\rho||\sigma)$

- Single-letter: de Finetti, take limits $(\mathrm{i})\ n \to \infty\ (ii)\ \varepsilon \to 0\ (iii)\ s \to 1$ in order [B. et al., CMP 21]
- Generally, with information variance $V(\rho||\sigma) := Tr[\rho(\log\rho - \log\sigma - D(\rho||\sigma))^2]$ to bound

$$\frac{1}{n}|D_s(\rho^{\otimes n}||\sigma^n) - D(\rho^{\otimes n}||\sigma^n)| \le \frac{s-1}{2}\cdot\frac{V(\rho^{\otimes n}||\sigma^n)}{n} + \frac{O\left((s-1)^2\right)}{n}$$

- [Brandão & Plenio, CMP 10] claimed that $V(\rho^{\otimes n}||\sigma^n) \le o(2^{-n})$, but already

  $V\left(\rho^{\otimes n}||\sigma^{\otimes n}\right) = n \cdot V(\rho||\sigma) \not\le o(2^{-n})$ → Remains open: de Finetti / Schur-Weyl duality?

2) Universal hypothesis tests via measured divergence

- Measured relative entropy [Donald, CMP 86] with [Brandão *et al.*, IEEE 20]

$D_M(\rho||\sigma) \coloneqq \sup_M D_{KL}(M(\rho)||M(\sigma))$ with $\inf_{\rho\in T,\sigma\in S} D_M(\rho||\sigma) = \sup_M \inf_{\rho\in T,\sigma\in S} D_{KL}(M(\rho)||M(\sigma))$

- (i) measure, (ii) apply classical composite hypothesis result, (iii) use asymptotic achievability of measured relative entropy for ρ^n, σ^n permutation invariant [B. et al., CMP 21]

$$\frac{1}{n} D_M(\rho^n||\sigma^n) \to \frac{1}{n} D(\rho^n||\sigma^n) \text{ for } n \to \infty$$

- Gives pseudo-entanglement theory and pseudo-entanglement in blocks [B. *et al.*, arXiv 22]
- Remains open: entanglement theory. Alternatively, one has [Brandão *et al.*, IEEE 20]

$$\lim_{n\to\infty} \frac{1}{n} \min_{\sigma^n\in S^n} D_{M_{SEP}}(\rho^{\otimes n}||\sigma^n) \to \lim_{n\to\infty} \frac{1}{n} \min_{\sigma^n\in S^n} D(\rho^{\otimes n}||\sigma^n)\,?$$

3) Universal hypothesis tests via max-relative entropy

- For $\varepsilon \in (0,1)$ we have [Anshu *et al.*, JMP 19]

$$-\frac{1}{n}\log \sup_{\sigma^n \in S^n} \beta_\varepsilon\left(\rho^{\otimes n}, \sigma^n\right) \geq \frac{1}{n} \min_{\sigma^n \in S^n} D_{\max}^{\sqrt{1-\varepsilon}}(\rho^{\otimes n}||\sigma^n) - \frac{1}{n}\log\frac{1}{\varepsilon}$$

- Previously mentioned asymptotic equipartition property (AEP) for max-relative entropy

$\lim_{\delta\to 0}\lim_{n\to\infty}\frac{1}{n}\min_{\sigma^n\in S^n} D_{\max}^{\delta}(\rho^{\otimes n}||\sigma^n) = \lim_{n\to\infty}\frac{1}{n}\min_{\sigma^n\in S^n} D(\rho^{\otimes n}||\sigma^n)$ not enough as no strong converse!

- Similar open problems:
  - Quantum channel AEP [Gour & Winter, PRL 19]
  - Strong converse channel discrimination & channel capacities [Fang *et al.*, arXiv 21] [Bergh *et al.*, arXiv 21]
  - Stronger entropy accumulation [Metger *et al.*, arXiv 22]

- Conclusion

Outlook

- Question if $E_D^{ANE}(\rho) = E_C^{ANE}(\rho)$ reduces to composite quantum hypothesis question

$$-\frac{1}{n}\log \beta_\varepsilon^n(\rho, S^n) \to \frac{1}{n}\min_{\sigma^n \in S^n} D(\rho^{\otimes n}||\sigma^n)\,?$$

  This remains open.

- Take step back, classical version of non-IID problem? Not clear, cf. [Mosonyi *et al.*, arXiv 21]
- Composite hypothesis testing will hold for some resource theories under suitable axiom set, but must be shown “manually” every time – and so far, we only have single-letter solutions
- Reversibility of resource theories? If I had to guess, reversibility does not hold in general
- Hint for resource theory of entanglement: [Lami & Regula, arXiv 21]

aws

Lami & Regula arXiv:2111.02438

- Title: No second law of entanglement manipulation after all
- Recall:
  - δ-non-entangling operations $NE_{\delta(AB \to A'B')} = \{\Lambda \in CPTP(AB \to A'B'): R_S\big(\Lambda(\sigma_{AB})\big) \leq \delta \ \forall \sigma_{AB} \in S_{A:B}\}$
  - with global resource robustness $R_S(\rho_{AB}) = \{s \geq 0: \frac{\rho_{AB} + s\sigma_{AB}}{1+s} \in S_{A:B}\}$
- Replace $R_S(\rho_{AB})$ with resource robustness

$$\bar{R}_s(\rho_{AB}) := \{s \geq 0: \frac{\rho_{AB} + s\sigma_{AB}}{1+s} \in S_{A:B}, \sigma_{AB} \in S_{A:B}\} \geq R_S(\rho_{AB})$$

and correspondingly

$$\overline{NE}_{\delta(AB \to A'B')} \coloneqq \{\Lambda \in CPTP(AB \to A'B'): \bar{R}_S\big(\Lambda(\sigma_{AB})\big) \leq \delta \ \forall \sigma_{AB} \in S_{AB}\}$$

- Main result: there exists quantum state ρ with $E_D^{\overline{ANE}}(\rho) < E_C^{\overline{ANE}}(\rho)$

Thank you!

- **B., Brandão, Hirche: CMP 385, 55 (2021)**
- **B., Brandão, Gour, Lami, Plenio, Regula, Tomamichel: arXiv:2205.02813 (2022)**
- Audenaert, Nussbaum, Szkola, Verstraete: CMP 279, 251 (2008)
- Brandão, Harrow, Lee, Peres: IEEE 66, 5037 (2020)
- Mosonyi, Szilágyi, Weiner: arXiv:2011.04645 (2021)
- Lami & Regula: arXiv:2111.02438 (2021)
- Bergh, Datta, Salzmann, Wilde: arXiv:2206.08350 (2022)