Recoverability in quantum information theory

Mark M. Wilde

Hearne Institute for Theoretical Physics,
Department of Physics and Astronomy,
Center for Computation and Technology,
Louisiana State University,
Baton Rouge, Louisiana, USA

mwilde@lsu.edu

Beyond i.i.d., July 5-10, 2015, Banff, Alberta, Canada

Main message

- Entropy inequalities established in the 1970s are a mathematical consequence of the postulates of quantum physics
- They are helpful in determining the ultimate limits on many physical processes (communication, thermodynamics, uncertainty relations)
- Many of these entropy inequalities are equivalent to each other, so we can say that together they constitute a fundamental law of quantum information theory
- There has been recent interest in refining these inequalities, trying to understand how well one can attempt to reverse an irreversible physical process
- This poster presentation discusses progress in this direction

Background — entropies

Umegaki relative entropy [Ume62]

The quantum relative entropy is a measure of dissimilarity between two quantum states. Defined for state ρ and positive semi-definite σ as

$$D(\rho\|\sigma) \equiv \mathrm{Tr}\{\rho[\log \rho - \log \sigma]\}$$

whenever $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$ and $+\infty$ otherwise

Physical interpretation with quantum Stein's lemma [HP91, NO00]

Given are n quantum systems, all of which are prepared in either the state ρ or σ. With a constraint of $\varepsilon \in (0,1)$ on the Type I error of misidentifying ρ, then the optimal error exponent for the Type II error of misidentifying σ is $D(\rho\|\sigma)$.

Background — entropies

Relative entropy as "mother" entropy

Many important entropies can be written in terms of relative entropy:

- $H(A)_\rho \equiv -D(\rho_A \| I_A)$ (entropy)
- $H(A|B)_\rho \equiv -D(\rho_{AB} \| I_A \otimes \rho_B)$ (conditional entropy)
- $I(A;B)_\rho \equiv D(\rho_{AB} \| \rho_A \otimes \rho_B)$ (mutual information)
- $I(A;B|C)_\rho \equiv D(\rho_{ABC} \| \exp\{\log \rho_{AC} + \log \rho_{BC} - \log \rho_C\})$ (cond. MI)

Equivalences

- $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$
- $I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho$
- $I(A;B)_\rho = H(B)_\rho - H(B|A)_\rho$
- $I(A;B|C)_\rho = H(AC)_\rho + H(BC)_\rho - H(ABC)_\rho - H(C)_\rho$
- $I(A;B|C)_\rho = H(B|C)_\rho - H(B|AC)_\rho$

Fundamental law of quantum information theory

Monotonicity of quantum relative entropy [Lin75, Uhl77]

Let ρ be a state, let σ be positive semi-definite, and let $\mathcal{N}$ be a quantum channel. Then

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$$

"Distinguishability does not increase under a physical process"
Characterizes a fundamental irreversibility in any physical process

Proof approaches

- Lieb concavity theorem [L73]
- relative modular operator method (see, e.g., [NP04])
- quantum Stein's lemma [BS03]

Strong subadditivity

Strong subadditivity [LR73]

Let ρ_{ABC} be a tripartite quantum state. Then

$$I(A;B|C)_\rho \geq 0$$

Equivalent statements (by definition)

- Entropy sum of two individual systems is larger than entropy sum of their union and intersection:

$$H(AC)_\rho + H(BC)_\rho \geq H(ABC)_\rho + H(C)_\rho$$

- Conditional entropy does not decrease under the loss of system A:

$$H(B|C)_\rho \geq H(B|AC)_\rho$$

Equality conditions [Pet86, Pet88]

When does equality in monotonicity of relative entropy hold?

- $D(\rho\|\sigma) = D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$ iff $\exists$ a recovery map $\mathcal{R}^P_{\sigma,\mathcal{N}}$ such that

$$\rho = (\mathcal{R}^P_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho), \qquad \sigma = (\mathcal{R}^P_{\sigma,\mathcal{N}} \circ \mathcal{N})(\sigma)$$

- This "Petz" recovery map has the following explicit form [HJPW04]:

$$\mathcal{R}^P_{\sigma,\mathcal{N}}(\omega) \equiv \sigma^{1/2}\mathcal{N}^\dagger \left((\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2} \right) \sigma^{1/2}$$

- Classical case: Distributions p_X and q_X and a channel $\mathcal{N}(y|x)$. Then the Petz recovery map $\mathcal{R}^P(x|y)$ is given by the Bayes theorem:

$$\mathcal{R}^P(x|y)q_Y(y) = \mathcal{N}(y|x)q_X(x)$$

where $q_Y(y) \equiv \sum_x \mathcal{N}(y|x)q_X(x)$

More on Petz recovery map

- Linear, completely positive by inspection and trace non-increasing because

$$
\begin{aligned}
\operatorname{Tr}\{\mathcal{R}^{P}_{\sigma,\mathcal{N}}(\omega)\} &= \operatorname{Tr}\{\sigma^{1/2}\mathcal{N}^{\dagger}\left((\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2}\right)\sigma^{1/2}\} \\
&= \operatorname{Tr}\{\sigma\mathcal{N}^{\dagger}\left((\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2}\right)\} \\
&= \operatorname{Tr}\{\mathcal{N}(\sigma)(\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2}\} \\
&\leq \operatorname{Tr}\{\omega\}
\end{aligned}
$$

- For $\mathcal{N}(\sigma)$ positive definite, the map perfectly recovers σ from $\mathcal{N}(\sigma)$:

$$
\begin{aligned}
\mathcal{R}^{P}_{\sigma,\mathcal{N}}(\mathcal{N}(\sigma)) &= \sigma^{1/2}\mathcal{N}^{\dagger}\left((\mathcal{N}(\sigma))^{-1/2}\mathcal{N}(\sigma)(\mathcal{N}(\sigma))^{-1/2}\right)\sigma^{1/2} \\
&= \sigma^{1/2}\mathcal{N}^{\dagger}(I)\,\sigma^{1/2} \\
&= \sigma
\end{aligned}
$$

Functoriality

Normalization [LW14]

For identity channel, the Petz recovery map is the identity map: $\mathcal{R}^P_{\sigma,\text{id}} = \text{id}$. "If there's no noise, then no need to recover"

Tensorial [LW14]

Given a tensor-product state and channel, then the Petz recovery map is a tensor product: $\mathcal{R}^P_{\sigma_1 \otimes \sigma_2, \mathcal{N}_1 \otimes \mathcal{N}_2} = \mathcal{R}^P_{\sigma_1, \mathcal{N}_1} \otimes \mathcal{R}^P_{\sigma_2, \mathcal{N}_2}$. "Individual action suffices for 'pretty good' recovery of individual states"

Composition [LW14]

Given $\mathcal{N}_2 \circ \mathcal{N}_1$, then $\mathcal{R}^P_{\sigma, \mathcal{N}_2 \circ \mathcal{N}_1} = \mathcal{R}^P_{\sigma, \mathcal{N}_1} \circ \mathcal{R}^P_{\mathcal{N}_1(\sigma), \mathcal{N}_2}$. "To recover 'pretty well' overall, recover 'pretty well' from the last noise first and the first noise last"

Petz recovery map for strong subadditivity

- Strong subadditivity is a special case of monotonicity of relative entropy with $\rho = \omega_{ABC}$, $\sigma = \omega_{AC} \otimes I_B$, and $\mathcal{N} = \text{Tr}_A$
- Then $\mathcal{N}^\dagger(\cdot) = (\cdot) \otimes I_A$ and Petz recovery map is

$$\mathcal{R}^P_{C\to AC}(\tau_C) = \omega_{AC}^{1/2} \left(\omega_C^{-1/2} \tau_C \omega_C^{-1/2} \otimes I_A\right) \omega_{AC}^{1/2}$$

- Interpretation: If system A is lost but $H(B|C)_\omega = H(B|AC)_\omega$, then one can recover the full state on ABC by performing the Petz recovery map on system C of ω_{BC}, i.e.,

$$\omega_{ABC} = \mathcal{R}^P_{C\to AC}(\omega_{BC})$$

Approximate case

Approximate case would be useful for applications

Approximate case for monotonicity of relative entropy

- What can we say when $D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) = \varepsilon$?
- Does there exist a CPTP map $\mathcal{R}$ that recovers σ perfectly from $\mathcal{N}(\sigma)$ while recovering ρ from $\mathcal{N}(\rho)$ approximately? [WL12]

Approximate case for strong subadditivity

- What can we say when $H(B|C)_\omega - H(B|AC)_\omega = \varepsilon$?
- Is ω_{ABC} approximately recoverable from ω_{BC} by performing a recovery map on system C alone? [WL12]

Other measures of similarity for quantum states

Trace distance

Trace distance between ρ and σ is $\|\rho - \sigma\|_1$ where $\|A\|_1 = \text{Tr}\{\sqrt{A^\dagger A}\}$. Has a one-shot operational interpretation as the bias in success probability when distinguishing ρ and σ with an optimal quantum measurement.

Fidelity [Uhl76]

Fidelity between ρ and σ is $F(\rho, \sigma) \equiv \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$. Has a one-shot operational interpretation as the probability with which a purification of ρ could pass a test for being a purification of σ.

Bures distance [Bur69]

Bures distance between ρ and σ is $D_B(\rho, \sigma) = \sqrt{2\left(1 - \sqrt{F(\rho, \sigma)}\right)}$.

Breakthrough result of [FR14]

Remainder term for strong subadditivity [FR14]

$\exists$ unitary channels $\mathcal{U}_C$ and $\mathcal{V}_{AC}$ such that

$$H(B|C)_\omega - H(B|AC)_\omega \geq -\log F\left(\omega_{ABC}, (\mathcal{V}_{AC} \circ \mathcal{R}^P_{C\to AC} \circ \mathcal{U}_C)(\omega_{BC})\right)$$

Nothing known from [FR14] about these unitaries! However, can conclude that $I(A;B|C)$ is small iff ω_{ABC} is approximately recoverable from system C alone after the loss of system A.

Remainder term for monotonicity of relative entropy [BLW14]

$\exists$ unitary channels $\mathcal{U}$ and $\mathcal{V}$ such that

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, (\mathcal{V} \circ \mathcal{R}^P_{\sigma,\mathcal{N}} \circ \mathcal{U})(\mathcal{N}(\rho))\right)$$

Again, nothing known from [BLW14] about $\mathcal{U}$ and $\mathcal{V}$.

New result of [Wil15]

New Theorem: Let ρ and σ be such that $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and let $\mathcal{N}$ be a quantum channel. Then the following inequality holds

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log\left[\sup_{t\in\mathbb{R}} F\left(\rho, \mathcal{R}^{P,t}_{\sigma,\mathcal{N}}(\mathcal{N}(\rho))\right)\right],$$

where $\mathcal{R}^{P,t}_{\sigma,\mathcal{N}}$ is the following rotated Petz recovery map:

$$\mathcal{R}^{P,t}_{\sigma,\mathcal{N}}(\cdot) \equiv \left(\mathcal{U}_{\sigma,t} \circ \mathcal{R}^{P}_{\sigma,\mathcal{N}} \circ \mathcal{U}_{\mathcal{N}(\sigma),-t}\right)(\cdot),$$

$\mathcal{R}^{P}_{\sigma,\mathcal{N}}$ is the Petz recovery map, and $\mathcal{U}_{\sigma,t}$ and $\mathcal{U}_{\mathcal{N}(\sigma),-t}$ are defined from $\mathcal{U}_{\omega,t}(\cdot) \equiv \omega^{it}(\cdot)\,\omega^{-it}$, with ω a positive semi-definite operator.

Two tools for proof: Rényi generalization of a relative entropy difference and the Hadamard three-line theorem

Rényi generalizations of a relative entropy difference

Definition from [BSW14, SBW14]

$$\widetilde{\Delta}_{\alpha}(\rho,\sigma,\mathcal{N}) \equiv \frac{2}{\alpha'}\log\left\|\left(\mathcal{N}(\rho)^{-\alpha'/2}\mathcal{N}(\sigma)^{\alpha'/2}\otimes I_E\right)U\sigma^{-\alpha'/2}\rho^{1/2}\right\|_{2\alpha},$$

where $\alpha \in (0,1)\cup(1,\infty)$, $\alpha' \equiv (\alpha-1)/\alpha$, and $U_{S\to BE}$ is an isometric extension of $\mathcal{N}$.

Important properties

$$\lim_{\alpha\to 1}\widetilde{\Delta}_{\alpha}(\rho,\sigma,\mathcal{N}) = D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)).$$

$$\widetilde{\Delta}_{1/2}(\rho,\sigma,\mathcal{N}) = -\log F\left(\rho,\mathcal{R}^{P}_{\sigma,\mathcal{N}}(\mathcal{N}(\rho))\right).$$

Hadamard three-line theorem

Let $S \equiv \{z \in \mathbb{C} : 0 \leq \text{Re}\{z\} \leq 1\}$, and let $L(\mathcal{H})$ be the space of bounded linear operators acting on a Hilbert space $\mathcal{H}$. Let $G : S \to L(\mathcal{H})$ be a bounded map that is holomorphic on the interior of S and continuous on the boundary. Let $\theta \in (0,1)$ and define p_θ by

$$\frac{1}{p_\theta} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1},$$

where $p_0, p_1 \in [1, \infty]$. For $k = 0, 1$ define

$$M_k = \sup_{t \in \mathbb{R}} \|G(k + it)\|_{p_k}.$$

Then

$$\|G(\theta)\|_{p_\theta} \leq M_0^{1-\theta} M_1^\theta.$$

Three (or so) line proof

Pick

$$G(z) \equiv \left([\mathcal{N}(\rho)]^{z/2} [\mathcal{N}(\sigma)]^{-z/2} \otimes I_E \right) U \sigma^{z/2} \rho^{1/2},$$

$$p_0 = 2, \;\; p_1 = 1, \;\; \theta \in (0,1) \;\; \Rightarrow p_\theta = \frac{2}{1+\theta}$$

Then

$$M_0 = \sup_{t\in\mathbb{R}} \left\| \left(\mathcal{N}(\rho)^{it/2} \mathcal{N}(\sigma)^{-it/2} \otimes I_E \right) U \sigma^{it} \rho^{1/2} \right\|_2 \leq \left\| \rho^{1/2} \right\|_2 = 1,$$

$$M_1 = \sup_{t\in\mathbb{R}} \| G(1+it) \|_1 = \left[\sup_{t\in\mathbb{R}} F\left(\rho, \mathcal{R}^{P,t}_{\sigma,\mathcal{N}}(\mathcal{N}(\rho)) \right) \right]^{1/2}.$$

Apply the three-line theorem to conclude that

$$\| G(\theta) \|_{2/(1+\theta)} \leq \left[\sup_{t\in\mathbb{R}} F\left(\rho, \mathcal{R}^{P,t}_{\sigma,\mathcal{N}}(\mathcal{N}(\rho)) \right) \right]^{\theta/2}.$$

Take a negative logarithm and the limit as $\theta \searrow 0$ to conclude.

SSA refinement as a special case

Let ρ_{ABC} be a density operator acting on a finite-dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Then the following inequality holds

$$I(A;B|C)_\rho \geq -\log\left[\sup_{t\in\mathbb{R}} F\left(\rho_{ABC}, \mathcal{R}^{P,t}_{C\to AC}(\rho_{BC})\right)\right],$$

where $\mathcal{R}^{P,t}_{C\to AC}$ is the following rotated Petz recovery map:

$$\mathcal{R}^{P,t}_{C\to AC}(\cdot) \equiv \left(\mathcal{U}_{\rho_{AC},t} \circ \mathcal{R}^{P}_{C\to AC} \circ \mathcal{U}_{\rho_C,-t}\right)(\cdot),$$

the Petz recovery map $\mathcal{R}^{P}_{C\to AC}$ is defined as

$$\mathcal{R}^{P}_{C\to AC}(\cdot) \equiv \rho_{AC}^{1/2}\left[\rho_C^{-1/2}(\cdot)\,\rho_C^{-1/2} \otimes I_A\right]\rho_{AC}^{1/2},$$

and the partial isometric maps $\mathcal{U}_{\rho_{AC},t}$ and $\mathcal{U}_{\rho_C,-t}$ are defined as before.

Conclusions

- The result of [FR14] already had a number of important implications in quantum information theory.
- The new result in [Wil15] applies to relative entropy differences, has a brief proof, and improves our understanding of the input and output unitaries (but see [SFR15] for the special case of SSA)
- By building on [SFR15, Wil15], we can now generalize these results: there is a universal recovery map which depends only on σ and $\mathcal{N}$ and has the form [SRWW15]:

$$X \to \int \mu(dt)\, \mathcal{R}^{P,t}_{\sigma,\mathcal{N}}(X)$$

  for some probability measure μ.
- It is still conjectured that the recovery map can be the Petz recovery map alone (not a rotated Petz map).

References I

[BLW14] Mario Berta, Marius Lemm, and Mark M. Wilde. Monotonicity of quantum relative entropy and recoverability. December 2014. arXiv:1412.4067.

[BS03] Igor Bjelakovic and Rainer Siegmund-Schultze. Quantum Stein's lemma revisited, inequalities for quantum entropies, and a concavity theorem of Lieb. July 2003. arXiv:quant-ph/0307170.

[BSW14] Mario Berta, Kaushik Seshadreesan, and Mark M. Wilde. Rényi generalizations of the conditional quantum mutual information. March 2014. arXiv:1403.6102.

[Bur69] Donald Bures. An extension of Kakutani's theorem on infinite product measures to the tensor product of semifinite w^*-algebras. *Transactions of the American Mathematical Society*, 135:199–212, January 1969.

[FR14] Omar Fawzi and Renato Renner. Quantum conditional mutual information and approximate Markov chains. October 2014. arXiv:1410.0664.

[HJPW04] Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Communications in Mathematical Physics*, 246(2):359–374, April 2004. arXiv:quant-ph/0304007.

References II

[HP91] Fumio Hiai and Denes Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143(1):99–114, December 1991.

[Lin75] Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40(2):147–151, June 1975.

[L73] Elliott H. Lieb. Convex Trace Functions and the Wigner-Yanase-Dyson Conjecture. *Advances in Mathematics*, 11(3), 267–288, December 1973.

[LR73] Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. *Journal of Mathematical Physics*, 14(12):1938–1941, December 1973.

[LW14] Ke Li and Andreas Winter. Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps. October 2014. arXiv:1410.4184.

[NO00] Hirsohi Nagaoka and Tomohiro Ogawa. Strong converse and Stein's lemma in quantum hypothesis testing. *IEEE Transactions on Information Theory*, 46(7):2428–2433, November 2000. arXiv:quant-ph/9906090.

References III

[NP04] Michael A. Nielsen and Denes Petz. A simple proof of the strong subadditivity inequality. arXiv:quant-ph/0408130.

[Pet86] Denes Petz. Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. *Communications in Mathematical Physics*, 105(1):123–131, March 1986.

[Pet88] Denes Petz. Sufficiency of channels over von Neumann algebras. *Quarterly Journal of Mathematics*, 39(1):97–108, 1988.

[SBW14] Kaushik P. Seshadreesan, Mario Berta, and Mark M. Wilde. Rényi squashed entanglement, discord, and relative entropy differences. October 2014. arXiv:1410.1443.

[SFR15] David Sutter, Omar Fawzi, and Renato Renner. Universal recovery map for approximate Markov chains. April 2015. arXiv:1504.07251.

[SRWW15] David Sutter, Renato Renner, Mark M. Wilde, and Andreas Winter. Universal recovery from a decrease of quantum relative entropy. June 2015. arXiv:150?.?????.

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[Uhl77] Armin Uhlmann. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Communications in Mathematical Physics*, 54(1):21–32, 1977.

[Ume62] Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

[Wil15] Mark M. Wilde. Recoverability in quantum information theory. May 2015. arXiv:1505.04661.

[WL12] Andreas Winter and Ke Li. A stronger subadditivity relation? http://www.maths.bris.ac.uk/∼csajw/stronger_subadditivity.pdf, 2012.