Universal recoverability in quantum information

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

Based on arXiv:1505.04661, 1506.00981, 1509.07127, 1511.00267, 1601.01207, 1608.07569, 1610.01262
with Berta, Buscemi, Das, Dupuis, Junge, Lami, Lemm, Renner, Sutter, Winter

QMATH 2016, Atlanta, Georgia, USA

Main message

- Entropy inequalities established in the 1970s are a mathematical consequence of the postulates of quantum physics
- They have a number of applications: for determining the ultimate limits on many physical processes (communication, thermodynamics, uncertainty relations, cloning)
- 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
- We discuss 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

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

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

Operational interpretation (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 $D(\rho\|\sigma)$.

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 (among many)

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

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 $\mathcal{P}_{\sigma,\mathcal{N}}$ such that

$$\rho = (\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho), \qquad \sigma = (\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\sigma)$$

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

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

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

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

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

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]

One-shot measure of similarity for quantum states

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.

New result of [Wil15, JSRWW15]

Recoverability Theorem

Let ρ and σ satisfy $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and let $\mathcal{N}$ be a channel. Then

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\int_{-\infty}^{\infty} dt\, p(t) \log\left[F\left(\rho, \mathcal{P}^{t/2}_{\sigma,\mathcal{N}}(\mathcal{N}(\rho))\right)\right],$$

where $p(t)$ is a distribution and $\mathcal{P}^{t}_{\sigma,\mathcal{N}}$ is a rotated Petz recovery map:

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

$\mathcal{P}_{\sigma,\mathcal{N}}$ 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 Stein–Hirschman operator interpolation theorem

Universal Recovery

Universal Recoverability Corollary

Let ρ and σ satisfy $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and let $\mathcal{N}$ be a channel. Then

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F(\rho, \mathcal{R}_{\sigma,\mathcal{N}}(\mathcal{N}(\rho))),$$

where

$$\mathcal{R}_{\sigma,\mathcal{N}} \equiv \int_{-\infty}^{\infty} dt\, p(t)\, \mathcal{P}_{\sigma,\mathcal{N}}^{t/2}$$

(follows from concavity of logarithm and fidelity)

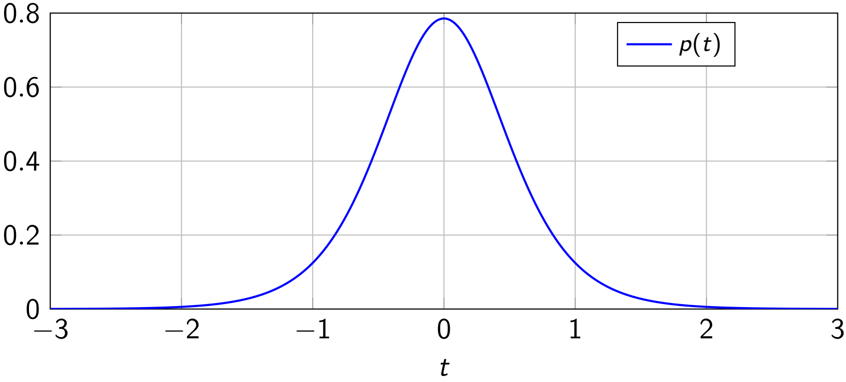

Figure: This plot depicts the probability density $p(t) := \frac{\pi}{2}\left(\cosh(\pi t) + 1\right)^{-1}$ as a function of $t \in \mathbb{R}$. We see that it is peaked around $t = 0$ which corresponds to the Petz recovery map.

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

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

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

Stein–Hirschman operator interpolation theorem (setup)

Let $S \equiv \{z \in \mathbb{C} : 0 < \text{Re}\{z\} < 1\}$, and let $L(\mathcal{H})$ be the space of bounded linear operators acting on $\mathcal{H}$. Let $G : \overline{S} \to L(\mathcal{H})$ be an operator-valued function bounded on $\overline{S}$, holomorphic on S, and continuous on the boundary $\partial\overline{S}$. Let $\theta \in (0,1)$ and define p_θ by

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

where $p_0, p_1 \in [1, \infty]$.

Stein–Hirschman operator interp. theorem (statement)

Then the following bound holds

$$\log \|G(\theta)\|_{p_\theta} \leq \int_{-\infty}^{\infty} dt \, \left(\alpha_\theta(t) \log \left[\|G(it)\|_{p_0}^{1-\theta}\right] + \beta_\theta(t) \log \left[\|G(1+it)\|_{p_1}^{\theta}\right]\right),$$

$$\text{where } \alpha_\theta(t) \equiv \frac{\sin(\pi\theta)}{2(1-\theta)\left[\cosh(\pi t) - \cos(\pi\theta)\right]},$$

$$\beta_\theta(t) \equiv \frac{\sin(\pi\theta)}{2\theta\left[\cosh(\pi t) + \cos(\pi\theta)\right]},$$

$$\lim_{\theta \searrow 0} \beta_\theta(t) = p(t).$$

Proof of Recoverability Theorem

Tune parameters

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

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

Evaluate norms

$$\|G(it)\|_2 = \left\| \left(\mathcal{N}(\rho)^{it/2} \mathcal{N}(\sigma)^{-it/2} \otimes I_E \right) U \sigma^{it/2} \rho^{1/2} \right\|_2 \leq \left\| \rho^{1/2} \right\|_2 = 1,$$

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

Proof of Recoverability Theorem (ctd.)

Apply the Stein–Hirschman theorem

$$\log \left\| \left([\mathcal{N}(\rho)]^{\theta/2} [\mathcal{N}(\sigma)]^{-\theta/2} \otimes I_E \right) U \sigma^{\theta/2} \rho^{1/2} \right\|_{2/(1+\theta)} \leq \int_{-\infty}^{\infty} dt \ \beta_\theta(t) \log \left[F\left(\rho, (\mathcal{P}_{\sigma,\mathcal{N}}^{t/2} \circ \mathcal{N})(\rho)\right)^{\theta/2} \right].$$

Final step

Apply a minus sign, multiply both sides by $2/\theta$, and take the limit as $\theta \searrow 0$ to conclude.

Specializing to the Holevo Bound

- Specializing to the Holevo bound leads to a refinement. Given

$$\rho_{XB} \equiv \sum_x p_X(x)|x\rangle\langle x|_X \otimes \rho_B^x, \qquad \omega_{XY} \equiv \sum_y \langle \varphi^y|_B \rho_{XB} |\varphi^y\rangle_B |y\rangle\langle y|_Y.$$

- Then the following inequality holds

$$I(X;B)_\rho - I(X;Y)_\omega \geq -2\log \sum_x p_X(x) \sqrt{F}(\rho_B^x, \mathcal{E}_B(\rho_B^x)),$$

- where $\mathcal{E}_B$ is an entanglement-breaking map of the form

$$\mathcal{E}_B(\cdot) \equiv \int_{-\infty}^{\infty} dt\ \beta_0(t)\ \sum_y \langle \varphi_y|_B (\cdot) |\varphi_y\rangle_B \frac{\rho_B^{(1+it)/2} |\varphi_y\rangle\langle\varphi_y|_B \rho_B^{(1-it)/2}}{\langle\varphi_y|_B \rho_B |\varphi_y\rangle_B}.$$

Applying to Entropy

Special case: Entropy gain (also called Entropy Production)

- Specializing to entropy gives the following bound for a unital quantum channel $\mathcal{N}$:

$$H(\mathcal{N}(\rho)) - H(\rho) \geq -\log F(\rho, \mathcal{N}^\dagger(\mathcal{N}(\rho)))$$

- A different approach [BDW16] gives a stronger bound and applies to more general maps. For $\mathcal{N}$ a positive, subunital, trace-preserving map:

$$H(\mathcal{N}(\rho)) - H(\rho) \geq D(\rho \| \mathcal{N}^\dagger(\mathcal{N}(\rho))) \geq 0$$

Application to entropy uncertainty relations [BWW15]

- Let ρ_{ABE} be a state for Alice, Bob, and Eve, and let $\mathbb{X} \equiv \{P_A^x\}$ and $\mathbb{Z} = \{Q_A^z\}$ be projection-valued measures for Alice's system
- Define the post-measurement states:

$$\sigma_{XBE} \equiv \sum_x |x\rangle\langle x|_X \otimes \sigma_{BE}^x \qquad \text{where}$$

$$\sigma_{BE}^x \equiv \mathrm{Tr}_A\{(P_A^x \otimes I_{BE})\rho_{ABE}\}$$

$$\omega_{ZBE} \equiv \sum_z |z\rangle\langle z|_Z \otimes \omega_{BE}^z \qquad \text{where}$$

$$\omega_{BE}^z \equiv \mathrm{Tr}_A\{(Q_A^z \otimes I_{BE})\rho_{ABE}\}$$

- Then

$$H(Z|E)_\omega + H(X|B)_\sigma \geq -\log \max_{x,z} \|P_A^x Q_A^z\|_\infty^2 - \log F(\rho_{AB}, \mathcal{R}_{XB\to AB}(\sigma_{XB}))$$

Case of quantum Gaussian channels

- If σ is a Gaussian state and $\mathcal{N}$ is a Gaussian channel, then the Petz recovery map $\mathcal{P}_{\sigma,\mathcal{N}}$ is a Gaussian channel (result with Lami and Das).
- We have an explicit form for the Petz recovery map in terms of its action on the mean vector and covariance matrix of a quantum Gaussian state.
- We have the same for rotated Petz recovery maps.

Quantum cloning, partial trace, and recovery [LW16]

- Let $\omega^{(n)}$ be a state with support in the symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$, let $\pi_{\text{sym}}^{d,n}$ denote the maximally mixed state on this symmetric subspace, let $\mathcal{C}_{k\to n}$ denote a universal quantum cloning machine, and $\mathcal{P}_{n\to k}$ the symmetrize partial trace. Then

$$D(\omega^{(n)}\|\pi_{\text{sym}}^{d,n}) \geq D(\mathcal{P}_{n\to k}(\omega^{(n)})\|\mathcal{P}_{n\to k}(\pi_{\text{sym}}^{d,n})) + D(\omega^{(n)}\|(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\omega^{(n)})).$$

- With the same notation, the following inequality holds

$$D(\omega^{(k)}\|\pi_{\text{sym}}^{d,k}) \geq D(\mathcal{C}_{k\to n}(\omega^{(k)})\|\mathcal{C}_{k\to n}(\pi_{\text{sym}}^{d,k})) + D(\omega^{(k)}\|(\mathcal{P}_{n\to k}\circ\mathcal{C}_{k\to n})(\omega^{(k)})).$$

- So cloning machines and partial trace are dual to each other in the above sense.

Generality of approach [DW15]

- Technique is very general and can be used to prove inequalities for norms of multiple operators chained together (called "Swiveled Renyi Entropies" in [DW15], due to presence of "unitary swivels")
- Example: The following quantity

$$\widetilde{L}'_{\alpha}\left(\rho_{A_1\cdots A_l}\right) \equiv \frac{2}{\alpha'} \max_{\left\{V_{\rho_S}\right\}_S} \log \left\| \left[\prod_{S\in\mathcal{P}'} \rho_S^{-a_S\alpha'/2} V_{\rho_S}\right] \rho_{A_1\cdots A_l}^{1/2} \right\|_{2\alpha},$$

where $\alpha' = (\alpha - 1)/\alpha$ is monotone increasing in α for $\alpha \in [1/2, \infty]$.

- Another example: for positive semi-definite operators $C_1, \ldots, C_L$, a unitary V_{C_i} commuting with C_i, and $p \geq 1$, the quantity

$$\max_{V_{C_1},\ldots,V_{C_L}} \left\| C_1^{1/p} V_{C_1} \cdots C_L^{1/p} V_{C_L} \right\|_p^p$$

is monotone decreasing in p for $p \geq 1$. (See also [Wil16])

Generality of approach (ctd.) [DW15]

- Another example: Let $C_1, \ldots, C_L$ be positive semi-definite operators, and let $p > q \geq 1$. Then the following holds [DW15, Wil16]:

$$\log \left\| C_1^{1/p} C_2^{1/p} \cdots C_L^{1/p} \right\|_p^p \leq \int_{-\infty}^{\infty} dt \ \beta_{q/p}(t) \ \log \left\| C_1^{(1+it)/q} C_2^{(1+it)/q} \cdots C_L^{(1+it)/q} \right\|_q^q .$$

- By taking a limit: Let $C_1, \ldots, C_L$ be positive definite operators, and let $q \geq 1$. Then the following inequality holds [DW15, Wil16]:

$$\log \operatorname{Tr}\left\{\exp\left\{\log C_1 + \cdots + \log C_L\right\}\right\} \leq \int_{-\infty}^{\infty} dt \ \beta_0(t) \ \log \left\| C_1^{(1+it)/q} C_2^{(1+it)/q} \cdots C_L^{(1+it)/q} \right\|_q^q .$$

Conclusions

- The result in [Wil15, JSRWW15] applies to relative entropy differences, has a brief proof, and yields a universal recovery map (depending only on σ and $\mathcal{N}$).
- Applications in a variety of areas, including entropy gain [BDW16], entropic uncertainty [BWW15], quantum cloning [LW16], quantum Gaussian channels, etc.
- Later results of [DW15] clarify how the approach is very general and leads to many other inequalities
- It has been conjectured that the recovery map can be the Petz recovery map alone (not a rotated Petz map), but it is unclear whether this will be true.

References I

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

[BWW15] Mario Berta, Stephanie Wehner, and Mark M. Wilde. Measurement reversibility and entropic uncertainty. November 2015. arXiv:1511.00267.

[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.

[BDW16] Francesco Buscemi, Siddhartha Das, and Mark M. Wilde. Approximate reversibility in the context of entropy gain, information gain, and complete positivity . January 2016. arXiv:1601.01207.

[DW15] Frederic Dupuis and Mark M. Wilde. Swiveled Renyi entropies. June 2015. arXiv:1506.00981.

References II

[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.

[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.

[JSRWW15] Marius Junge, David Sutter, Renato Renner, Mark M. Wilde, and Andreas Winter. Universal recovery from a decrease of quantum relative entropy. September 2015. arXiv:1509.07127.

[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.

References III

[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.

[LW16] Marius Lemm and Mark M. Wilde. Information-theoretic limitations on approximate quantum cloning and broadcasting. August 2016. arXiv:1608.07569.

[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.

[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.

References IV

[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.

[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.

References V

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

[Wil16] Mark M. Wilde. Monotonicity of p-norms of multiple operators via unitary swivels. October 2016. arXiv:1610.01262.

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