Recoverability in quantum information theory

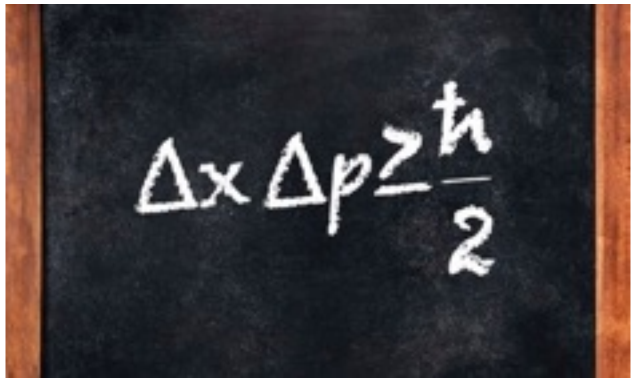
Mark M. Wilde

Department of Physics and Astronomy
Center for Computation and Technology
Louisiana State University
Baton Rouge, Louisiana 70803, USA

Based on arXiv:1505.04661
Accepted for publication in Proceedings of the Royal Society A

What do the second law of thermodynamics,

the Heisenberg uncertainty principle,



and the capacity of communication channels

have in common?

These physical limitations are a consequence of a **fundamental principle**, called

DECREASE OF QUANTUM RELATIVE ENTROPY

What is that?

G. Lindblad, *Communications in Mathematical Physics*, 40(2):147–151, June 1975.

Background

- A **quantum state** is described by a density operator acting on a Hilbert space:

$$\mathcal{D}(\mathcal{H}) = \{\rho : \rho \geq 0 \text{ and } \mathrm{Tr}(\rho) = 1\}$$

- A **quantum evolution** (channel) is a linear, completely positive trace-preserving map

$$\mathcal{N}(\rho) = \sum_i A_i \rho A_i^\dagger \quad \text{where} \quad \sum_i A_i^\dagger A_i = I$$

Physical Realization of a Quantum Channel

Stinespring representation theorem

Any quantum channel can be realized by adjoining a bath to the system, unitarily interacting them, and discarding the bath system:

$$\mathcal{N}(\rho) = \mathrm{Tr}_B\{U_{SB}(\rho_S \otimes \tau_B)U_{SB}^\dagger\}$$

W. F. Stinespring. *Proceedings of the American Mathematical Society*, 6(2):211–216, April 1955.

Quantum Relative Entropy

Let ρ be a density operator and σ be a positive semi-definite operator (σ could be a density operator).

Then the **quantum relative entropy** is defined as

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

Quantum relative entropy is a fundamental entropic measure of **distinguishability**.

H. Umegaki. *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

Decrease of Quantum Relative Entropy

Most important property

Quantum relative entropy **does not increase** with respect to a quantum channel:

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

Interpretation: If you're trying to distinguish ρ from σ, then it does not help to apply a channel first before trying to distinguish them.

G. Lindblad, *Communications in Mathematical Physics*, 40(2):147–151, June 1975.

"Mother of All Entropies"

Many entropies follow from quantum relative entropy:

von Neumann entropy:

$$S(\rho) = -\operatorname{Tr}\{\rho \log \rho\} = -D(\rho \| I)$$

Conditional entropy of ρ_{AB}:

$$\begin{aligned} S(A|B)_\rho &= S(\rho_{AB}) - S(\rho_B) \\ &= -D(\rho_{AB} \| I_A \otimes \rho_B) \end{aligned}$$

Mutual information of ρ_{AB}:

$$\begin{aligned} I(A;B)_\rho &= S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \\ &= D(\rho_{AB} \| \rho_A \otimes \rho_B) \end{aligned}$$

Relative Entropy in Thermodynamics

Suppose we have states ρ and σ and a Hamiltonian H

Helmholtz free energy is a thermodynamic potential measuring useful work at temperature T:

$$F(\rho) = \langle H \rangle_\rho - k_B T S(\rho)$$

Second law states that a transition from ρ to σ is possible via a thermal operation only if

$$F(\rho) \geq F(\sigma)$$

2nd Law and Relative Entropy

Rewrite free energy as **relative entropy to a thermal state**

$$F(\rho) = \mathrm{Tr}\{\rho H\} + k_B T\,\mathrm{Tr}\{\rho \log \rho\}$$
$$= k_B T\left[D(\rho\|\tau) - \log Z\right]$$

where $\tau = \exp\{-H/k_B T\}/Z$

So if there is a thermal operation such that

$$\mathcal{T}(\rho) = \sigma, \quad \mathcal{T}(\tau) = \tau$$

then **necessarily** $D(\rho\|\tau) \geq D(\mathcal{T}(\rho)\|\mathcal{T}(\tau))$

M. J. Donald. *Journal of Statistical Physics*, 49(1):81-87, October 1987.

Uncertainty Principle

The original **Heisenberg-Robertson uncertainty relation** has the following form:

$$\Delta X \Delta Z \geq \frac{1}{2} |\langle\psi|[X, Z]|\psi\rangle|$$

for two observables *X* and *Z* and a quantum state $|\psi\rangle$

Interpretation in terms of two different experiments

Deficiency: In finite dim., there always exists a $|\psi\rangle$ for which the lower bound vanishes, even if *X* and *Z* are incompatible (thus rendering the bound trivial)

W. Heisenberg. *Zeitschrift fur Physik*, 43:172–198, 1927.
H. P. Robertson. *Physical Review*, 34:163, 1929.

Entropic Uncertainty

Solution: Use **entropies** to quantify uncertainty:

$$H(X) + H(Z) \geq -\log c$$

where $\quad c := \max_{x,z} |\langle \psi_z | \phi_x \rangle|^2$

$H(X)$ is the **Shannon entropy** of the distribution resulting from measuring X on state $|\psi\rangle$, and similar for $H(Z)$

The parameter c quantifies **measurement incompatibility** and does not depend on $|\psi\rangle$

H. Maassen and J. B. M. Uffink. *Physical Review Letters*, 60(12):1103–1106, March 1988.

Relative Entropy and Entropic Uncertainty

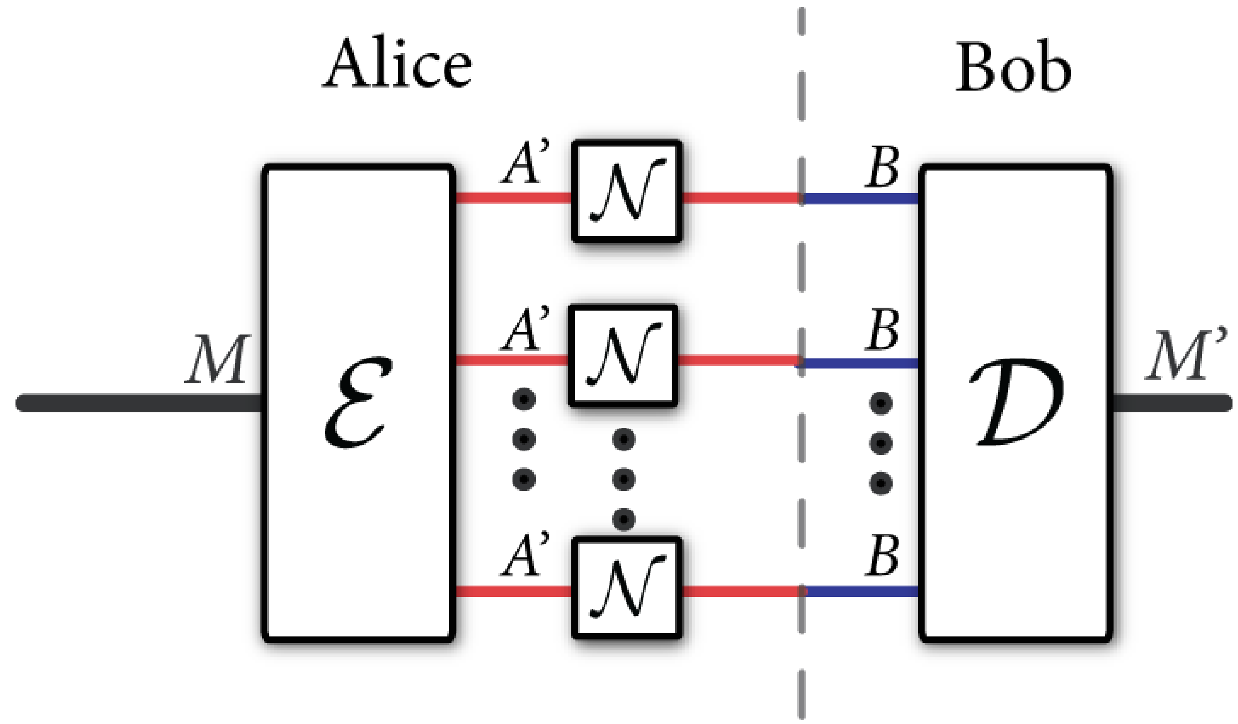
How to prove? Use relative entropy!

Let $\mathcal{M}_X$ and $\mathcal{M}_Z$ be measurement channels for *X* and *Z*

$$\begin{aligned} H(X) &= D(\psi \| \mathcal{M}_X(\psi)) \\ &\geq D(\mathcal{M}_Z(\psi) \| \mathcal{M}_Z(\mathcal{M}_X(\psi))) \\ &\geq -H(Z) - \log c \end{aligned}$$

P. J. Coles, L. Yu, and M. Zwolak. arXiv:1105.4865, May 2011.

Communication



- In a communication protocol, Alice wishes to send a message to Bob using a noisy channel *N* many times.
- They make use of an encoding and decoding in order to achieve the capacity of the channel (maximum possible rate)

Holevo Bound

- In 1973, Holevo proved a bound, essential to our understanding of capacity of quantum channels

- There is a **simple proof** using quantum relative entropy

- Let ρ_{MB} denote the state of the message system and the channel output. Then

$$\begin{aligned} I(M;B)_\rho &= D(\rho_{MB} \| \rho_M \otimes \rho_B) \\ &\geq D(\mathcal{D}_{B\to M'}(\rho_{MB}) \| \rho_M \otimes \mathcal{D}_{B\to M'}(\rho_B)) \\ &= I(M;M') \end{aligned}$$

- From there, we can relate to **success probability** and **rate**, and obtain an upper bound on **capacity**

A. S. Holevo. *Problems of Information Transmission*, 9:177–183, 1973.

Refining the Decrease of Quantum Relative Entropy

- Given the **fundamental role** of the inequality

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

  it is natural to ask further questions about it

- *What if the inequality is saturated?*

- *What if it is nearly saturated?*

Saturation Case

The inequality is a statement of **irreversibility**:

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

So, might suspect that saturation implies **reversibility**

Petz proved this:

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

if and only if

$$\exists \mathcal{R} : (\mathcal{R} \circ \mathcal{N})(\rho) = \rho \text{ and}$$

$$(\mathcal{R} \circ \mathcal{N})(\sigma) = \sigma$$

D. Petz. *Communications in Mathematical Physics*, 105(1):123–131, March 1986.
D. Petz. *Quarterly Journal of Mathematics*, 39(1):97– 108, 1988.

Saturation Case (ctd.)

- Petz proved even more: The recovery map *R* can take an **explicit form**, now known as the *Petz recovery map*

$$\mathcal{R}(X) := \sigma^{1/2}\mathcal{N}^{\dagger}\left([\mathcal{N}(\sigma)]^{-1/2}X[\mathcal{N}(\sigma)]^{-1/2}\right)\sigma^{1/2}$$

- The Petz recovery map **always** perfectly reverses the action of *N* on *σ*:

$$\mathcal{R}(\mathcal{N}(\sigma)) = \sigma$$

- And it **perfectly** reverses the action of *N* on *ρ* if

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

D. Petz. *Communications in Mathematical Physics*, 105(1):123–131, March 1986.
D. Petz. *Quarterly Journal of Mathematics*, 39(1):97– 108, 1988.

Near Saturation Case?

- It would be far more useful in **applications** to characterize the near saturation case

- Based on Petz's results, it is natural to wonder whether

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

implies that

$$\mathcal{R}(\mathcal{N}(\rho)) \approx \rho$$

- We cannot prove this at the moment, but can get *something nearly as good*…

Quantum Fidelity

- How to characterize the near-saturation case?

- Define the **fidelity** between two states ω and τ as

$$F(\omega, \tau) := \|\sqrt{\omega}\sqrt{\tau}\|_1^2$$

- Reduces to usual **squared overlap** for pure states

- Always between zero and one:

  Equal to one if and only if $\omega = \tau$ and

  Equal to zero if and only if ω orthogonal to τ

A. Uhlmann. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

Near Saturation Case

Theorem: There exists a real number *t* such that

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

where R^t is a **rotated** Petz recovery map:

$$\mathcal{R}^t(X) := (\mathcal{U}_{\sigma,t} \circ \mathcal{R} \circ \mathcal{U}_{\mathcal{N}(\sigma),-t})(X)$$

with the **unitary rotations** defined as

$$\mathcal{U}_{\omega,t}(X) := \omega^{it} X \omega^{-it}$$

Observe that

$$\mathcal{U}_{\omega,t}(\omega) = \omega$$

M. M. Wilde. Accepted in *Proceedings of the Royal Society A*, arXiv:1505.04661.

Interpretation of Result

- What does the theorem tell us?

- Any rotated Petz recovery map perfectly recovers σ:

$$\mathcal{R}^t(\mathcal{N}(\sigma)) = \sigma$$

- while if $D(\rho\|\sigma) \approx D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$

- then $\mathcal{R}^t(\mathcal{N}(\rho)) \approx \rho$

- The parameter *t* could depend on the state ρ, so the same recovery map does not work *universally* for all ρ

M. M. Wilde. Accepted in *Proceedings of the Royal Society A*, arXiv:1505.04661.

How to prove this?

- Proof involves two ingredients:

  1) Rényi entropies
  2) Hadamard's three-line theorem

- The approach is called the **method of complex interpolation** (*basic tool for non-commutative L_p spaces*)

Primer on Rényi Entropies

Rényi entropy:

$$S_\alpha(\rho) := \frac{\alpha}{1-\alpha} \log \|\rho\|_\alpha$$

where $\alpha \in (0,1) \cup (1,\infty)$

Key Properties:

$$\lim_{\alpha \to 1} S_\alpha(\rho) = S(\rho)$$

$$S_\alpha(\rho) \leq S_\beta(\rho) \text{ for } \alpha \geq \beta$$

Rényi Relative Entropy

Rényi relative entropy:

$$D_\alpha(\rho\|\sigma) := \frac{2\alpha}{\alpha-1}\log\left\|\sigma^{(1-\alpha)/2\alpha}\rho^{1/2}\right\|_{2\alpha}$$

where $\alpha \in (0,1)\cup(1,\infty)$

Key Properties: $\lim_{\alpha\to 1} D_\alpha(\rho\|\sigma) = D(\rho\|\sigma)$

$$D_{1/2}(\rho\|\sigma) = -\log F(\rho,\sigma)$$

$$D_\alpha(\rho\|\sigma) \geq D_\beta(\rho\|\sigma) \text{ for } \alpha \geq \beta$$

M. Muller-Lennert, F. Dupuis, O. Szehr, S. Fehr, M. Tomamichel. *J. Mathematical Physics*, 54(12):122203, Dec. 2013.
M. M. Wilde, A. Winter, D. Yang. *Communications in Mathematical Physics*, 331(2):593-622, October 2014.

Rényi "Monster" Quantity

Rényi generalization of a relative entropy difference:

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

where $\alpha \in (0,1) \cup (1,\infty)$ and $\alpha' := (\alpha - 1)/\alpha$

Key Properties:

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

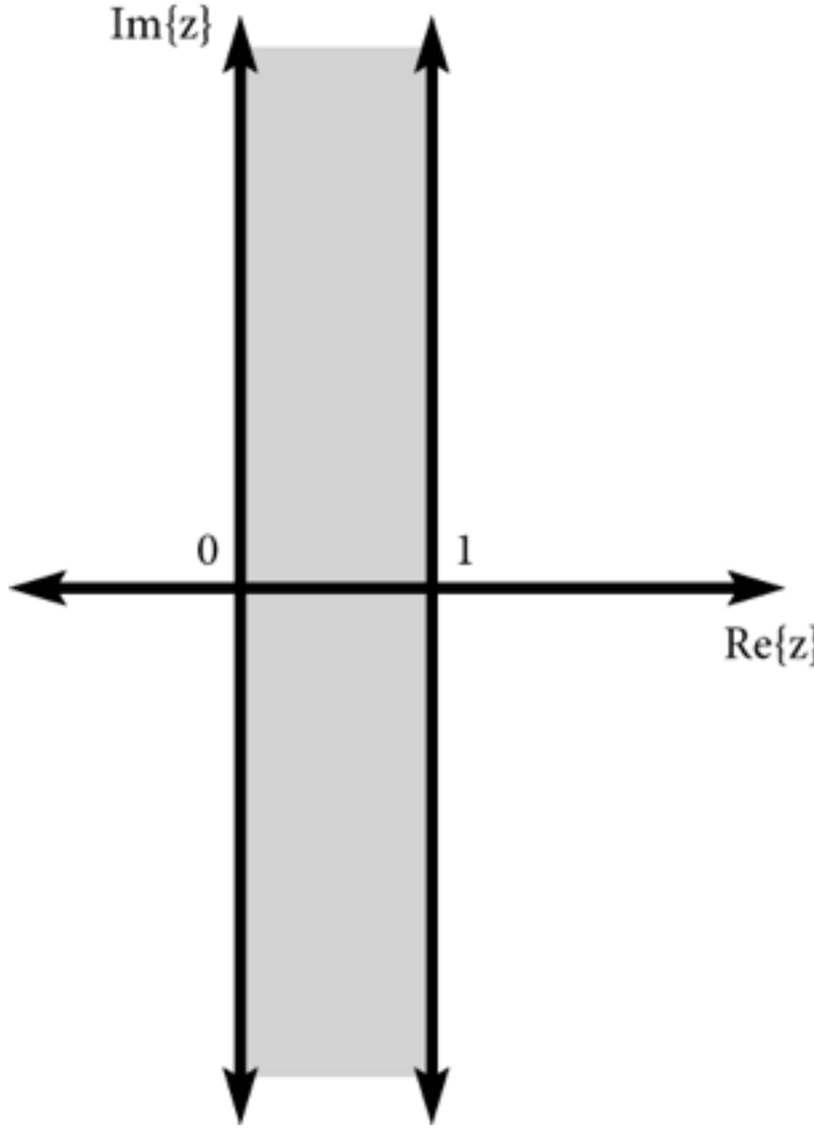
$$\widetilde{\Delta}_{1/2}(\rho,\sigma,\mathcal{N}) = -\log F(\rho, (\mathcal{R} \circ \mathcal{N})(\rho))$$

K. P. Seshadreesan, M. Berta, and M. M. Wilde. Accepted in *Journal of Physics A*. arXiv:1410.1443.

Hadamard 3-Line Theorem

- Let $S := \{z \in \mathbb{C} : 0 \leq \mathrm{Re}\{z\} \leq 1\}$
- Suppose *f*(*z*) holomorphic on the interior of *S* and continuous on its boundary
- Can bound *f*(*z*) anywhere inside *S* in terms of the maximum values of *f*(*z*) on the boundaries Re{*z*} = 0 and Re{*z*} = 1

  (*consequence of maximum modulus principle*)



Hadamard 3-Line Theorem

Formal statement:

Theorem Hadamard's three-line theorem *Let $f : S \to \mathbb{C}$ be a bounded function that is holomorphic in the interior of S and continuous on the boundary. For $k = 0, 1$ let*

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

Then for every $0 \le \theta \le 1$ we have $|f(\theta)| \le M_0^{1-\theta} M_1^{\theta}$.

Can extend to a statement for operator-valued functions:

Theorem *Let*

$$S \equiv \{z \in \mathbb{C} : 0 \le \mathrm{Re}\{z\} \le 1\}, \tag{2.1}$$

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.[1] *Let $\theta \in (0, 1)$ and define p_θ by*

$$\frac{1}{p_\theta} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}, \tag{2.2}$$

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

$$\|G(\theta)\|_{p_\theta} \le M_0^{1-\theta} M_1^{\theta}. \tag{2.3}$$

Proof Conclusion

Can use these tools to conclude the following inequality for all $\alpha \in (1/2, 1)$

$$\widetilde{\Delta}_\alpha(\rho, \sigma, \mathcal{N}) \geq -\log \sup_t F(\rho, (\mathcal{R}^t \circ \mathcal{N})(\rho))$$

Taking the limit *α* → 1 then gives that there exists a real number *t* such that

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

M. M. Wilde. Accepted in *Proceedings of the Royal Society A*, arXiv:1505.04661.

Universal Recovery

Recent improvement: Can pick the recovery map to be explicit and universal (exclusively a function of $\mathcal{N}$ and σ)

$$\overline{\mathcal{R}}(X) := \int_{-\infty}^{\infty} dt \; \frac{\pi}{2(\cosh(\pi t) + 1)} \; \mathcal{R}^t(X)$$

We then get the following inequality holding for all ρ:

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

Follows from a strengthening of Hadamard 3-line due to Hirschman

M. Junge, R. Renner, D. Sutter, M. M. Wilde, A. Winter. In preparation.

Consequences

- **Refinement of 2nd law**: if difference of free energies is small, then can reverse transformation approximately without using any energy (arXiv:1506.08145)

- **Uncertainty principle**: can add in another term related to how well one can reverse one of the measurements (unpublished)

- **Holevo bound**: if difference between mutual information before and after measurement is small, then states are approximately commuting (arXiv:1505.04661)

- Other applications in entanglement theory, quantum correlations, quantum measurements, Fisher information, open system dynamics (exploring with Siddhartha Das)