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
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 $\rho$ and positive semi-definite $\sigma$ as

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

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 $\rho$ or $\sigma$. With a constraint of $\varepsilon \in (0, 1)$ on the Type I error of misidentifying $\rho$, then the optimal error exponent for the Type II error of misidentifying $\sigma$ is $D(\rho \parallel \sigma)$. 
Fundamental law of quantum information theory

**Monotonicity of quantum relative entropy [Lin75, Uhl77]**
Let $\rho$ be a state, let $\sigma$ be positive semi-definite, and let $\mathcal{N}$ be a quantum channel. Then

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

“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

\[
\rho = (\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho), \quad \sigma = (\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\sigma)
\]

- 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 $\sigma$ perfectly from $\mathcal{N}(\sigma)$ while recovering $\rho$ from $\mathcal{N}(\rho)$ approximately? [WL12]
One-shot measure of similarity for quantum states

Fidelity [Uhl76]

Fidelity between $\rho$ and $\sigma$ 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 $\rho$ could pass a test for being a purification of $\sigma$. 
**New result of [Wil15, JSRWW15]**

**Recoverability Theorem**

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

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

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

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

$\mathcal{P}_{\sigma,\mathcal{N}}$ 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 $\omega$ a positive semi-definite operator.

**Two tools for proof**

Rényi generalization of a relative entropy difference and the Stein–Hirschman operator interpolation theorem
Universal Recoverability Corollary

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

$$D(\rho \parallel \sigma) − D(\mathcal{N}(\rho) \parallel \mathcal{N}(\sigma)) \geq − \log F(\rho, R_{\sigma,\mathcal{N}}(\mathcal{N}(\rho))),$$

where

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

(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]**

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

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**

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

\[
\tilde{\Delta}_{1/2}(\rho, \sigma, \mathcal{N}) = - \log F(\rho, \mathcal{P}_{\sigma, \mathcal{N}}(\mathcal{N}(\rho))).
\]
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 \( G : \overline{S} \rightarrow L(\mathcal{H}) \) 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 \( p_\theta \) by

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

where \( p_0, p_1 \in [1, \infty] \).
Then the following bound holds

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

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

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

\( \lim_{\theta \downarrow 0} \beta_\theta(t) = p(t). \)
Proof of Recoverability Theorem

Tune parameters

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

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

Evaluate norms

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

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

Mark M. Wilde (LSU)
Apply the Stein–Hirschman theorem

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

Final step

Apply a minus sign, multiply both sides by \(2/\theta\), and take the limit as \(\theta \downarrow 0\) to conclude.
Specializing to the Holevo Bound

Specializing to the Holevo bound leads to a refinement. Given

\[ \rho_{XB} \equiv \sum_x p_X(x) |x\rangle\langle x| \otimes \rho^x_B, \quad \omega_{XY} \equiv \sum_y \langle \varphi^y_B | \rho_{XB} | \varphi^y_B \rangle |y\rangle \langle y| \].

Then the following inequality holds

\[ I(X; B)_\rho - I(X; Y)_\omega \geq -2 \log \sum_x p_X(x) \sqrt{F(\rho^x_B, E_B(\rho^x_B))}, \]

where \( E_B \) is an entanglement-breaking map of the form

\[ E_B(\cdot) \equiv \int_{-\infty}^{\infty} dt \beta_0(t) \sum_y \langle \varphi_y_B(\cdot) | \varphi_y_B \rangle \frac{\rho_B^{(1+it)/2} | \varphi_y \rangle \langle \varphi_y | B \rho_B^{(1-it)/2}}{\langle \varphi_y | B \rho_B | \varphi_y \rangle_B}. \]
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:

$$H(\mathcal{N}(\rho)) - H(\rho) \geq D(\rho \parallel \mathcal{N}^\dagger(\mathcal{N}(\rho))) \geq 0$$
Let $\rho_{ABE}$ be a state for Alice, Bob, and Eve, and let $X \equiv \{P^x_A\}$ and $Z = \{Q^z_A\}$ be projection-valued measures for Alice’s system.

Define the post-measurement states:

$$
\sigma_{XBE} \equiv \sum_x |x\rangle\langle x| X \otimes \sigma^x_{BE}
$$

where

$$
\sigma^x_{BE} \equiv \text{Tr}_A\{(P^x_A \otimes I_{BE})\rho_{ABE}\}
$$

$$
\omega_{ZBE} \equiv \sum_z |z\rangle\langle z| Z \otimes \omega^z_{BE}
$$

where

$$
\omega^z_{BE} \equiv \text{Tr}_A\{(Q^z_A \otimes I_{BE})\rho_{ABE}\}
$$

Then

$$
H(Z|E)_\omega + H(X|B)_\sigma
\geq - \log \max_{x,z} \|P^x_A Q^z_A\|_\infty^2 - \log F(\rho_{AB}, R_{XB\rightarrow AB}(\sigma_{XB}))
$$
If $\sigma$ 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.
Let $\omega^{(n)}$ be a state with support in the symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$, let $\pi_{sym}^{d,n}$ denote the maximally mixed state on this symmetric subspace, let $C_{k \rightarrow n}$ denote a universal quantum cloning machine, and $P_{n \rightarrow k}$ the symmetrize partial trace. Then

$$D(\omega^{(n)} \parallel \pi_{sym}^{d,n}) \geq D(P_{n \rightarrow k}(\omega^{(n)}) \parallel P_{n \rightarrow k}(\pi_{sym}^{d,n}))$$

$$+ D(\omega^{(n)} \parallel (C_{k \rightarrow n} \circ P_{n \rightarrow k})(\omega^{(n)})).$$

With the same notation, the following inequality holds

$$D(\omega^{(k)} \parallel \pi_{sym}^{d,k}) \geq D(C_{k \rightarrow n}(\omega^{(k)}) \parallel C_{k \rightarrow n}(\pi_{sym}^{d,k}))$$

$$+ D(\omega^{(k)} \parallel (P_{n \rightarrow k} \circ C_{k \rightarrow n})(\omega^{(k)})).$$

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

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

where $\alpha' = (\alpha - 1) / \alpha$ is monotone increasing in $\alpha$ 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]:

$$\log \text{Tr} \left\{ \exp \left\{ \log C_1 + \cdots + \log C_L \right\} \right\} \leq \int_{-\infty}^{\infty} dt \ \beta_0(t) \ \log \left\| C_1^{(1+it)/q} C_2^{(1+it)/q} \cdots C_L^{(1+it)/q} \right\|^q_q.$$
The result in [Wil15, JSRWW15] applies to relative entropy differences, has a brief proof, and yields a universal recovery map (depending only on $\sigma$ and $N$).

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 III


