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

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

whenever $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ 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 $\rho$ 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 $D(\rho\|\sigma)$. 
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

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

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

“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

Let $\rho_{ABC}$ 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 \( \mathcal{R}_{\sigma,\mathcal{N}}^P \) such that

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

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

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

- 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

\[
\text{Tr}\{\mathcal{R}_{\sigma,N}^{P}(\omega)\} = \text{Tr}\{\sigma^{1/2}\mathcal{N}^\dagger \left( (\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2} \right) \sigma^{1/2} \} \\
= \text{Tr}\{\sigma\mathcal{N}^\dagger \left( (\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2} \right) \} \\
= \text{Tr}\{\mathcal{N}(\sigma)(\mathcal{N}(\sigma))^{-1/2}\omega(\mathcal{N}(\sigma))^{-1/2} \} \\
\leq \text{Tr}\{\omega\}
\]

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

\[
\mathcal{R}_{\sigma,N}^{P}(\mathcal{N}(\sigma)) = \sigma^{1/2}\mathcal{N}^\dagger \left( (\mathcal{N}(\sigma))^{-1/2}\mathcal{N}(\sigma)(\mathcal{N}(\sigma))^{-1/2} \right) \sigma^{1/2} \\
= \sigma^{1/2}\mathcal{N}^\dagger (I) \sigma^{1/2} \\
= \sigma
\]
### Functoriality

**Normalization [LW14]**

For identity channel, the Petz recovery map is the identity map:
\[ \mathcal{R}_{\sigma,\text{id}}^P = \text{id}. \] “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:
\[ \mathcal{R}_{\sigma_1 \otimes \sigma_2, N_1 \otimes N_2}^P = \mathcal{R}_{\sigma_1, N_1}^P \otimes \mathcal{R}_{\sigma_2, N_2}^P. \] “Individual action suffices for ‘pretty good’ recovery of individual states”

**Composition [LW14]**

Given \( N_2 \circ N_1 \), then \( \mathcal{R}_{\sigma, N_2 \circ N_1}^P = \mathcal{R}_{\sigma, N_1}^P \circ \mathcal{R}_{N_1(\sigma), N_2}^P. \) “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 \( \omega_{BC} \), i.e.,

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

**Approximate case for strong subadditivity**
- What can we say when $H(B|C)_\omega - H(B|AC)_\omega = \varepsilon$?
- Is $\omega_{ABC}$ approximately recoverable from $\omega_{BC}$ by performing a recovery map on system $C$ alone? [WL12]
**Other measures of similarity for quantum states**

### Trace distance

Trace distance between $\rho$ and $\sigma$ 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 $\rho$ and $\sigma$ with an optimal quantum measurement.

### 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 $\sigma$.

### Bures distance [Bur69]

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

Mark M. Wilde (LSU)
Breakthrough result of [FR14]

**Remainder term for strong subadditivity [FR14]**

∃ unitary channels $U_C$ and $V_{AC}$ such that

$$H(B|C) - H(B|AC) \geq -\log F(\omega_{ABC}, (V_{AC} \circ R_{C\rightarrow AC} \circ U_C)(\omega_{BC}))$$

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

**Remainder term for monotonicity of relative entropy [BLW14]**

∃ unitary channels $U$ and $V$ such that

$$D(\rho||\sigma) - D(\mathcal{N}(\rho)||\mathcal{N}(\sigma)) \geq -\log F(\rho, (V \circ R_{\sigma,\mathcal{N}} \circ U)(\mathcal{N}(\rho)))$$

Again, nothing known from [BLW14] about $U$ and $V$. 

Mark M. Wilde (LSU) 13 / 23
New result of [Wil15]

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

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

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

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

$\mathcal{R}_{\sigma,\mathcal{N}}^{P}$ 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 Hadamard three-line theorem.
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 \( U_{S \rightarrow BE} \) is an isometric extension of \( \mathcal{N} \).

**Important properties**

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

\[ \tilde{\Delta}_{1/2} (\rho, \sigma, \mathcal{N}) = - \log F \left( \rho, \mathcal{R}_{\sigma, \mathcal{N}}^P(\mathcal{N}(\rho)) \right). \]
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 \( G : S \rightarrow L (\mathcal{H}) \) be a bounded map that is holomorphic on the interior of \( S \) and continuous on the boundary. Let \( \theta \in (0, 1) \) and define \( p_\theta \) 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

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

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

Then

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

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

Apply the three-line theorem to conclude that

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

Take a negative logarithm and the limit as \( \theta \downarrow 0 \) to conclude.
SSA refinement as a special case

Let $\rho_{ABC}$ 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

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

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

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

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

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

and the partial isometric maps $U_{\rho_{AC}, t}$ and $U_{\rho_{C}, -t}$ 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 $\sigma$ and $\mathcal{N}$ and has the form [SRWW15]:

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

for some probability measure $\mu$.

- It is still conjectured that the recovery map can be the Petz recovery map alone (not a rotated Petz map).


References III


References IV


