Entropy Inequalities

Mario Berta

Institute for Quantum Information and Matter
California Institute of Technology

Based on joint work with Marius Lemm, Kaushik Seshadreesan, Marco Tomamichel, Mark Wilde

Caltech

Entropy I

- Shannon entropy of random variable $(\mathcal{X}, \{p_x\}_{x\in\mathcal{X}})$:

$$H(X) := -\sum_{x\in\mathcal{X}} p_x \log p_x$$

—> "measure of uncertainty". Ex: $H(X)_\delta = 0$, $H(X)_{\mathrm{unif}} = \log|\mathcal{X}|$

[Shannon (48)]

Entropy I

- Shannon entropy of random variable $(\mathcal{X}, \{p_x\}_{x\in\mathcal{X}})$:

$$H(X) := -\sum_{x\in\mathcal{X}} p_x \log p_x$$

[Shannon (48)]

—> "measure of uncertainty". Ex: $H(X)_\delta = 0$, $H(X)_{\text{unif}} = \log|\mathcal{X}|$

- Turns out to be an important quantity in classical physics, classical information theory, classical theory of computing, etc.

Entropy I

- Shannon entropy of random variable $(\mathcal{X}, \{p_x\}_{x\in\mathcal{X}})$:

$$H(X) := -\sum_{x\in\mathcal{X}} p_x \log p_x$$

[Shannon (48)]

—> "measure of uncertainty". Ex: $H(X)_\delta = 0$, $H(X)_{\text{unif}} = \log|\mathcal{X}|$

- Turns out to be an important quantity in classical physics, classical information theory, classical theory of computing, etc.

- Von Neumann entropy of quantum state ρ_A:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

$\left(\rho_A \in \mathrm{Lin}(\mathcal{H}_A) \text{ with } \rho_A \geq 0,\ \mathrm{tr}\left[\rho_A\right] = 1\right)$

[von Neumann (32)]

Ex: $H(A)_\psi = 0$, $H(A)_{\frac{1}{|A|}} = \log|A|$

Entropy I

- Shannon entropy of random variable $(\mathcal{X}, \{p_x\}_{x\in\mathcal{X}})$:

$$H(X) := -\sum_{x\in\mathcal{X}} p_x \log p_x$$

[Shannon (48)]

—> "measure of uncertainty". Ex: $H(X)_\delta = 0$
$H(X)_{\mathrm{unif}} = \log|\mathcal{X}|$

- Turns out to be an important quantity in classical physics, classical information theory, classical theory of computing, etc.

- Von Neumann entropy of quantum state ρ_A:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

$\left(\rho_A \in \mathrm{Lin}(\mathcal{H}_A) \text{ with } \rho_A \geq 0,\ \mathrm{tr}\left[\rho_A\right] = 1\right)$

Ex: $H(A)_\psi = 0$
$H(A)_{\frac{1}{|A|}} = \log|A|$

[von Neumann (32)]

- Turns out to be an important quantity in quantum physics, quantum information theory, quantum theory of computing, etc.

Entropy I

- Shannon entropy of random variable $(\mathcal{X}, \{p_x\}_{x\in\mathcal{X}})$:

$$H(X) := -\sum_{x\in\mathcal{X}} p_x \log p_x$$

[Shannon (48)]

—> "measure of uncertainty". Ex: $H(X)_\delta = 0$, $H(X)_{\text{unif}} = \log|\mathcal{X}|$

- Turns out to be an important quantity in classical physics, classical information theory, classical theory of computing, etc.

- Von Neumann entropy of quantum state ρ_A:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

$\left(\rho_A \in \mathrm{Lin}(\mathcal{H}_A) \text{ with } \rho_A \geq 0,\ \mathrm{tr}\left[\rho_A\right] = 1\right)$

Ex: $H(A)_\psi = 0$, $H(A)_{\frac{1}{|A|}} = \log|A|$

[von Neumann (32)]

- Turns out to be an important quantity in quantum physics, quantum information theory, quantum theory of computing, etc.

- I would like to study the mathematical properties of this quantity.

Entropy II

- Entropy:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

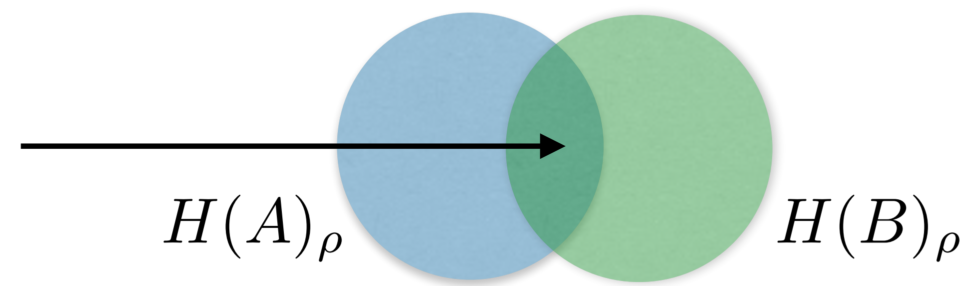
Entropy II

- Entropy:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

- Mutual information:

$$I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$$



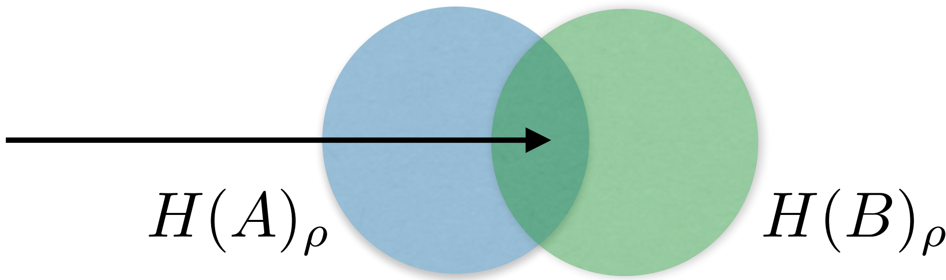
Entropy II

- Entropy:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

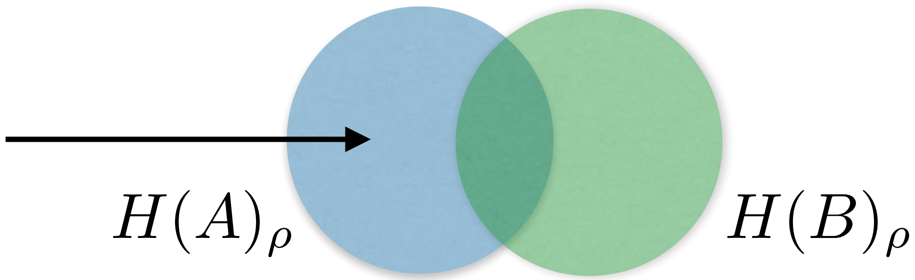
- Mutual information:

$$I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$$



- Conditional entropy:

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$$



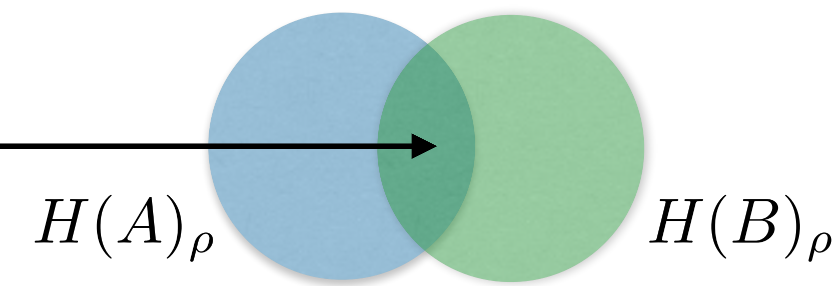
Entropy II

- Entropy:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

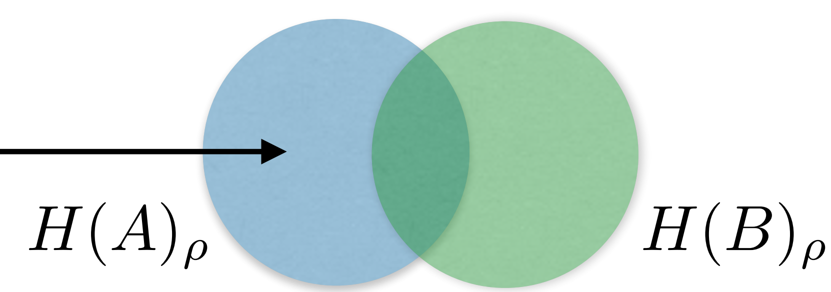
- Mutual information:

$$I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$$



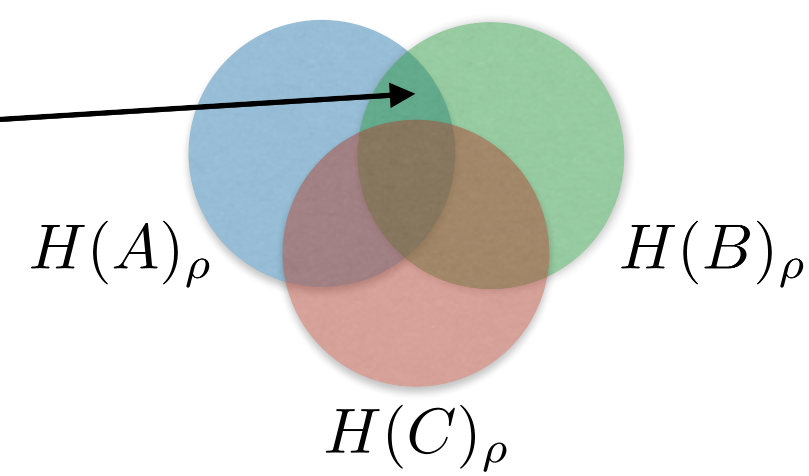
- Conditional entropy:

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$$



- Conditional mutual information:

$$\begin{aligned} I(A:B|C)_\rho := {} & H(AC)_\rho + H(BC)_\rho \\ & - H(ABC)_\rho - H(C)_\rho \end{aligned}$$



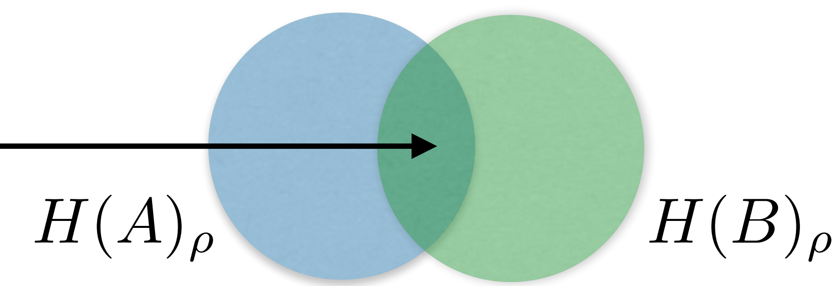
Entropy II

- Entropy:

$$H(A)_\rho := -\mathrm{tr}\left[\rho_A \log \rho_A\right]$$

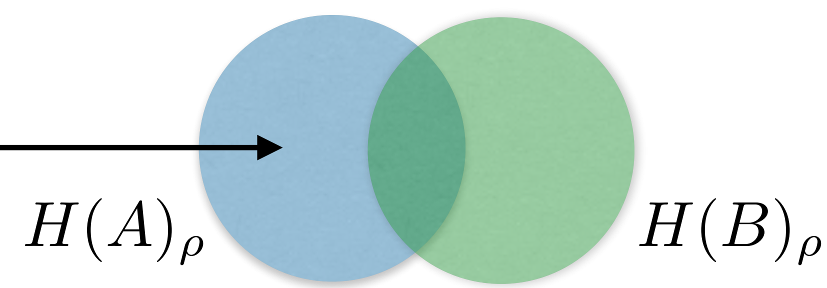
- Mutual information:

$$I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$$



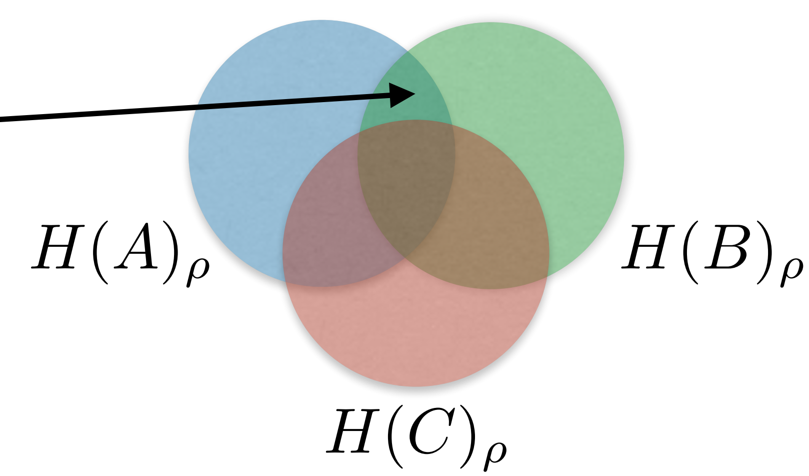
- Conditional entropy:

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$$



- Conditional mutual information:

$$\begin{aligned} I(A:B|C)_\rho := &\, H(AC)_\rho + H(BC)_\rho \\ &- H(ABC)_\rho - H(C)_\rho \end{aligned}$$



- … (other combinations, more parties, etc.)

Outline

- Entropy - operational significance
- Entropy inequalities - laws of information theory
- Recent progress on refining these laws
- Extension: quantum relative entropy and its inequalities
- Conclusions

Outline

- Entropy - operational significance
- Entropy inequalities - laws of information theory
- Recent progress on refining these laws
- Extension: quantum relative entropy and its inequalities
- Conclusions

Operational Significance I

- **Compression**: $A \overset{\text{Enc}}{\to} M \overset{\text{Dec}}{\to} A$

  —> asymptotic rate for compression of $\rho_A^{\otimes n}$ is

$$\lim_{n\to\infty} \frac{|M^n|}{n} = H(A)_\rho$$

[Ohya, Petz (93)] [Schumacher (95)]

Operational Significance I

- **Compression**: $A \overset{\text{Enc}}{\to} M \overset{\text{Dec}}{\to} A$

  —> asymptotic rate for compression of $\rho_A^{\otimes n}$ is $\lim_{n\to\infty} \frac{|M^n|}{n} = H(A)_\rho$

  [Ohya, Petz (93)] [Schumacher (95)]

- **Communication** over channel: $M \overset{\text{Enc}}{\to} \mathcal{N}_{A\to B} \overset{\text{Dec}}{\to} M$

  —> asymptotic rate of transmission (entanglement assisted) for $\mathcal{N}_{A\to B}^{\otimes n}$ is

  $\lim_{n\to\infty} \frac{|M^n|}{n} = \max_\rho I(B:R)_{\mathcal{N}(\rho)}$ where $(\mathcal{N}_{A\to B} \otimes \mathcal{I}_R)(\rho_{AR})$ with ρ_{AR} pure

entanglement assisted channel capacity

[Bennett et al. (99, 02)]

Operational Significance I

- **Compression**: $A \xrightarrow{\text{Enc}} M \xrightarrow{\text{Dec}} A$

  —> asymptotic rate for compression of $\rho_A^{\otimes n}$ is $\lim_{n\to\infty} \frac{|M^n|}{n} = H(A)_\rho$

  [Ohya, Petz (93)] [Schumacher (95)]

- **Communication** over channel: $M \xrightarrow{\text{Enc}} \mathcal{N}_{A\to B} \xrightarrow{\text{Dec}} M$

  —> asymptotic rate of transmission (entanglement assisted) for $\mathcal{N}_{A\to B}^{\otimes n}$ is

  $\lim_{n\to\infty} \frac{|M^n|}{n} = \max_\rho I(B:R)_{\mathcal{N}(\rho)}$ where $(\mathcal{N}_{A\to B} \otimes \mathcal{I}_R)(\rho_{AR})$ with ρ_{AR} pure

entanglement assisted channel capacity

[Bennett et al. (99, 02)]

- **Entanglement manipulation** (distillation, dilution, etc.)

- **Distributed compression**: quantum state merging, quantum state splitting, the mother protocol, quantum state redistribution etc.

- **...**

Operational Significance II

- Entropy, conditional entropy, mutual information, conditional mutual information etc. crucial (tool) for:
  - Quantum Shannon theory (cf. last slide)
  - Entanglement / correlation measures
  - Entropic uncertainty relations
  - Entanglement in quantum many body systems
  - Quantum error correction
  - Quantum statistical mechanics
  - Thermodynamics
  - Quantum communication complexity
  - Quantum de Finetti theorems
  - …

Outline

- Entropy - operational significance
- Entropy inequalities - laws of information theory
- Recent progress on refining these laws
- Extension: quantum relative entropy and its inequalities
- Conclusions

Entropy Inequalities I

- Entropy: $0 \leq H(A)_\rho \leq \log |A|$

Entropy Inequalities I

- Entropy: $$0 \leq H(A)_\rho \leq \log |A|$$
- Mutual information: $$0 \leq I(A:B)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$

Entropy Inequalities I

- Entropy: $$0 \leq H(A)_\rho \leq \log|A|$$

- Mutual information: $I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$ $$0 \leq I(A:B)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$

- Conditional entropy: $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$ $$-\log|A| \leq H(A|B)_\rho \leq \log|A|$$

Entropy Inequalities I

- Entropy: $$0 \leq H(A)_\rho \leq \log|A|$$

- Mutual information: $$0 \leq I(A:B)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$

- Conditional entropy: $$-\log|A| \leq H(A|B)_\rho \leq \log|A|$$
  $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$

- Conditional mutual information: $$0 \leq I(A:B|C)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $$I(A:B|C)_\rho := H(AC)_\rho + H(BC)_\rho - H(ABC)_\rho - H(C)_\rho$$

Entropy Inequalities I

- Entropy: $$0 \leq H(A)_\rho \leq \log|A|$$
- Mutual information: $$0 \leq I(A:B)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$
- Conditional entropy: $$-\log|A| \leq H(A|B)_\rho \leq \log|A|$$
  $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$
- Conditional mutual information: $$0 \leq I(A:B|C)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $I(A:B|C)_\rho := H(AC)_\rho + H(BC)_\rho - H(ABC)_\rho - H(C)_\rho$
- **Strong subadditivity of entropy (SSA)**:
  $$I(A:B|C)_\rho \geq 0$$
  $$\Leftrightarrow H(A|C)_\rho \geq H(A|BC)_\rho$$

[Lieb, Ruskai (73)]

Entropy Inequalities I

- Entropy: $$0 \leq H(A)_\rho \leq \log|A|$$
- Mutual information: $$0 \leq I(A:B)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$
- Conditional entropy: $$-\log|A| \leq H(A|B)_\rho \leq \log|A|$$
  $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$
- Conditional mutual information: $$0 \leq I(A:B|C)_\rho \leq \min\{2\log|A|, 2\log|B|\}$$
  $I(A:B|C)_\rho := H(AC)_\rho + H(BC)_\rho - H(ABC)_\rho - H(C)_\rho$
- **Strong subadditivity of entropy (SSA)**:

  —> generates all other inequalities,
  "all we know about entropy"!

$$I(A:B|C)_\rho \geq 0$$
$$\Leftrightarrow H(A|C)_\rho \geq H(A|BC)_\rho$$

[Lieb, Ruskai (73)]

Entropy Inequalities II

- Can we improve SSA (in an operationally useful way)?
  [Ibinson, Linden, Winter (06)] [Li, Winter (12)]
  [Christandl, Schuch, Winter (09)]
  [Brandao, Christandl, Yard (10)]

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

vs.

$I(A:B|C)_\rho \geq f(\rho_{ABC})$?

Entropy Inequalities II

- Can we improve SSA (in an operationally useful way)?
  [Ibinson, Linden, Winter (06)] [Li, Winter (12)]
  [Christandl, Schuch, Winter (09)]
  [Brandao, Christandl, Yard (10)]

$I(A:B|C)_\rho \geq 0$
vs.
$I(A:B|C)_\rho \geq f(\rho_{ABC})$?

- What are the equality conditions of SSA?

$$I(A:B|C)_\rho = 0 \Leftrightarrow \rho_{ABC} = \left(\mathcal{I}_A \otimes \Lambda^{\text{Petz}}_{C\to BC}\right)(\rho_{AC})$$

recoverable states
[Petz (88)]

with $\Lambda^{\text{Petz}}_{C\to BC}(\cdot) := \rho_{BC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{BC}^{1/2}$

—> this is a quantum operation, recovery map: $\Lambda^{\text{Petz}}_{C\to BC}(\rho_C) = \rho_{BC}$

Entropy Inequalities II

- Can we improve SSA (in an operationally useful way)?
  [Ibinson, Linden, Winter (06)] [Li, Winter (12)]
  [Christandl, Schuch, Winter (09)]
  [Brandao, Christandl, Yard (10)]

$I(A:B|C)_\rho \geq 0$
vs.
$I(A:B|C)_\rho \geq f(\rho_{ABC})$?

- What are the equality conditions of SSA?

$$I(A:B|C)_\rho = 0 \Leftrightarrow \rho_{ABC} = \left(\mathcal{I}_A \otimes \Lambda^{\text{Petz}}_{C\to BC}\right)(\rho_{AC})$$

recoverable states
[Petz (88)]

with $\Lambda^{\text{Petz}}_{C\to BC}(\cdot) := \rho_{BC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{BC}^{1/2}$

—> this is a quantum operation, recovery map: $\Lambda^{\text{Petz}}_{C\to BC}(\rho_C) = \rho_{BC}$

- This characterises quantum states with conditional quantum mutual information equal to zero, but what about: $I(A:B|C)_\rho \approx 0 \Rightarrow \rho_{ABC} = ?$

—> maybe: $I(A:B|C)_\rho \geq f(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC}))$?

Outline

- Entropy - operational significance
- Entropy inequalities - laws of information theory
- Recent progress on refining these laws
- Extension: quantum relative entropy and its inequalities
- Conclusions

Refinements I

- One way of lower bounding entropy is via **quantum Renyi entropies**:

$$H_\alpha(A)_\rho := \frac{1}{1-\alpha} \log \mathrm{tr}\left[\rho_A^\alpha\right], \quad \alpha \geq 0$$ [Renyi (61)]

  - von Neumann entropy: $H_1(A)_\rho = H(A)_\rho$
  - monotone in Renyi parameter: $\alpha \geq \beta \quad \Rightarrow \quad H_\alpha(A)_\rho \geq H_\beta(A)_\rho$
  - in particular (Pinsker's inequality): $H(A)_\rho \geq H_{1/2}(A)_\rho = \log \mathrm{tr}\left[\sqrt{\rho_A}\right]^2$

Refinements I

- One way of lower bounding entropy is via **quantum Renyi entropies**:

$$H_\alpha(A)_\rho := \frac{1}{1-\alpha} \log \mathrm{tr}\left[\rho_A^\alpha\right], \quad \alpha \geq 0$$ [Renyi (61)]

  - von Neumann entropy: $H_1(A)_\rho = H(A)_\rho$
  - monotone in Renyi parameter: $\alpha \geq \beta \quad \Rightarrow \quad H_\alpha(A)_\rho \geq H_\beta(A)_\rho$
  - in particular (Pinsker's inequality): $H(A)_\rho \geq H_{1/2}(A)_\rho = \log \mathrm{tr}\left[\sqrt{\rho_A}\right]^2$

- Define **Renyi conditional quantum mutual information**:

$I_\alpha(A:B|C)_\rho = \ldots$ —> with: $I_1(A:B|C)_\rho = I(A:B|C)_\rho$

[B., Wilde, Seshadreesan (14)]

Refinements I

- One way of lower bounding entropy is via **quantum Renyi entropies**:

$$H_\alpha(A)_\rho := \frac{1}{1-\alpha} \log \mathrm{tr}\left[\rho_A^\alpha\right], \quad \alpha \geq 0$$ [Renyi (61)]

  - von Neumann entropy: $H_1(A)_\rho = H(A)_\rho$
  - monotone in Renyi parameter: $\alpha \geq \beta \quad \Rightarrow \quad H_\alpha(A)_\rho \geq H_\beta(A)_\rho$
  - in particular (Pinsker's inequality): $H(A)_\rho \geq H_{1/2}(A)_\rho = \log \mathrm{tr}\left[\sqrt{\rho_A}\right]^2$

- Define **Renyi conditional quantum mutual information**:

$I_\alpha(A:B|C)_\rho = \ldots$ —> with: $I_1(A:B|C)_\rho = I(A:B|C)_\rho$

[B., Wilde, Seshadreesan (14)]

- Monotone? $\alpha \geq \beta \quad \Rightarrow \quad I_\alpha(A:B|C)_\rho \geq I_\beta(A:B|C)_\rho$?

Refinements II

- **Conjecture:** $$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})) \ ?$$

[B., Wilde, Seshadreesan (14)]

$$F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 \quad \|\rho\|_1 := \mathrm{tr}\left[\sqrt{\rho^\dagger \rho}\right]$$

$$\Lambda^{\text{Petz}}_{C\to BC}(\cdot) := \rho_{BC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{BC}^{1/2}$$

—> previous ideas: $I(A:B|C)_\rho \geq \frac{1}{4}\left\|\rho_{ABC} - \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})\right\|_1^2 \ ?$

[Kim (13)] [Zhang (13)]

Refinements II

- **Conjecture:** $$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC}))\ ?$$

[B., Wilde, Seshadreesan (14)]

$$F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 \quad \|\rho\|_1 := \mathrm{tr}\left[\sqrt{\rho^\dagger \rho}\right]$$

$$\Lambda^{\text{Petz}}_{C\to BC}(\cdot) := \rho_{BC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{BC}^{1/2}$$

—> previous ideas: $I(A:B|C)_\rho \geq \frac{1}{4}\left\|\rho_{ABC} - \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})\right\|_1^2\ ?$

[Kim (13)] [Zhang (13)]

- This would give a characterisation of states with small conditional quantum mutual information:

$I(A:B|C)_\rho \approx 0 \Rightarrow \rho_{ABC} = ?$ —> we had: $F\left(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})\right) \approx 1$

approximately recoverable states

Refinements II

- **Conjecture:** $$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC}))\ ?$$

[B., Wilde, Seshadreesan (14)]

$$F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 \quad \|\rho\|_1 := \operatorname{tr}\left[\sqrt{\rho^\dagger \rho}\right]$$

$$\Lambda^{\text{Petz}}_{C\to BC}(\cdot) := \rho_{BC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{BC}^{1/2}$$

—> previous ideas: $I(A:B|C)_\rho \geq \frac{1}{4}\left\|\rho_{ABC} - \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})\right\|_1^2\ ?$

[Kim (13)] [Zhang (13)]

- This would give a characterisation of states with small conditional quantum mutual information:

$I(A:B|C)_\rho \approx 0 \Rightarrow \rho_{ABC} = ?$ —> we had: $F\left(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})\right) \approx 1$

approximately recoverable states

- However, we only have proofs for special cases (analytical evidence) and numerical evidence…

Refinements III

- **Recent breakthrough:**

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{V}_{BC} \circ \Lambda^{\text{Petz}}_{C\to BC} \circ \mathcal{U}_C(\rho_{AC}))$$

[Fawzi, Renner (14)]

$\mathcal{U}_C, \mathcal{V}_{BC}:$ unitaries

Refinements III

- **Recent breakthrough:**

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{V}_{BC} \circ \Lambda^{\mathrm{Petz}}_{C\to BC} \circ \mathcal{U}_C(\rho_{AC}))$$

[Fawzi, Renner (14)]

$\mathcal{U}_C, \mathcal{V}_{BC}$: unitaries

- Proof: very involved (e.g., de Finetti reductions)

Refinements III

- **Recent breakthrough:**

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{V}_{BC} \circ \Lambda^{\mathrm{Petz}}_{C\to BC} \circ \mathcal{U}_C(\rho_{AC}))$$

[Fawzi, Renner (14)]

$\mathcal{U}_C, \mathcal{V}_{BC}$: unitaries

- Proof: very involved (e.g., de Finetti reductions)

- **Fidelity of recovery**:

$$F(A:B|C)_\rho := -\log \sup_{\Lambda_{C\to BC}} F(\rho_{ABC}, \Lambda_{C\to BC}(\rho_{AC}))$$

[Wilde, Seshadreesan (14)]

Refinements III

- **Recent breakthrough:**

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{V}_{BC} \circ \Lambda^{\mathrm{Petz}}_{C\to BC} \circ \mathcal{U}_C(\rho_{AC}))$$

[Fawzi, Renner (14)]

$\mathcal{U}_C, \mathcal{V}_{BC}$: unitaries

- Proof: very involved (e.g., de Finetti reductions)

- **Fidelity of recovery**:

$$F(A:B|C)_\rho := -\log \sup_{\Lambda_{C\to BC}} F(\rho_{ABC}, \Lambda_{C\to BC}(\rho_{AC}))$$

[Wilde, Seshadreesan (14)]

- Alternative, operational (simpler) proofs for:

$$I(A:B|C)_\rho \geq F(A:B|C)_\rho$$

[Brandao, Harrow, Oppenheim, Strelchuk (14)]

[B., Tomamichel (15)]

Refinements III

- **Recent breakthrough:**

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{V}_{BC} \circ \Lambda^{\text{Petz}}_{C\to BC} \circ \mathcal{U}_C(\rho_{AC}))$$

[Fawzi, Renner (14)]

$\mathcal{U}_C, \mathcal{V}_{BC}$: unitaries

- Proof: very involved (e.g., de Finetti reductions)

- **Fidelity of recovery**:

$$F(A:B|C)_\rho := -\log \sup_{\Lambda_{C\to BC}} F(\rho_{ABC}, \Lambda_{C\to BC}(\rho_{AC}))$$

[Wilde, Seshadreesan (14)]

- Alternative, operational (simpler) proofs for:

$$I(A:B|C)_\rho \geq F(A:B|C)_\rho$$

[Brandao, Harrow, Oppenheim, Strelchuk (14)]

[B., Tomamichel (15)]

- Applications so far: understanding quantum correlations better

[Wilde, Seshadreesan (14)] [Wilde (14)] [Li, Winter (14)][Piani (15)]

Outline

- Entropy - operational significance
- Entropy inequalities - laws of information theory
- Recent progress on refining these laws
- Extension: quantum relative entropy and its inequalities
- Conclusions

Quantum Relative Entropy I

- Parent quantity: $$D(\rho\|\sigma) := \mathrm{tr}\left[\rho \log \rho\right] - \mathrm{tr}\left[\rho \log \sigma\right]$$ [Umegaki (62)]

$(\rho, \sigma > 0)$

Quantum Relative Entropy I

- Parent quantity: $$D(\rho\|\sigma) := \mathrm{tr}\left[\rho\log\rho\right] - \mathrm{tr}\left[\rho\log\sigma\right]$$ [Umegaki (62)]

$(\rho, \sigma > 0)$

—> we have: $D(\rho_A\|1_A) = -H(A)_\rho$

$$D(\rho_{AB}\|1_A \otimes \rho_B) = -H(A|B)_\rho$$

$$D(\rho_{AB}\|\rho_A \otimes \rho_B) = I(A:B)_\rho$$

$$D(\rho_{ABC}\|\exp(\log\rho_{AC} + \log\rho_{BC} - \log\rho_C)) = I(A:B|C)_\rho$$

Quantum Relative Entropy I

- Parent quantity: $D(\rho\|\sigma) := \mathrm{tr}\left[\rho \log \rho\right] - \mathrm{tr}\left[\rho \log \sigma\right]$ [Umegaki (62)]

$(\rho, \sigma > 0)$

—> we have: $D(\rho_A\|1_A) = -H(A)_\rho$

$$D(\rho_{AB}\|1_A \otimes \rho_B) = -H(A|B)_\rho$$

$$D(\rho_{AB}\|\rho_A \otimes \rho_B) = I(A:B)_\rho$$

$$D(\rho_{ABC}\|\exp(\log \rho_{AC} + \log \rho_{BC} - \log \rho_C)) = I(A:B|C)_\rho$$

- Monotonicity of relative entropy under quantum operations (MONO):

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$

[Linblad (75)] [Uhlmann (77)]

—> irreversibility in quantum mechanics, parent inequality

Quantum Relative Entropy I

- Parent quantity: $$D(\rho\|\sigma) := \mathrm{tr}\left[\rho \log \rho\right] - \mathrm{tr}\left[\rho \log \sigma\right]$$ [Umegaki (62)]

  $(\rho, \sigma > 0)$

  —> we have:
$$D(\rho_A \| 1_A) = -H(A)_\rho$$
$$D(\rho_{AB} \| 1_A \otimes \rho_B) = -H(A|B)_\rho$$
$$D(\rho_{AB} \| \rho_A \otimes \rho_B) = I(A:B)_\rho$$
$$D(\rho_{ABC} \| \exp(\log \rho_{AC} + \log \rho_{BC} - \log \rho_C)) = I(A:B|C)_\rho$$

- Monotonicity of relative entropy under quantum operations (MONO):

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$ [Linblad (75)] [Uhlmann (77)]

  —> irreversibility in quantum mechanics, parent inequality

- Example: strong subadditivity of entropy (SSA)

$$\rho = \rho_{ABC},\ \sigma = 1_A \otimes \rho_{BC},\ \mathcal{N}(\cdot) = \mathrm{tr}_B[\cdot] \ \Rightarrow\ \mathcal{N}(\rho) = \rho_{AC},\ \mathcal{N}(\sigma) = 1_A \otimes \rho_C$$
$$0 \leq D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) = -H(A|BC)_\rho + H(A|C)_\rho = I(A:B|C)_\rho$$

Quantum Relative Entropy II

- Can we improve MONO (in an operationally useful way)? [Li, Winter (12, 14)]

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$

vs.

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) \geq f(\rho,\sigma,\mathcal{N})\ ?$$

Quantum Relative Entropy II

- Can we improve MONO (in an operationally useful way)? [Li, Winter (12, 14)]

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$

vs.

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) \geq f(\rho, \sigma, \mathcal{N}) \ ?$$

- What are the equality conditions for MONO?

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) = 0 \ \Leftrightarrow \ \rho = \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho)) \\ \sigma = \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\sigma))$$

[Petz (88)]

with $\Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\cdot) := \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

—> this is a quantum operation, recovery map.

Quantum Relative Entropy II

- Can we improve MONO (in an operationally useful way)? [Li, Winter (12, 14)]

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$

vs.

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) \geq f(\rho, \sigma, \mathcal{N}) \ ?$$

- What are the equality conditions for MONO?

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) = 0 \ \Leftrightarrow \ \rho = \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho)) \quad \sigma = \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\sigma))$$

[Petz (88)]

with $\Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\cdot) := \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

—> this is a quantum operation, recovery map.

- If the relative entropy difference is zero we can undo noisy quantum operation!

Quantum Relative Entropy II

- Can we improve MONO (in an operationally useful way)? [Li, Winter (12, 14)]

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$

vs.

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) \geq f(\rho, \sigma, \mathcal{N}) \ ?$$

- What are the equality conditions for MONO?

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma) = 0 \ \Leftrightarrow \ \rho = \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho))$$
$$\sigma = \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\sigma))$$

[Petz (88)]

with $\Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\cdot) := \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

—> this is a quantum operation, recovery map.

- If the relative entropy difference is zero we can undo noisy quantum operation!
- But we also need to understand the approximate case…

Quantum Relative Entropy III

- **Conjecture:**

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho))\right) \ ?$$

[Zhang (13)] [B., Wilde, Seshadreesan (14)]

with $\Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\cdot) := \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

Quantum Relative Entropy III

- **Conjecture:**

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \Lambda_{\mathcal{N},\sigma}^{\text{Petz}}(\mathcal{N}(\rho))\right) \ ?$$

[Zhang (13)] [B., Wilde, Seshadreesan (14)]

with $\Lambda_{\mathcal{N},\sigma}^{\text{Petz}}(\cdot) := \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

- Approximate equality case (approximately undoing noisy quantum operations):

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \approx 0 \ \Rightarrow \ \Lambda_{\mathcal{N},\sigma}^{\text{Petz}}(\mathcal{N}(\rho)) \approx \rho \quad \Lambda_{\mathcal{N},\sigma}^{\text{Petz}}(\mathcal{N}(\sigma)) = \sigma$$

Quantum Relative Entropy III

- **Conjecture:**

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho))\right) \ ?$$

[Zhang (13)] [B., Wilde, Seshadreesan (14)]

with $\Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\cdot) := \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

- Approximate equality case (approximately undoing noisy quantum operations):

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \approx 0 \ \Rightarrow \ \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho)) \approx \rho \quad \Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\sigma)) = \sigma$$

- Like in the case of SSA only an alternative bound is known:

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \mathcal{V}\circ\Lambda^{\mathrm{Petz}}_{\mathcal{N},\sigma}\circ\mathcal{U}(\mathcal{N}(\rho))\right)$$

[B., Lemm, Wilde (14)]

$\mathcal{U},\mathcal{V}:$ unitaries

Quantum Relative Entropy III

- **Conjecture:**

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \Lambda^{\text{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho))\right) \ ?$$

[Zhang (13)] [B., Wilde, Seshadreesan (14)]

with $\Lambda^{\text{Petz}}_{\mathcal{N},\sigma}(\cdot) := \sigma^{1/2}\mathcal{N}^\dagger\left(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}$

- Approximate equality case (approximately undoing noisy quantum operations):

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \approx 0 \ \Rightarrow \ \Lambda^{\text{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho)) \approx \rho \quad \Lambda^{\text{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\sigma)) = \sigma$$

- Like in the case of SSA only an alternative bound is known:

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \mathcal{V}\circ\Lambda^{\text{Petz}}_{\mathcal{N},\sigma}\circ\mathcal{U}(\mathcal{N}(\rho))\right)$$

[B., Lemm, Wilde (14)] $\mathcal{U},\mathcal{V}:$ unitaries

—> however, we would like to know more about the unitaries…

Equivalence

- The following are **equivalent**:
  - Strong subadditivity of entropy (SSA)
    $$I(A:B|C)_\rho \geq 0$$
  - Monotonicity of relative entropy under quantum operations (MONO):
    $$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$
  - Joint convexity of relative entropy (JC)
  - Concavity of conditional entropy (CC)

[Ruskai (02)]

Equivalence

- The following are **equivalent**:

  - Strong subadditivity of entropy (SSA)
    $$I(A:B|C)_\rho \geq 0$$
  - Monotonicity of relative entropy under quantum operations (MONO):
    $$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$
  - Joint convexity of relative entropy (JC)
  - Concavity of conditional entropy (CC)

[Ruskai (02)]

- **Refinements** in terms of Petz recovery map are **equivalent as well**:

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})) \;\Leftrightarrow\; D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \Lambda^{\text{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho))\right)$$
$$\Leftrightarrow \; \ldots$$

[B., Lemm, Wilde (14)]

Equivalence

- The following are **equivalent**:
  - Strong subadditivity of entropy (SSA)
    $$I(A:B|C)_\rho \geq 0$$
  - Monotonicity of relative entropy under quantum operations (MONO):
    $$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$
  - Joint convexity of relative entropy (JC)
  - Concavity of conditional entropy (CC)

[Ruskai (02)]

- **Refinements** in terms of Petz recovery map are **equivalent as well**:

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \Lambda^{\text{Petz}}_{C\to BC}(\rho_{AC})) \;\Leftrightarrow\; D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \Lambda^{\text{Petz}}_{\mathcal{N},\sigma}(\mathcal{N}(\rho))\right)$$
$$\Leftrightarrow \;\ldots$$

[B., Lemm, Wilde (14)]

—> however, we do not know if they actually hold: either all of these refinements (in terms of the Petz recovery map) are true or all are wrong…

Outline

- Entropy - operational significance
- Entropy inequalities - laws of information theory
- Recent progress on refining these laws
- Extension: quantum relative entropy and its inequalities
- Conclusions

Conclusions

- Strong subadditivity of entropy (SSA):

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

extended to

$$I(A:B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{V}_{BC} \circ \Lambda^{\text{Petz}}_{C\to BC} \circ \mathcal{U}_C(\rho_{AC}))$$

- Monotonicity of relative entropy under quantum operations (MONO):

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq 0$$

extended to

$$D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F\left(\rho, \mathcal{V} \circ \Lambda^{\text{Petz}}_{\mathcal{N},\sigma} \circ \mathcal{U}(\mathcal{N}(\rho))\right)$$

- Petz recovery map form to (dis)prove, many potential applications