Quantum conditional mutual information and approximate Markov chains

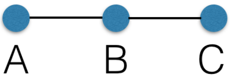
Omar Fawzi

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

ENS DE LYON

Banff, January 13th, 2015

Joint work with Renato Renner arXiv:1410.0664



$$I(A : C|B)$$

Correlation measure between A and C from point of view of B

Objective:

$$\boxed{\text{Structure of states on } A \otimes B \otimes C \text{ with } I(A : C|B) \leq \epsilon}$$

Outline:

1. Definition and properties of conditional mutual information
2. How to ensure that $I(A : C|B) \leq \epsilon$?
3. What is the right operational property?
4. Statement and overview of the proof

Entropy and conditioning

Entropy: measure of uncertainty in a system

Shannon entropy for distribution p_X:

$$H(X) = -\sum_x p_X(x) \log p_X(x) \in [0, \log|X|]$$

Quantum von Neumann entropy for density operator ρ_A:

$$H(A) = -\operatorname{tr}(\rho_A \log \rho_A) \in [0, \log|A|]$$

Entropy and conditioning

Entropy: measure of uncertainty in a system

Shannon entropy for distribution p_X:

$$H(X) = -\sum_x p_X(x) \log p_X(x) \in [0, \log |X|]$$

Quantum von Neumann entropy for density operator ρ_A:

$$H(A) = -\operatorname{tr}(\rho_A \log \rho_A) \in [0, \log |A|]$$

Multiple systems: State ρ_{AB} acting on $A \otimes B$

Conditional entropy of A from B's viewpoint

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

Entropy and conditioning

Entropy: measure of uncertainty in a system

Shannon entropy for distribution p_X:

$$H(X) = -\sum_x p_X(x) \log p_X(x) \in [0, \log |X|]$$

Quantum von Neumann entropy for density operator ρ_A:

$$H(A) = -\operatorname{tr}(\rho_A \log \rho_A) \in [0, \log |A|]$$

Multiple systems: State ρ_{AB} acting on $A \otimes B$

Conditional entropy of A from B's viewpoint

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

Interpretation:

- Classical B: $\rho_{AB} = \sum_b \rho_A(b) \otimes p(b)|b\rangle\langle b|$

$$H(A|B)_\rho = \sum_b p(b) H(A)_{\rho(b)}$$

- Quantum B: More subtle
  $H(A|B)_\rho$ can be negative when ρ entangled

$$-\log |A| \leq H(A|B)_\rho \leq \log |A|$$

Mutual information and conditioning

- State ρ_{AC} acting on $A \otimes C$
  Mutual Information:

$$I(A:C)_\rho = H(C)_\rho - H(C|A)_\rho$$

  - Classical ρ: $0 \leq I(A:C)_\rho \leq \min\{\log|A|, \log|C|\}$
  - Quantum ρ: $0 \leq I(A:C)_\rho \leq 2\min\{\log|A|, \log|C|\}$

- State ρ_{ABC} acting on $A \otimes B \otimes C$
  Conditional Mutual Information:

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

  - Classical B: $\rho_{ABC} = \sum_b \rho_{AC}(b) \otimes p(b)|b\rangle\langle b|_B$

$$I(A:C|B)_\rho = \sum_b p(b) I(A:C)_{\rho(b)} \in [0, \min\{\log|A|, \log|C|\}]$$

  - Quantum B: More subtle

$$0 \leq I(A:C|B)_\rho \leq 2\min\{\log|A|, \log|C|\}$$

Useful property

Additivity property make it a very useful measure:

$\boxed{\textbf{Chain rule}}$

$$
\begin{aligned}
&I(A_1 \dots A_n : C|B) \\
&\qquad = I(A_1 : C|B) + I(A_2 : C|BA_1) + \cdots + I(A_n : C|BA_1 \dots A_{n-1})
\end{aligned}
$$

Correlations can be decomposed into parts

Useful property

Additivity property make it a very useful measure:

$$\boxed{\textbf{Chain rule}}$$

$$\begin{aligned} &I(A_1 \dots A_n : C|B) \\ &\quad = I(A_1 : C|B) + I(A_2 : C|BA_1) + \cdots + I(A_n : C|BA_1 \dots A_{n-1}) \end{aligned}$$

Correlations can be decomposed into parts

Some applications:

- Direct sum results in communication complexity [Talk Braverman et al. tomorrow]
- Entanglement measures (squashed entanglement) [Christandl, Winter, 2003]
- de Finetti-type statements [Raghavendra, Tan, 2011] [Brandao, Harrow, 2013]
- ...

Useful property

Additivity property make it a very useful measure:

$$\boxed{\textbf{Chain rule}}$$

$$I(A_1 \dots A_n : C|B)$$
$$= I(A_1 : C|B) + I(A_2 : C|BA_1) + \dots + I(A_n : C|BA_1 \dots A_{n-1})$$

Correlations can be decomposed into parts

Some applications:

- Direct sum results in communication complexity [Talk Braverman et al. tomorrow]
- Entanglement measures (squashed entanglement) [Christandl, Winter, 2003]
- de Finetti-type statements [Raghavendra, Tan, 2011] [Brandao, Harrow, 2013]
- ...

Typical argument:

1. Total correlation between $A_1 \dots A_n$ and C bounded:
$$I(A_1 \dots A_n : C|B) \leq 2 \log |C|$$
2. Correlation has to be spread:
$$\frac{1}{n} \sum_{i=1}^{n} I(A_i : C|BA_1 \dots A_{i-1}) \leq \frac{2 \log |C|}{n}$$

Sample application

Intuition: loosing one bit can be replaced with some advice

Theorem

For any joint distribution $P_{X_1 \dots X_n YZ}$ where Y is a bit. There exists a subset $L \subset \{1, \dots, n\}$ of length $|L| \leq 1/\epsilon$

$$\text{for all } i, \quad \mathrm{P}_{\mathrm{guess}}(X_i|ZX_L) \geq \mathrm{P}_{\mathrm{guess}}(X_i|ZY) - \sqrt{(2\ln 2)\epsilon}$$

Interpretation: Y can be replaced by a small number of bits of $X_1 \dots X_n$

Sample application

Intuition: loosing one bit can be replaced with some advice

Theorem

For any joint distribution $P_{X_1 \dots X_n YZ}$ where Y is a bit. There exists a subset $L \subset \{1, \dots, n\}$ of length $|L| \leq 1/\epsilon$

$$\textit{for all } i, \quad \mathrm{P}_{\text{guess}}(X_i | Z X_L) \geq \mathrm{P}_{\text{guess}}(X_i | Z Y) - \sqrt{(2 \ln 2)\epsilon}$$

Interpretation: Y can be replaced by a small number of bits of $X_1 \dots X_n$

Algorithm to construct L

$L \leftarrow \emptyset$
while $\exists i \in \{1, \dots, n\}$ st $I(X_i : Y | Z X_L) > \epsilon$
  $L \leftarrow L \cup \{i\}$

Sample application

Intuition: loosing one bit can be replaced with some advice

Theorem

For any joint distribution $P_{X_1 \ldots X_n YZ}$ where Y is a bit. There exists a subset $L \subset \{1, \ldots, n\}$ of length $|L| \leq 1/\epsilon$

$$\textit{for all } i, \quad \mathrm{P}_{\text{guess}}(X_i|ZX_L) \geq \mathrm{P}_{\text{guess}}(X_i|ZY) - \sqrt{(2 \ln 2)\epsilon}$$

Interpretation: Y can be replaced by a small number of bits of $X_1 \ldots X_n$

Algorithm to construct L

$L \leftarrow \emptyset$

while $\exists i \in \{1, \ldots, n\}$ st $I(X_i : Y|ZX_L) > \epsilon$

$\quad L \leftarrow L \cup \{i\}$

Claim 1: The algorithm terminates in $< 1/\epsilon$ steps

Claim 2: When algorithm terminates, $\mathrm{P}_{\text{guess}}(X_i|ZX_L) \gtrapprox_\epsilon \mathrm{P}_{\text{guess}}(X_i|ZY)$

Sample application (Proof of claim 1)

Theorem

For any joint distribution $P_{X_1 \ldots X_n YZ}$ where Y is a bit. There exists a subset $L \subset \{1, \ldots, n\}$ of length $|L| \leq 1/\epsilon$

$$\textit{for all } i, \quad \mathrm{P}_{\text{guess}}(X_i|ZX_L) \geq \mathrm{P}_{\text{guess}}(X_i|ZY) - \sqrt{(2\ln 2)\epsilon}$$

Algorithm to construct L
$L \leftarrow \emptyset$
while $\exists i \in \{1, \ldots, n\}$ st $I(X_i : Y|ZX_L) > \epsilon$
  $L \leftarrow L \cup \{i\}$

Claim 1: The algorithm terminates in at most $1/\epsilon$ steps
$L = \{i_1, \ldots, i_\ell\}$

$$I(X_L : Y|Z) = \sum_{p=1}^{\ell} I(X_{i_p} : Y|ZX_{i_1 \ldots i_{p-1}}) \geq \ell \cdot \epsilon$$

But $I(X_L : Y|Z) \leq 1$ because Y is one bit

So $\ell \leq \frac{1}{\epsilon}$ $\square$

Sample application (Proof of claim 2)

Theorem

For any joint distribution $P_{X_1 \dots X_n YZ}$ where Y is a bit. There exists a subset $L \subset \{1, \dots, n\}$ of length $|L| \leq 1/\epsilon$

$$\textit{for all } i, \quad \mathrm{P}_{\mathrm{guess}}(X_i|ZX_L) \geq \mathrm{P}_{\mathrm{guess}}(X_i|ZY) - \sqrt{(2\ln 2)\epsilon}$$

Algorithm to construct L
$L \leftarrow \emptyset$
while $\exists i \in \{1, \dots, n\}$ st $I(X_i : Y|ZX_L) > \epsilon$
$L \leftarrow L \cup \{i\}$

Claim 2: When algorithm terminates, $\mathrm{P}_{\mathrm{guess}}(X_i|ZX_L) \gtrapprox_\epsilon \mathrm{P}_{\mathrm{guess}}(X_i|ZY)$
For all i,

$$\begin{aligned}
\epsilon \geq I(X_i : Y|ZX_L) &= \mathop{\mathbb{E}}_{zx_L} \left\{ I(X_i : Y)_{P_{X_i Y|zx_L}} \right\} \\
&\geq \mathop{\mathbb{E}}_{zx_L} \left\{ \frac{1}{2\ln 2} \left\| P_{X_i Y|zx_L} - P_{X_i|zx_L} \times P_{Y|zx_L} \right\|_1^2 \right\} \\
&\geq \frac{1}{2\ln 2} \left(\mathop{\mathbb{E}}_{zx_L} \left\{ \left\| P_{X_i|zx_L y} - P_{X_i|zx_L} \right\|_1 \right\} \right)^2 \\
&\geq \frac{1}{2\ln 2} \left(\mathrm{P}_{\mathrm{guess}}(X_i|ZX_L Y) - \mathrm{P}_{\mathrm{guess}}(X_i|ZX_L) \right)^2
\end{aligned}$$

$$\mathrm{P}_{\mathrm{guess}}(X_i|ZX_L) \geq \mathrm{P}_{\mathrm{guess}}(X_i|ZX_L Y) - \sqrt{(2\ln 2)\epsilon} \geq \mathrm{P}_{\mathrm{guess}}(X_i|ZY) - \sqrt{(2\ln 2)\epsilon} \quad \square$$

Sample application: quantum systems

Wanted

For any **quantum** *density operator* $\rho_{X_1 \ldots X_n CB}$ *where* C *is a qubit. There exists a subset* $L \subset \{1, \ldots, n\}$ *of length* $|L| \leq 2/\epsilon$

$$\text{for all } i, \quad \mathrm{P}_{\text{guess}}(X_i | B X_L) \geq \mathrm{P}_{\text{guess}}(X_i | BC) - \sqrt{(2 \ln 2)\epsilon}$$

Algorithm to construct L
$L \leftarrow \emptyset$
while $\exists i \in \{1, \ldots, n\}$ st $I(X_i : C | B X_L) > \epsilon$
  $L \leftarrow L \cup \{i\}$

Claim 1: The algorithm terminates in at most $2/\epsilon$ steps
Only used **chain rule** and $I(X : C|B) \leq 2 \log |C|$, which still holds quantum ✓

Sample application: quantum systems

Wanted

For any **quantum** *density operator* $\rho_{X_1 \dots X_n CB}$ *where* C *is a qubit. There exists a subset* $L \subset \{1, \dots, n\}$ *of length* $|L| \leq 2/\epsilon$

$$\textit{for all } i, \quad \mathrm{P}_{\mathrm{guess}}(X_i|BX_L) \geq \mathrm{P}_{\mathrm{guess}}(X_i|BC) - \sqrt{(2\ln 2)\epsilon}$$

Algorithm to construct L
$L \leftarrow \emptyset$
while $\exists i \in \{1, \dots, n\}$ st $I(X_i : C|BX_L) > \epsilon$
  $L \leftarrow L \cup \{i\}$

Claim 1: The algorithm terminates in at most $2/\epsilon$ steps
Only used **chain rule** and $I(X : C|B) \leq 2\log|C|$, which still holds quantum ✓

Claim 2: When algorithm terminates, $\mathrm{P}_{\mathrm{guess}}(X_i|BX_L) \gtrapprox_\epsilon \mathrm{P}_{\mathrm{guess}}(X_i|BC)$? quantum ?
We have for all i, $I(X_i : C|BX_L) \leq \epsilon$. But how to conclude?

$$\epsilon \geq I(X_i : Y|ZX_L) = \mathop{\mathbb{E}}_{zx_L}\left\{ I(X_i : Y)_{P_{X_iY|zx_L}} \right\}$$? quantum ?

$$\geq \mathop{\mathbb{E}}_{zx_L}\left\{ \frac{1}{2\ln 2} \left\| P_{X_iY|zx_L} - P_{X_i|zx_L} \times P_{Y|zx_L} \right\|_1^2 \right\}$$? quantum ?

$$\geq \frac{1}{2\ln 2}\left(\mathrm{P}_{\mathrm{guess}}(X_i|ZX_LY) - \mathrm{P}_{\mathrm{guess}}(X_i|ZX_L)\right)^2$$

Structure of states with small QCMI: $\epsilon = 0$ case

Theorem (Strong subadditivity [Lieb, Ruskai, 1973])

For all quantum states ρ, $I(A:C|B)_\rho \geq 0$

Rewritten: $H(A|B) + H(C|B) \geq H(AC|B)$

Structure of states with small QCMI: $\epsilon = 0$ case

Theorem (Strong subadditivity [Lieb, Ruskai, 1973])

For all quantum states ρ, $I(A:C|B)_\rho \geq 0$

Rewritten: $H(A|B) + H(C|B) \geq H(AC|B)$

Theorem (QCMI and Markov chains [Petz, 1988])

$$I(A:C|B)_\rho = 0 \quad \Leftrightarrow \quad \exists \mathcal{T} : B \to BC, \ (\mathcal{I}_A \otimes \mathcal{T}_{BC\leftarrow B})(\rho_{AB}) = \rho_{ABC}$$

Interpretation: C can be generated by acting only on B (without acting on A)

Structure of $\mathcal{T}$: $\mathcal{T}_{BC\leftarrow B}(\gamma) = \rho_{BC}^{1/2}\rho_B^{-1/2}(\gamma \otimes \mathrm{id}_C)\rho_B^{-1/2}\rho_{BC}^{1/2}$

Structure of states with small QCMI: $\epsilon = 0$ case

Theorem (Strong subadditivity [Lieb, Ruskai, 1973])

For all quantum states ρ, $I(A:C|B)_\rho \geq 0$

Rewritten: $H(A|B) + H(C|B) \geq H(AC|B)$

Theorem (QCMI and Markov chains [Petz, 1988])

$$I(A:C|B)_\rho = 0 \quad \Leftrightarrow \quad \exists \mathcal{T} : B \to BC,\ (\mathcal{I}_A \otimes \mathcal{T}_{BC \leftarrow B})(\rho_{AB}) = \rho_{ABC}$$

Interpretation: C can be generated by acting only on B (without acting on A)

Structure of $\mathcal{T}$: $\mathcal{T}_{BC \leftarrow B}(\gamma) = \rho_{BC}^{1/2} \rho_B^{-1/2} (\gamma \otimes \mathrm{id}_C) \rho_B^{-1/2} \rho_{BC}^{1/2}$

ρ_{ABC} is a **quantum Markov chain:** $\exists \mathcal{T} : B \to BC,\ (\mathcal{I}_A \otimes \mathcal{T}_{BC \leftarrow B})(\rho_{AB}) = \rho_{ABC}$

Illustration of Markov chain condition

$I(A_1 : A_3 | A_2) = 0$

$I(A_1 A_2 : A_4 | A_3) = 0$

$\ddots$

$I(A_1 \ldots A_{n-2} : A_n | A_{n-1}) = 0$

Illustration of Markov chain condition

$I(A_1 : A_3 | A_2) = 0$

$I(A_1 A_2 : A_4 | A_3) = 0$

$\ddots$

$I(A_1 \ldots A_{n-2} : A_n | A_{n-1}) = 0$

Then

$$
\begin{aligned}
\rho_{A_1 A_2 A_3} &= (\mathcal{I}_{A_1} \otimes \mathcal{T}_{A_2 A_3 \leftarrow A_2})(\rho_{A_1 A_2}) \\
\rho_{A_1 A_2 A_3 A_4} &= (\mathcal{I}_{A_1 A_2} \otimes \mathcal{T}_{A_3 A_4 \leftarrow A_3})(\rho_{A_1 A_2 A_3}) \\
&\vdots \\
\rho_{A_1 \ldots A_n} &= (\mathcal{I}_{A_1 \ldots A_{n-2}} \otimes \mathcal{T}_{A_{n-1} A_n \leftarrow A_{n-1}})(\rho_{A_1 \ldots A_{n-1}}) \\
\Longrightarrow \quad \rho_{A_1 \ldots A_n} &= \left(\mathcal{T}_{A_{n-1} A_n \leftarrow A_{n-1}} \circ \cdots \circ \mathcal{T}_{A_2 A_3 \leftarrow A_2}\right) (\rho_{A_1 A_2})
\end{aligned}
$$

Illustration of Markov chain condition

I(A1:A3|A2)=0

I(A1A2:A4|A3)=0

$\ddots$

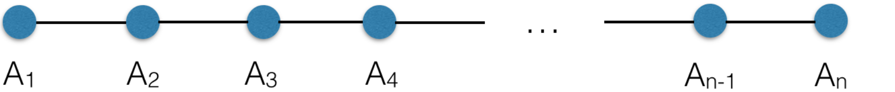
I(A1…An-2:An|An-1)=0

Then

$$
\begin{aligned}
\rho_{A_1A_2A_3} &= (\mathcal{I}_{A_1} \otimes \mathcal{T}_{A_2A_3\leftarrow A_2})(\rho_{A_1A_2}) \\
\rho_{A_1A_2A_3A_4} &= (\mathcal{I}_{A_1A_2} \otimes \mathcal{T}_{A_3A_4\leftarrow A_3})(\rho_{A_1A_2A_3}) \\
&\vdots \\
\rho_{A_1\ldots A_n} &= (\mathcal{I}_{A_1\ldots A_{n-2}} \otimes \mathcal{T}_{A_{n-1}A_n\leftarrow A_{n-1}})(\rho_{A_1\ldots A_{n-1}}) \\
\Longrightarrow \rho_{A_1\ldots A_n} &= \left(\mathcal{T}_{A_{n-1}A_n\leftarrow A_{n-1}} \circ \cdots \circ \mathcal{T}_{A_2A_3\leftarrow A_2}\right)(\rho_{A_1A_2})
\end{aligned}
$$

Efficient representation of $\rho_{A_1\ldots A_n}$: only $O(n)$ bits (compare to $2^{\Omega(n)}$ in general)

Illustration of Markov chain condition



$I(A_1 : A_3 | A_2) = 0$

$I(A_1 A_2 : A_4 | A_3) = 0$

$\ddots$

$I(A_1 \ldots A_{n-2} : A_n | A_{n-1}) = 0$

Then

$$\begin{aligned} \rho_{A_1A_2A_3} &= (\mathcal{I}_{A_1} \otimes \mathcal{T}_{A_2A_3 \leftarrow A_2})(\rho_{A_1A_2}) \\ \rho_{A_1A_2A_3A_4} &= (\mathcal{I}_{A_1A_2} \otimes \mathcal{T}_{A_3A_4 \leftarrow A_3})(\rho_{A_1A_2A_3}) \\ &\vdots \\ \rho_{A_1\ldots A_n} &= (\mathcal{I}_{A_1\ldots A_{n-2}} \otimes \mathcal{T}_{A_{n-1}A_n \leftarrow A_{n-1}})(\rho_{A_1\ldots A_{n-1}}) \\ \implies \rho_{A_1\ldots A_n} &= \left(\mathcal{T}_{A_{n-1}A_n \leftarrow A_{n-1}} \circ \cdots \circ \mathcal{T}_{A_2A_3 \leftarrow A_2}\right)(\rho_{A_1A_2}) \end{aligned}$$

Efficient representation of $\rho_{A_1\ldots A_n}$: only $O(n)$ bits (compare to $2^{\Omega(n)}$ in general)

Hope: if $I(A_1 \ldots A_{i-1} : A_{i+1} | A_i) \leq \epsilon$

$\implies$ then efficient approximate representation of $\rho_{A_1\ldots A_n}$

Small QCMI: $\epsilon > 0$ (Known lower bounds on QCMI)

Theorem (Remainder term for SSA [Carlen, Lieb, 2014] see also [Zhang, Wu 2014])

$$I(A:C|B)_\rho \geq \operatorname{tr}\left[\sqrt{\rho_{ABC}} - \exp\left(\frac{1}{2}\log\rho_{AB} - \frac{1}{2}\log\rho_B + \frac{1}{2}\log\rho_{BC}\right)\right]^2$$

Problem: Term $\exp(\log + \log)$ difficult to interpret **operationally**

Small QCMI: $\epsilon > 0$ (Known lower bounds on QCMI)

Theorem (Remainder term for SSA [Carlen, Lieb, 2014] see also [Zhang, Wu 2014])

$$I(A:C|B)_\rho \geq \mathrm{tr}\left[\sqrt{\rho_{ABC}} - \exp\left(\frac{1}{2}\log\rho_{AB} - \frac{1}{2}\log\rho_B + \frac{1}{2}\log\rho_{BC}\right)\right]^2$$

Problem: Term $\exp(\log + \log)$ difficult to interpret **operationally**

Theorem (Faithful squashed entanglement [Brandao, Christandl, Yard, 2010])

$$I(A:C|B)_\rho \geq \min_{\sigma_{AC}\ \textit{separable}} \frac{1}{8\ln 2}\|\rho_{AC} - \sigma_{AC}\|^2_{LOCC}$$

Problem: Bound is independent of B, value 0 when A or C classical

QCMI used to quantify entanglement: $E_{sq}(A:C)_\rho = \inf_{\rho_{ABC}} \frac{1}{2} I(A:C|B)_\rho$

Small QCMI: $\epsilon > 0$ case

ρ_{ABC} is a **quantum Markov chain:** $\exists \mathcal{T} : B \to BC, \ (\mathcal{I}_A \otimes \mathcal{T}_{BC\leftarrow B})(\rho_{AB}) = \rho_{ABC}$

Candidate conjecture 1:

$$I(A:C|B)_\rho \leq \epsilon \quad \Rightarrow \quad \rho_{ABC} \approx_{f(\epsilon)} \omega_{ABC}, \text{ with } \omega_{ABC} \text{ Markov chain}$$

Counterexamples [Ibinson, Linden, Winter, 2006] and [Christandl, Schuch, Winter, 2012] $\to f$ has to depend on dimensions

Small QCMI: $\epsilon > 0$ case

ρ_{ABC} is a **quantum Markov chain:** $\exists \mathcal{T} : B \to BC,\ (\mathcal{I}_A \otimes \mathcal{T}_{BC \leftarrow B})(\rho_{AB}) = \rho_{ABC}$

Candidate conjecture 1:

$$I(A:C|B)_\rho \le \epsilon \quad \Rightarrow \quad \rho_{ABC} \approx_{f(\epsilon)} \omega_{ABC},\ \text{with } \omega_{ABC} \text{ Markov chain}$$

Counterexamples [Ibinson, Linden, Winter, 2006] and [Christandl, Schuch, Winter, 2012]
$\to f$ has to depend on dimensions

Candidate conjecture 2:
[Li, Winter, 2012], [Kim, 2013], [Zhang, 2013], [Berta, Seshadreesan, Wilde, 2014]

$$I(A:C|B)_\rho \le \epsilon \quad \Rightarrow \quad \exists \mathcal{T} : B \to BC,\ (\mathcal{I}_A \otimes \mathcal{T})(\rho_{AB}) \approx_\epsilon \rho_{ABC}$$

with $\mathcal{T}(\gamma) = \rho_{BC}^{1/2} \rho_B^{-1/2} (\gamma \otimes \mathrm{id}_C) \rho_B^{-1/2} \rho_{BC}^{1/2}$

Remarks:

- **Conj. 1** and **Conj. 2** are true for **classical** states
- General **quantum** case: **Conj. 2** does **not** imply **Conj. 1**

Main result

A proof of a variant of **Conj. 2**

Theorem

For any ρ_{ABC}, there exists $\mathcal{T} : B \to BC$ such that

$$I(A:C|B)_\rho \geq -2\log F(\rho_{ABC}, \mathcal{T}_{BC\leftarrow B}(\rho_{AB}))$$

Remarks:

- $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the fidelity
- Implies $I(A:C|B)_\rho \geq \frac{1}{4\ln 2}\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1^2$

Main result

A proof of a variant of **Conj. 2**

Theorem

For any ρ_{ABC}, there exists $\mathcal{T} : B \to BC$ such that

$$I(A : C|B)_\rho \geq -2 \log F(\rho_{ABC}, \mathcal{T}_{BC\leftarrow B}(\rho_{AB}))$$

Remarks:

- $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the fidelity
- Implies $I(A : C|B)_\rho \geq \frac{1}{4 \ln 2}\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1^2$
- Properties of the map $\mathcal{T}$

$$\mathcal{T}_{BC\leftarrow B}(\gamma) = V_{BC}\rho_{BC}^{1/2}\rho_B^{-1/2}U_B(\gamma \otimes \mathrm{id}_C)U_B^\dagger\rho_B^{-1/2}\rho_{BC}^{1/2}V_{BC}^\dagger$$

Structure of states ρ_{ABC} with $I(A : C|B)_\rho \leq \epsilon$

$\implies$ states for which C can be approximately reconstructed from B

Back to our sample applications (replacing lost C)

Main result: $I(A:C|B)_\rho \geq \frac{1}{4\ln 2}\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1^2$

Theorem

For any **quantum** *density operator* $\rho_{X_1 \ldots X_n CB}$ *where* C *is a qubit. There exists a subset* $L \subset \{1, \ldots, n\}$ *of length* $|L| \leq 1/\epsilon$

$$\text{for all } i, \quad \mathrm{P}_{\mathrm{guess}}(X_i|BX_L) \geq \mathrm{P}_{\mathrm{guess}}(X_i|BC) - \sqrt{(4\ln 2)\epsilon}$$

Algorithm to construct L

$L \leftarrow \emptyset$

while $\exists i \in \{1, \ldots, n\}$ st $I(X_i : C|BX_L) > \epsilon$

  $L \leftarrow L \cup \{i\}$

Claim 1: The algorithm terminates in at most $2/\epsilon$ steps quantum ✓

Claim 2: When algorithm terminates, $\mathrm{P}_{\mathrm{guess}}(X_i|BX_L) \gtrapprox_\epsilon \mathrm{P}_{\mathrm{guess}}(X_i|BC)$

We have for all i, $I(X_i : C|BX_L) \leq \epsilon$

Back to our sample applications (replacing lost C)

Main result: $I(A:C|B)_\rho \geq \frac{1}{4\ln 2}\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1^2$

Theorem

For any **quantum** *density operator* $\rho_{X_1\ldots X_n CB}$ *where* C *is a qubit. There exists a subset* $L \subset \{1,\ldots,n\}$ *of length* $|L| \leq 1/\epsilon$

$$\text{for all } i, \quad \mathrm{P}_{\mathrm{guess}}(X_i|BX_L) \geq \mathrm{P}_{\mathrm{guess}}(X_i|BC) - \sqrt{(4\ln 2)\epsilon}$$

Algorithm to construct L

$L \leftarrow \emptyset$
while $\exists i \in \{1,\ldots,n\}$ st $I(X_i : C|BX_L) > \epsilon$
  $L \leftarrow L \cup \{i\}$

Claim 1: The algorithm terminates in at most $2/\epsilon$ steps   quantum ✓
Claim 2: When algorithm terminates, $\mathrm{P}_{\mathrm{guess}}(X_i|BX_L) \gtrapprox_\epsilon \mathrm{P}_{\mathrm{guess}}(X_i|BC)$

We have for all i, $I(X_i : C|BX_L) \leq \epsilon$
Apply **main result**: $\rho_{X_iCBX_L} \approx_\delta \mathcal{T}_{BX_LC\leftarrow BX_L}(\rho_{X_iBX_L})$ with $\delta = \sqrt{(4\ln 2)\epsilon}$
Strategy for guessing X_i from B and X_L:

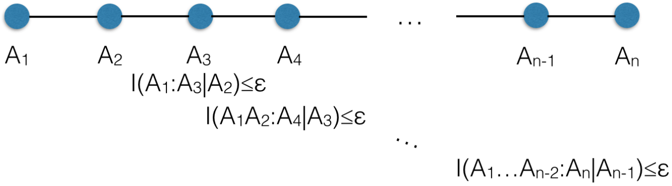
1. Construct the state $\mathcal{T}_{BX_LC\leftarrow BX_L}(\rho_{X_iBX_L})$
2. Pretend the state was $\rho_{X_iCBX_L}$ and use its optimal guessing strategy

$$\mathrm{P}_{\mathrm{guess}}(X_i|BX_L)_\rho \geq \mathrm{P}_{\mathrm{guess}}(X_i|BX_LC)_\rho - \delta \geq \mathrm{P}_{\mathrm{guess}}(X_i|BC)_\rho - \delta$$

Back to our sample applications (long chain)

Main result: $I(A:C|B)_\rho \geq \frac{1}{4\ln 2}\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1^2$

Let $\rho_{A_1\ldots A_n}$ be of the form



Let $\delta = \sqrt{(4\ln 2)\epsilon}$, then

$$\begin{aligned}
\rho_{A_1\ldots A_n} &\approx_\delta \mathcal{T}_{A_{n-1}A_n\leftarrow A_{n-1}}(\rho_{A_1\ldots A_{n-1}}) \\
&\approx_{2\delta} \mathcal{T}_{A_{n-1}A_n\leftarrow A_{n-1}}(\mathcal{T}_{A_{n-2}A_{n-1}\leftarrow A_{n-2}}(\rho_{A_1\ldots A_{n-2}})) \\
&\;\vdots \\
&\approx_{(n-2)\delta} \left(\mathcal{T}_{A_{n-1}A_n\leftarrow A_{n-1}} \circ \cdots \circ \mathcal{T}_{A_2A_3\leftarrow A_2}\right)(\rho_{A_1A_2})
\end{aligned}$$

If $\epsilon \ll \frac{1}{n^2}$, good approximation of $\rho_{A_1\ldots A_n}$ in $O(n)$ memory

Main result: proof sketch

Statement to prove:

$$\exists \mathcal{T} : B \to BC, \quad F(\rho_{ABC}, \mathcal{T}_{BC\leftarrow B}(\rho_{AB})) \geq 2^{-\frac{1}{2} I(A:C|B)}$$

1. Easy special case: **flat marginals** $\rho_B = \frac{\Pi_B}{r_B}$ and $\rho_{BC} = \frac{\Pi_{BC}}{r_{BC}}$

$$F(\rho_{ABC}, \rho_{BC}^{1/2}\rho_B^{-1/2}\rho_{AB}\rho_B^{-1/2}\rho_{BC}^{1/2}) = \sqrt{\frac{r_{BC}}{r_B}} F(\rho_{ABC}, \Pi_{BC}\Pi_B\rho_{AB}\Pi_B\Pi_{BC})$$
$$\geq 2^{-\frac{1}{2}(H(BC)_\rho - H(B)_\rho)} 2^{-\frac{1}{2}D(\rho_{ABC}\|\rho_{AB}\otimes \mathrm{id}_C)} = 2^{-\frac{1}{2}I(A:C|B)_\rho}$$

2. General case $\to \approx$ flat marginals: **study $\rho^{\otimes n}$** and consider types

$$I(A:C|B)_\rho = \frac{I(A^n : C^n|B^n)_{\rho^{\otimes n}}}{n}$$

   Obtain $\mathcal{T}^n_{B^nC^n\leftarrow B^n}$ such that $F(\rho_{ABC}^{\otimes n}, \mathcal{T}^n(\rho_{AB}^{\otimes n})) \geq 2^{-\frac{1}{2}I(A^n:C^n|B^n)_{\rho^{\otimes n}}}$

3. If $\mathcal{T}^n_{B^nC^n\leftarrow B^n} = \mathcal{T}^{\otimes n}_{BC\leftarrow B}$, done.
   For that, **de Finetti reduction**: $\mathcal{T}^n \leq \mathrm{poly}(n) \int \mathcal{T}^{\otimes n} d\mathcal{T}$

Map of known proofs

$$I(A:C|B)_\rho = \frac{1}{n} I(A:C|B)_{\rho^{\otimes n}}$$

$$\geq$$

[FR15]: Properties of fidelity $\mathbb{D} = -2\log F$

[BHOS15]: Quantum state redistribution $\mathbb{D} = D$

[STH16]: Properties of pinching map $\mathbb{D} = D$

$$\frac{1}{n}\mathbb{D}(\rho_{ABC}^{\otimes n} \| \mathcal{T}^n_{B^n C^n \leftarrow B^n}(\rho_{AB}^{\otimes n}))$$

$$\geq$$

[FR15]: de Finetti reduction

[BT15]: SDP duality

[STH16]: Minimax theorem

$$\frac{1}{n}\mathbb{D}(\rho_{ABC}^{\otimes n} \| \mathcal{T}^{\otimes n}_{BC \leftarrow B}(\rho_{AB}^{\otimes n})) = \mathbb{D}(\rho_{ABC} \| \mathcal{T}_{BC \leftarrow B}(\rho_{AB}))$$

Map of known proofs

$$I(A:C|B)_\rho = \frac{1}{n} I(A:C|B)_{\rho^{\otimes n}}$$

$\geq$ [FR15]: Properties of fidelity $\mathbb{D} = -2\log F$

[BHOS15]: Quantum state redistribution $\mathbb{D} = D$

[STH16]: Properties of pinching map $\mathbb{D} = D$

$$\frac{1}{n}\mathbb{D}(\rho_{ABC}^{\otimes n} \| \mathcal{T}^n_{B^n C^n \leftarrow B^n}(\rho_{AB}^{\otimes n}))$$

$\geq$ [FR15]: de Finetti reduction

[BT15]: SDP duality

[STH16]: Minimax theorem

$$\frac{1}{n}\mathbb{D}(\rho_{ABC}^{\otimes n} \| \mathcal{T}^{\otimes n}_{BC \leftarrow B}(\rho_{AB}^{\otimes n})) = \mathbb{D}(\rho_{ABC} \| \mathcal{T}_{BC\leftarrow B}(\rho_{AB}))$$

Proof not following this scheme: see next talk

Conclusion

- Conditional mutual information useful for its additivity properties
- **Main result:**

$$I(A:C|B)_\rho \leq \epsilon$$
$$\Rightarrow \ \rho_{ABC} \text{ approximately satisfies Markov chain condition}$$

- Can show a similar upper bound on $I(A:C|B)$:

$$\frac{1}{4\ln 2}\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1^2 \leq I(A:C|B)_\rho \leq 7\log d_A\sqrt{\|\rho_{ABC} - \mathcal{T}_{BC\leftarrow B}(\rho_{AB})\|_1}$$

Conclusion

- Conditional mutual information useful for its additivity properties
- **Main result:**

$$I(A : C|B)_\rho \leq \epsilon$$
$$\Rightarrow \ \rho_{ABC} \text{ approximately satisfies Markov chain condition}$$

- Can show a similar upper bound on $I(A : C|B)$:

$$\frac{1}{4 \ln 2} \|\rho_{ABC} - \mathcal{T}_{BC \leftarrow B}(\rho_{AB})\|_1^2 \leq I(A : C|B)_\rho \leq 7 \log d_A \sqrt{\|\rho_{ABC} - \mathcal{T}_{BC \leftarrow B}(\rho_{AB})\|_1}$$

- **Open questions:**
  - Many natural improvements: next talk
  - More applications of recoverability: direct sum communication complexity? lower bounds using restricted norms (LOCC, ...)?