Fawzi-Renner Inequality by State Redistribution

Fernando G.S.L. Brandão
University College London -> Microsoft Research

based on arXiv:1411.4921 with

Aram Harrow
Jonathan Oppenheim
Sergii Strelchuk

Coogee 2015

Strong Subadditivity

(Lieb and Ruskai '73) For ρ_{CRB}

$$S(CB) + S(RB) \geq S(CRB) + S(B)$$

Strong Subadditivity and CMI

(Lieb and Ruskai '73) For ρ_{CRB}

$$S(CB) + S(RB) \geq S(CRB) + S(B)$$

Conditional Mutual Information (CMI)

$$I(C:R|B) := S(CB) + S(RB) - S(CRB) - S(B)$$

By SSA: $I(C:R|B) \geq 0$

Strong Subadditivity and CMI

(Lieb and Ruskai '73) For ρ_{CRB}

$$S(CB) + S(RB) \geq S(CRB) + S(B)$$

Conditional Mutual Information (CMI)

$$I(C:R|B) := S(CB) + S(RB) - S(CRB) - S(B)$$

By SSA: $I(C:R|B) \geq 0$

Can we improve SSA?

I.e. Is there a positive non-identically-zero function f *s.t.*

$$I(C:R|B) \geq f(\rho_{CRB})$$

CMI for Probability Distributions

For a probability distribution p_{XYZ}:

$$I(X:Y|Z) = \mathop{\mathbb{E}}_{z' \sim p(z)} I(X:Y)_{p(x,y|z=z')}$$

CMI for Probability Distributions

For a probability distribution p_{XYZ}:

$$I(X:Y|Z) = \mathop{\mathbb{E}}_{z' \sim p(z)} I(X:Y)_{p(x,y|z=z')}$$

and

$$I(X:Y|Z) = \min_{q \in \mathrm{MC}} S(p_{XYZ} || q_{XYZ})$$

MC := {q : x-z-y form a *Markov chain*}

Relative entropy: $$S(p||q) := \sum_i p_i \log(p_i/q_i)$$

CMI for Probability Distributions

For a probability distribution p_{XYZ}:

$$I(X:Y|Z) = \mathop{\mathbb{E}}_{z' \sim p(z)} I(X:Y)_{p(x,y|z=z')}$$

and

$$I(X:Y|Z) = \min_{q \in \mathrm{MC}} S(p_{XYZ} || q_{XYZ})$$

MC := {*q* : x-z-y form a *Markov chain*}

Relative entropy: $S(p||q) := \sum_i p_i \log(p_i / q_i)$

Since $S(p||q) \geq \|p-q\|_1^2 / \ln(4)$ (Pinsker's inequality),

$I(X{:}Y|Z) \leq \varepsilon$ implies p is $O(\varepsilon^{1/2})$ close to a Markov chain

CMI for Probability Distributions

For a probability distribution p_{XYZ}:

$$I(X:Y|Z) = \mathop{\mathbb{E}}_{z' \sim p(z)} I(X:Y)_{p(x,y|z=z')}$$

and

$$I(X:Y|Z) = \min_{q \in \mathrm{MC}} S(p_{XYZ} \| q_{XYZ})$$???

How about for quantum states?

We don’t know how to condition on quantum information…

The second equality could still work. But what is the set of “quantum Markov chains”?

Quantum Markov States

Classical:

i) *x*-*z*-*y* Markov if *x* and *y* are independent conditioned on *z*

Quantum Markov States

Classical:

i) *x-z-y* Markov if *x* and *y* are independent conditioned on *z*

ii) *x-z-y* Markov if there is a channel $\Lambda : Z \to YZ$ s.t. $\Lambda(p_{XZ}) = p_{XYZ}$

Quantum Markov States

Classical:

i) *x-z-y* Markov if *x* and *y* are independent conditioned on *z*

ii) *x-z-y* Markov if there is a channel $\Lambda : Z \rightarrow YZ$ s.t. $\Lambda(p_{XZ}) = p_{XYZ}$

Quantum:

i) ρ_{CRB} Markov quantum state if *C* and *R* are independent conditioned on *B*, i.e. $H_B \simeq \bigoplus_k H_{B_{L,k}} \otimes H_{B_{R,k}}$ and

$$\rho_{CRB} = \bigoplus_k p_k \rho_{CB_{L,k}} \otimes \rho_{B_{R,k}R}$$

Quantum Markov States

Classical:

i) *x-z-y* Markov if *x* and *y* are independent conditioned on *z*

ii) *x-z-y* Markov if there is a channel $\Lambda : Z \to YZ$ s.t. $\Lambda(p_{XZ}) = p_{XYZ}$

Quantum:

i) ρ_{CRB} Markov quantum state if *C* and *R* are independent conditioned on *B*, i.e. $H_B \simeq \bigoplus_k H_{B_{L,k}} \otimes H_{B_{R,k}}$ and

$$\rho_{CRB} = \bigoplus_k p_k \rho_{CB_{L,k}} \otimes \rho_{B_{R,k}R}$$

ii) ρ_{CRB} Markov if there is channel $\Lambda : B \to RB$ s.t. $\Lambda(\rho_{CB}) = \rho_{CRB}$

Quantum Markov States vs CMI

(Hayden, Jozsa, Petz, Winter '03) *I(C:R|B)=0* iff ρ_{CRB} is quantum Markov

$$I(C:R|B)=0$$

$$\rho_{CRB} = \bigoplus_k p_k \rho_{CB_{L,k}} \otimes \rho_{B_{R,k}R}$$

Quantum Markov States vs CMI

(Hayden, Jozsa, Petz, Winter '03) *I(C:R|B)=0* iff ρ_{CRB} is quantum Markov

$$I(C:R|B) = 0$$

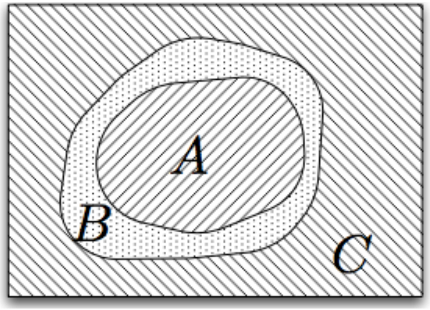
$$\exists \ \Lambda : B \to BR \ \text{ s.t.}$$
$$I_C \otimes \Lambda(\rho_{CB}) = \rho_{CRB}$$

obs:
$$\Lambda(X) = \rho_{RB}^{1/2} \rho_B^{-1/2} X \rho_B^{-1/2} \rho_{RB}^{1/2}$$

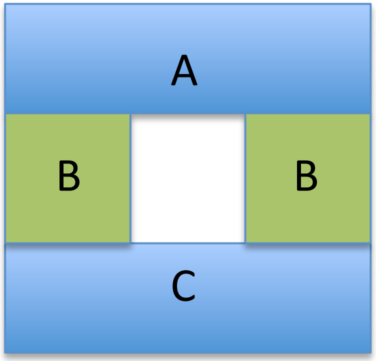
$$\rho_{CRB} = \bigoplus_k p_k \rho_{CB_{L,k}} \otimes \rho_{B_{R,k}R}$$

Applications

(Brown and Poulin '12)
(Quantum Hammersley-Clifford thm) Every many body state with vanishing CMI is the Gibbs state of a commuting model (on triangle-free graphs)



(Lewin and Wen '06)
CMI is equal to twice topological entanglement entropy. If $S(X) = a|\partial X| - \gamma$, I(A:C|B) = 2γ



(Kitaev, unpublished)
If γ=0, the state (+ ancilas) can be created by a constant depth circuit

What if merely CMI ≈ 0? (Ex. $S(X) = a|\partial X| - \gamma + 2^{-O(|\partial X|)}$)

CMI vs Quantum Markov States

Does $I(C:R|B)_\rho \geq \Omega\left(\min_{\sigma_{CRB} \in QMC} S(\rho||\sigma)\right)$?

or just $I(C:R|B) \geq f\left(\min_{\sigma_{CRB} \in \mathrm{QMC}} \|\rho - \sigma\|_1\right)$?

QMC := {σ_{CRB} : $\sigma_{CRB} = \bigoplus_k p_k \rho_{CB_{L,k}} \otimes \rho_{B_{R,k}R}$ }

CMI vs Quantum Markov States

Does $I(C:R|B)_\rho \geq \Omega\left(\min_{\sigma_{CRB} \in QMC} S(\rho||\sigma)\right)$?

or just $I(C:R|B) \geq f\left(\min_{\sigma_{CRB} \in \text{QMC}} \|\rho - \sigma\|_1\right)$?

NO!!!

QMC := {σ_{CRB} : $\sigma_{CRB} = \bigoplus_k p_k \rho_{CB_{L,k}} \otimes \rho_{B_{R,k}R}$ }

(Ibinson, Linden, Winter '06; Christandl, Schuch, Winter '11)

If ρ_{CRB} is QMC, ρ_{CR} is *separable* ($\sigma_{CR} = \sum_k p_k \rho_{C,k} \otimes \rho_{R,k}$)

For an extension ρ_{CRB} of the *d x d* anti-symmetric state ρ_{CR},

$$I(C:R|B)_\rho \leq 2/d \qquad \min_{\sigma_{CR} \in \text{SEP}} \|\rho_{CR} - \sigma_{CR}\|_1 \geq 1/4$$

Partial Progress

(B., Christandl, Yard '10; Li, Winter '12; B., Harrow, Lee, Peres '13)

$$I(C:R|B) \geq \min_{\sigma_{CR} \in \mathrm{SEP}} \max_{M_R \in \mathcal{M}} S(I_C \otimes M_R(\rho_{CR}) || I_C \otimes M_R(\sigma_{CR}))$$

$$\mathcal{M} := \{M(X) \sum_i \mathrm{tr}(L_i X)|i\rangle\langle i|, \quad L_i \geq 0, \sum_i L_i = I\}$$

Applications: quasipolynomial-time algorithm for testing separability, faithfulness squashed entanglement, SoS hierarchy, etc…

Partial Progress

(B., Christandl, Yard '10; Li, Winter '12; B., Harrow, Lee, Peres '13)

$$I(C:R|B) \geq \min_{\sigma_{CR} \in \mathrm{SEP}} \max_{M_R \in \mathcal{M}} S(I_C \otimes M_R(\rho_{CR}) || I_C \otimes M_R(\sigma_{CR}))$$

$$\mathcal{M} := \{M(X) \sum_i \mathrm{tr}(L_i X)|i\rangle\langle i|, \quad L_i \geq 0, \sum_i L_i = I\}$$

Applications: quasipolynomial-time algorithm for testing separability, faithfulness squashed entanglement, SoS hierarchy, etc…

How about the distance to QMC? Open question:

$$I(C:R|B) \overset{?}{\geq} \min_{\sigma \in \mathrm{QMC}} \max_{M_C, M_R, M_B} S(M_C \otimes M_R \otimes M_B(\rho) || M_C \otimes M_R \otimes M_B(\sigma))$$

Approximate Reconstruction

"Small CMI" and "being close to QMC state" are *not* equivalent
(in a dimensional independent way for trace norm or fidelity)

Classically:

$$I(X:Y|Z) = \min_{q \in \mathrm{MC}} S(p||q)$$
$$= \min_{\Lambda : Z \to YZ} S(p_{XYZ}||I_X \otimes \Lambda(p_{XZ}))$$

Approximate Reconstruction

"Small CMI" and "being close to QMC state" are *not* equivalent
(in a dimensional independent way for trace norm or fidelity)

Classically: $$I(X:Y|Z) = \min_{q \in \mathrm{MC}} S(p||q) = \min_{\Lambda : Z \to YZ} S(p_{XYZ}||I_X \otimes \Lambda(p_{XZ}))$$

Conjecture (I. Kim; A. Kitaev; L. Zhang; Berta, Seshadreesan, Wilde, …)

$$I(C:R|B) \geq \min_{\Lambda : B \to RB} S(\rho_{CRB}||I_C \otimes \Lambda(\rho_{CB}))$$

or $$I(C:R|B) \geq f\left(\min_{\Lambda : B \to RB} \|\rho_{CRB} - I_C \otimes \Lambda(\rho_{CB})\|_1\right)$$

Fawzi-Renner Inequality

thm (Fawzi, Renner '14)

$$I(C:R|B) \geq \min_{\Lambda: B \to RB} -2\log(F(\rho_{CRB}, I_C \otimes \Lambda_B(\rho_{CB})))$$

Fidelity: $F(\rho, \sigma) := \mathrm{tr}(\sqrt{\sigma^{1/2}\rho\sigma^{1/2}})$

½ Renyi Relative Entropy: $S_{1/2}(\rho||\sigma) := -2\log(F(\rho,\sigma))$

We have: $S(\rho||\sigma) \geq S_{1/2}(\rho||\sigma)$

Weaker than classical inequality

Strengthening of Fawzi-Renner

thm (B., Harrow, Oppenheim, Strelchuk '14)

$$I(C:R|B)_\rho$$

$$\geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

Strengthening of Fawzi-Renner

thm (B., Harrow, Oppenheim, Strelchuk '14)

$$I(C:R|B)_\rho$$

$$\geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

$$\geq \min_{\Lambda : B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

$$\mathbb{M}S(\rho||\sigma) := \max_{M \in \mathcal{M}} S(M(\rho)||M(\sigma))$$

$$\mathcal{M} := \{M : M(X) = \sum_i \mathrm{tr}(L_i X)|i\rangle\langle i|, \;\; L_i \geq 0, \;\; \sum_i L_i = I\}$$

Strengthening of Fawzi-Renner

thm (B., Harrow, Oppenheim, Strelchuk '14)

$$I(C:R|B)_\rho$$

$$\geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

$$\geq \min_{\Lambda: B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

$$\geq \min_{\Lambda: B \to BC} S_{1/2}(\rho_{BCR} \| \Lambda \otimes I_R(\rho_{BR}))$$

Strengthening of Fawzi-Renner

thm (B., Harrow, Oppenheim, Strelchuk '14)

$$I(C:R|B)_\rho$$

$$\geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

$$\geq \min_{\Lambda : B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

$$\geq \min_{\Lambda : B \to BC} S_{1/2}(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

From: $S(\rho||\sigma) \geq S_{1/2}(\rho||\sigma)$ and $\min_{M \in \mathcal{M}} F(M(\rho), M(\sigma)) = F(\rho, \sigma)$

Strengthening of Fawzi-Renner

thm (B., Harrow, Oppenheim, Strelchuk '14)

$$I(C:R|B)_\rho$$

$$\geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

$$\geq \min_{\Lambda : B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

$$\geq \min_{\Lambda : B \to BC} S_{1/2}(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

From: $S(\rho||\sigma) \geq S_{1/2}(\rho||\sigma)$ and $\min_{M \in \mathcal{M}} F(M(\rho), M(\sigma)) = F(\rho, \sigma)$

From: Properties relative entropy (Piani '09)

Strengthening of Fawzi-Renner

thm (B., Harrow, Oppenheim, Strelchuk '14)

$$I(C:R|B)_\rho$$

$$\geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

$$\geq \min_{\Lambda : B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

$$\geq \min_{\Lambda : B \to BC} S_{1/2}(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

- From: $S(\rho||\sigma) \geq S_{1/2}(\rho||\sigma)$ and $\min_{M \in \mathcal{M}} F(M(\rho), M(\sigma)) = F(\rho, \sigma)$
- From: Properties relative entropy (Piani '09)
- From: State Redistribution Protocol (Devetak, Yard '04)

Comparison Lower Bounds on CMI

$$I(C:R|B) \geq \min_{\sigma_{CR} \in \text{SEP}} \max_{M_R \in \mathcal{M}} S(I_C \otimes M_R(\rho_{CR}) || I_C \otimes M_R(\sigma_{CR}))$$

1. State Redistribution:

$$I(C:R|B) \quad \geq \quad E_R^\infty(\rho_{C:BR}) - E_R^\infty(\rho_{C:B})$$

Regularized relative entropy of entanglement:

$$E_R^\infty(\rho_{A:B}) := \lim_{n \to \infty} \frac{1}{n} \min_{\sigma_{A^n B^n} \in \text{SEP}} S(\rho_{AB}^{\otimes n} || \sigma_{A^n B^n})$$

2. Hypothesis Testing:

$$E_R^\infty(\rho_{C:BR}) - E_R^\infty(\rho_{C:B}) \geq \min_{\sigma_{CR} \in \text{SEP}} \max_{M_R \in \mathcal{M}} S(I_C \otimes M_R(\rho_{CR}) || I_C \otimes M_R(\sigma_{CR}))$$

$$I(C:R|B) \geq \min_{\Lambda: B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

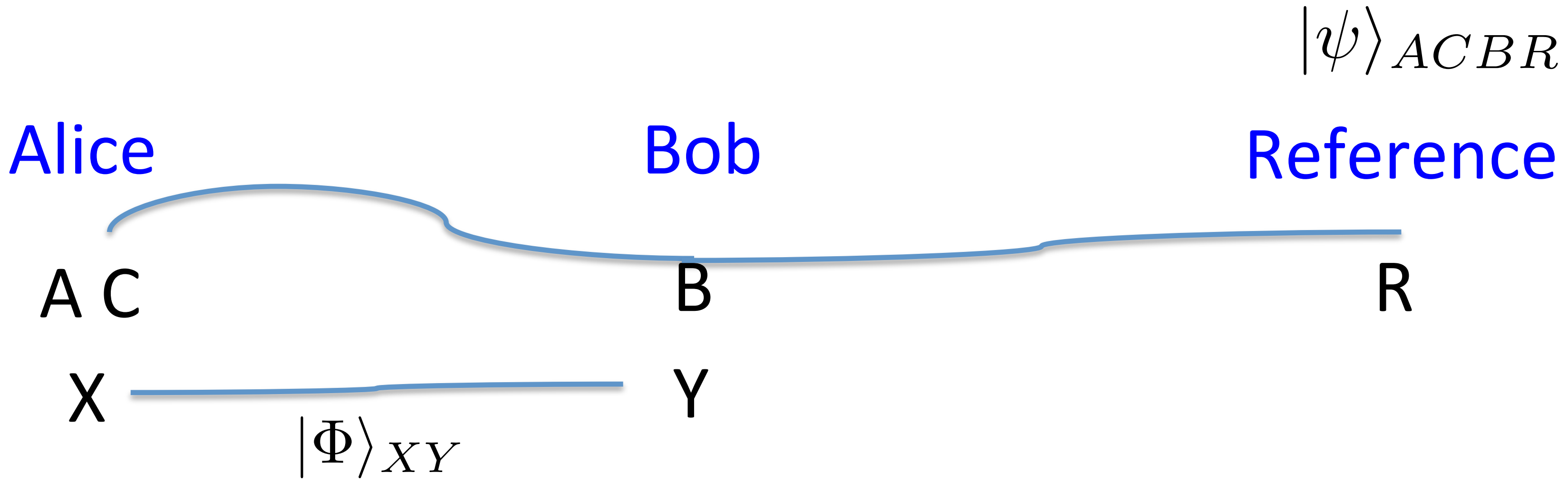
1. State Redistribution:

$$I(C:R|B) \geq \lim_{n \to \infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda_n \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$$

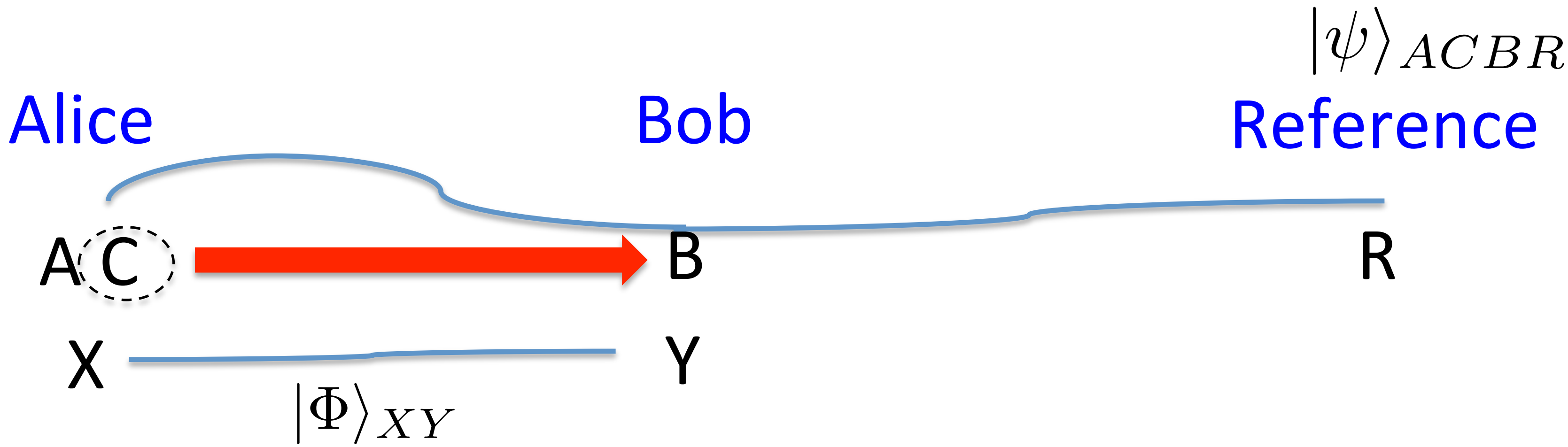
2. Hypothesis Testing:

$$\geq \min_{\Lambda: B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes I_R(\rho_{BR}))$$

State Redistribution



State Redistribution



(Devetak, Yard '06)

Optimal quantum communication rate: *½ I(C:R|B)*

I.e. there exist encodings E_n : $A^nC^nX_n$ -> A^nG_n and
decodings D_n : $B^nG_nY_n$ -> B^nC^n s.t.

$$\lim_{n\to\infty} \| D_n \circ E_n(|\psi\rangle\langle\psi|_{ABCR}^{\otimes n} \otimes \Phi_{X_nY_n}) - |\psi\rangle\langle\psi|_{ABCR}^{\otimes n}\|_1 = 0$$

$$\lim_{n\to\infty} \frac{\log \dim(G_n)}{n} = \frac{1}{2} I(C:R|B)$$

Proof of …

… $I(C:R|B) \geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$

Idea: Consider the optimal state redistribution protocol and replace the quantum communication by white noise (maximally mixed state)

Proof of …

… $I(C:R|B) \geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$

Idea: Consider the optimal state redistribution protocol and replace the quantum communication by white noise (maximally mixed state)

After encoding: $\phi_{G_n Y_n A^n B^n R^n} := E_n \otimes I_{B^n R^n Y_n}(|\psi\rangle\langle\psi|_{ABCR}^{\otimes n} \otimes \Phi_{X_n Y_n})$

As $\phi_{G_n Y_n B^n R^n} \leq \dim(G_n) I_{G_n} \otimes \phi_{Y_n B^n R^n}$ and $\phi_{Y_n B^n R^n} = \tau_{Y_n} \otimes \rho_{BR}^{\otimes n}$

$$(D_n \otimes I_{R^n})(\tau_{G_n} \otimes \tau_{Y_n} \otimes \rho_{BR}^{\otimes n}) \geq \dim(G_n)^{-2} (D_n \otimes I_{R^n})(\phi_{G_n Y_n B^n R^n})$$

Proof of …

… $I(C:R|B) \geq \lim_{n\to\infty} \min_{\Lambda_n : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes I_{R^n}(\rho_{BR}^{\otimes n}))$

Idea: Consider the optimal state redistribution protocol and replace the quantum communication by white noise (maximally mixed state)

After encoding: $\phi_{G_n Y_n A^n B^n R^n} := E_n \otimes I_{B^n R^n Y_n}(|\psi\rangle\langle\psi|_{ABCR}^{\otimes n} \otimes \Phi_{X_n Y_n})$

As $\phi_{G_n Y_n B^n R^n} \leq \dim(G_n) I_{G_n} \otimes \phi_{Y_n B^n R^n}$ and $\phi_{Y_n B^n R^n} = \tau_{Y_n} \otimes \rho_{BR}^{\otimes n}$

$$(D_n \otimes I_{R^n})(\tau_{G_n} \otimes \tau_{Y_n} \otimes \rho_{BR}^{\otimes n}) \geq \dim(G_n)^{-2}(D_n \otimes I_{R^n})(\phi_{G_n Y_n B^n R^n})$$

By op monotonicity of the log:

$$\begin{aligned} & S(\rho_{BCR}^{\otimes n} || (D_n \otimes I_{R^n})(\tau_{G_n} \otimes \tau_{Y_n} \otimes \rho_{BR}^{\otimes n})) \\ \leq \quad & S(\rho_{BCR}^{\otimes n} || (D_n \otimes I_{R^n})(\phi_{G_n Y_n B^n R^n})) + 2\log(\dim(G_n)) \end{aligned}$$

0 $\qquad\qquad\qquad\qquad$ $nI(C:R|B)$

Open questions:

- Improve bound to relative entropy (like the classical)

- Prove the bound for the transpose channel

- Prove Li-Winter conjecture:
  For every states *ρ, σ* and channel *Λ* there is a channel *Γ* s.t.
  Γ(Λ(σ)) = σ and

$$S(\rho||\sigma) \geq S(\Lambda(\rho)||\Lambda(\sigma)) + S(\rho||\Gamma \circ \Lambda(\rho))$$

  see (Berta, Lemm, Wilde '14) for partial progress

- Find (more) applications of the FR inequality!
- Find more improvements of SSA; see (Kim '12) for another

- (dis)Prove: $I(C:R|B) \geq$

$$\min_{\sigma \in \text{QMC}} \max_{M_C, M_R, M_B} S(M_C \otimes M_R \otimes M_B(\rho)||M_C \otimes M_R \otimes M_B(\sigma))$$