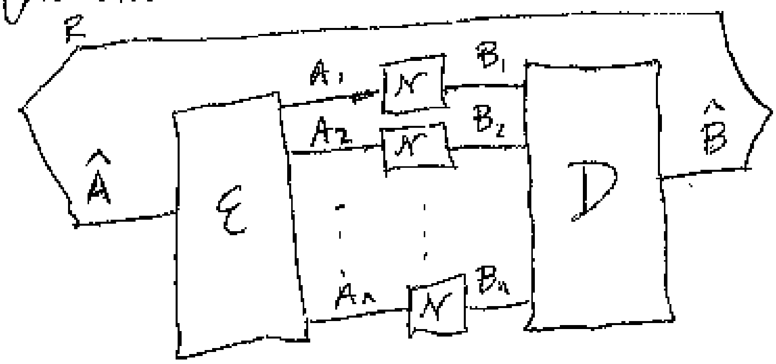
Strong converse bounds for quantum communication

arXiv:1406.2946

joint w/ Marco Tomamichel & Andreas Winter

Quantum capacity of a channel is equal to the maximum rate at which a sender can transmit quantum data to a receiver such that he can recover it w/ arbitrarily high fidelity in the limit of many channel uses.

In more detail, a (n, Q, ε) code for quantum communication consists of



$\mathcal{E}$ - encoding, $\mathcal{D}$ - decoding

& is such that

$$\forall \rho_{R\hat{A}} \quad F\left(\mathcal{D}_{B^n\to\hat{B}}\left(\mathcal{N}_{A^n\to B^n}\left(\mathcal{E}_{\hat{A}\to A^n}\left(\rho_{R\hat{A}}\right)\right)\right), \rho_{R\hat{B}}\right) \geq 1-\varepsilon$$

where $\mathcal{N}_{A^n\to B^n} = \mathcal{N}^{\otimes n}$

rate of q. comm. is $\frac{\log|\hat{A}|}{n} = Q$

A rate Q is achievable if
$\forall \varepsilon > 0$ + sufficiently large n
$\exists$ an (n, Q, ε) code.

Quantum capacity of a channel is
the supremum of all achievable rates.

Two parts to establishing the
quantum capacity theorem.

1) Achievability - Prove the existence of
a sequence of codes
where $Q(\mathcal{N})$ is an
achievable rate.

2) Weak Converse - Show that Q
is not an achievable
rate if $Q > Q(\mathcal{N})$

Let $M^*(\mathcal{N}^{\otimes n}, \varepsilon)$ be the maximum
dimension of a quantum system such that
$\exists$ an $(n, \frac{\log M^*}{n}, \varepsilon)$ code exists

Then 1) establishes

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \log M^*(\mathcal{N}, \varepsilon) \geq L(\mathcal{N})$$

& 2) establishes $U(N) \geq \lim_{\varepsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M^*(\mathcal{N}^{\otimes n}, \ldots$

If $U(N) = L(N)$ matches, then the theorem is proved.

Best known characterization of quantum capacity is in terms of coherent information

$$I_c(N) = \max_{\phi_{RA}} I(R\rangle B)_\rho \quad \& \quad Q(N) = \lim_{n\to\infty} \frac{1}{n} I_c(N^{\otimes n})$$

where $\rho_{RB} = N_{A\to B}(\phi_{RA})$ &

$I(R\rangle B) = H(B) - H(RB)$ where

$$H(B) = -\text{Tr}\{\rho_B \log \rho_B\}$$
$$H(RB) = -\text{Tr}\{\rho_{RB} \log \rho_{RB}\}$$

can also write $I(R\rangle B)$ as

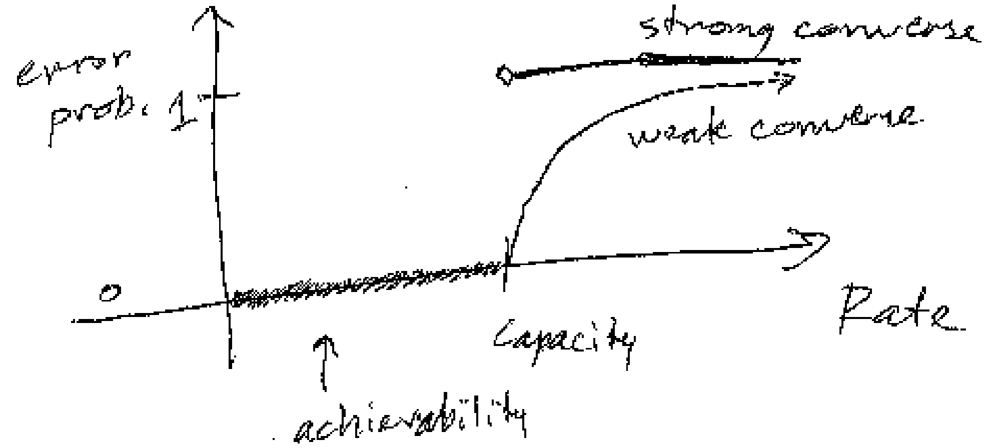
$$I(R\rangle B) \equiv \min_{\sigma_B} D(\rho_{RB} \| I_R \otimes \sigma_B)$$

where $D(\omega \| \tau) = \text{Tr}\{\omega[\log \omega - \log \tau]\}$

If we think of relative entropy as a distance, in some sense, coherent info. compares output of channel ρ_{RB} w/ a "state" $I_R \otimes \sigma_B$ that is output from a "useless" channel

Weak converse theorem can be improved classically to establish what is known as a strong converse theorem

Idea of strong converse: (picture in limit as $n \to \infty$)



strong converse eliminates possibility of a trade-off between rate & error probability.

Main result: The Rains information of a channel is a strong converse bound for quantum communication. I.e., if rate exceeds Rains info., then fidelity of scheme tends to zero exponentially fast w/ increasing # of channel uses.

Idea of Rains information is to compare output of the channel w/ a different class of states that are useless for sending quantum data.

$$R(\mathcal{N}) = \max_{\phi_{RA}} \min_{\tau_{RB} \in \mathcal{T}(R:B)} D(\rho_{RB} \| \tau_{RB})$$

where $\rho_{RB} = \mathcal{N}_{A\to B}(\phi_{RA})$

& $\mathcal{T}(R:B) \equiv \{ \tau_{RB} : \tau_{RB} \geq 0 \wedge \| T_B(\tau_{RB}) \|_1 \leq 1 \}$

where T_B is the partial transpose operation. The set $\mathcal{T}(R:B)$ is closely related to the PPT set of states. It contains the PPT set of states & constitutes a set of states which have no distillable entanglement & are thus useless for sending quantum data.

Rains entropy of state ρ_{RB}

$$R(\rho_{RB}) \equiv \min_{\tau_{RB} \in \mathcal{T}(R:B)} D(\rho_{RB} \| \tau_{RB})$$

is monotone decreasing under LOCC b/c set $\mathcal{T}(R:B)$ is preserved under LOCC

Property of $\tau_{RB} \in \mathcal{T}(R:B)$ essential for our application. If we ask whether it is maximally entangled or not, the chance of getting the answer "yes" is very small, i.e.,

$$\mathrm{Tr}\{\tau_{RB}\,\Phi_{RB}\} \leq \frac{1}{M}$$

where M is Schmidt rank of Φ_{RB}

This is b/c $\mathrm{Tr}\{\Phi_{RB}\,\tau_{RB}\}$

$$= \mathrm{Tr}\{T_B(\Phi_{RB})\,T_B(\tau_{RB})\}$$

$$= \frac{1}{M}\,\mathrm{Tr}\{F_{RB}\,T_B(\tau_{RB})\}$$

$$\leq \frac{1}{M}\,\|T_B(\tau_{RB})\|_1 \leq \frac{1}{M}$$

Covariance lemma for Rains information:

Let $N_{A\to B}$ be a covariant channel w/ respect to a group G + unitary representations $U_A(g)$ + $V_B(g)$

$\forall g \in G, \rho \quad \mathcal{N}_{A\to B}(U_A(g)\,\rho\, U_A^\dagger(g))$

$\quad = V_B(g)\, \mathcal{N}_{A\to B}(\rho)\, V_B^\dagger(g)$

Given density operator ρ_A, let $|\phi^\rho\rangle_{RA}$ be a purification of it.

Consider group averaged state

$$\bar{\rho}_A = \frac{1}{|G|} \sum_g U_A(g)\, \rho_A\, U_A^\dagger(g)$$

& let $|\phi^{\bar\rho}\rangle_{RA}$ be a purification

Then $R(\mathcal{N}_{A\to B}(\phi^{\bar\rho}_{RA})) \geq R(\mathcal{N}_{A\to B}(\phi^\rho_{RA}$

Pf. Consider

$$|\psi\rangle_{PRA} = \sum_g \frac{1}{\sqrt{|G|}} |g\rangle_P [I_R \otimes U_A(g)] |\phi^\rho\rangle_{RA}$$

this is a purification of $\bar{\rho}_A$.

Let $\tau_{PRB} \in \mathcal{T}(PR:B)$

Consider that

$$D\left(\mathcal{N}_{A\to B}(\psi_{PRA}) \,\|\, \tau_{PRB}\right)$$

$$\geq D\Big(\sum_g \frac{1}{|G|} |g\rangle\langle g|_P \otimes \mathcal{N}_{A\to B}\big(\mathcal{U}_A(g)\phi^{\rho}_{RA}\mathcal{U}_A^{\dagger}(g)\big) \,\|\, \sum_g p(g)\, |g\rangle\langle g|_P \otimes \tau^{g}_{RB}\Big)$$

$$= D\Big(\sum_g \frac{1}{|G|} |g\rangle\langle g|_P \otimes V_B(g)\, \mathcal{N}_{A\to B}(\phi^{\rho}_{RA})\, V_B^{\dagger}(g) \,\|\, \cdots\Big)$$

$$= D\Big(\sum_g \frac{1}{|G|} |g\rangle\langle g|_P \otimes \mathcal{N}_{A\to B}(\phi^{\rho}_{RA}) \,\|\, \sum_g p(g)\, |g\rangle\langle g|_P \otimes V_B^{\dagger}(g)\, \tau^{g}_{RB}\, V_B(g)\Big)$$

$$\geq D\Big(\mathcal{N}_{A\to B}(\phi^{\rho}_{RA}) \,\|\, \sum_g p(g)\, V_B^{\dagger}(g)\, \tau^{g}_{RB}\, V_B(g)\Big)$$

$$\geq R\left(\mathcal{N}_{A\to B}(\phi^{\rho}_{RA})\right)$$

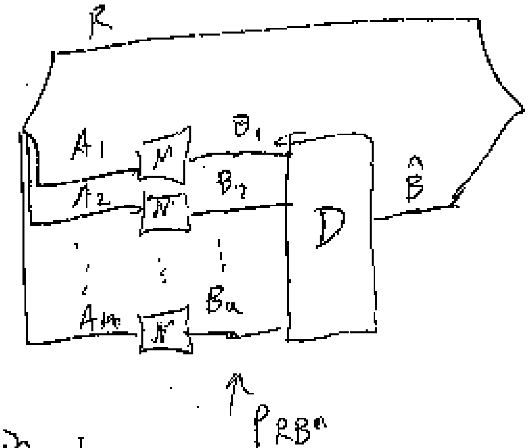
works for any relative entropy

divergence framework —

Use sandwiched Renyi relative entropy

$$\widetilde{D}_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{Tr}\left\{\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\,\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right\}$$

consider only codes for entanglement generation, i.e.,



begin by comparing ρ_{RB^n} to $\tau_{RB^n} \in \mathcal{T}(R:B^n)$

$$\widetilde{D}_\alpha(\rho_{RB^n}\|\tau_{RB^n}) \geq \widetilde{D}_\alpha(\mathcal{D}_{B^n\to\hat{B}}(\rho_{RB^n})\|\mathcal{D}_{B^n\to\hat{B}}(\tau_{RB^n}))$$

Now perform a measurement

$\{\Phi_{R\hat{B}}, I_{R\hat{B}} - \Phi_{R\hat{B}}\}$ is entanglement decoded or not?

result on 1st state is $(F, 1-F)$

~~result~~ on second operator is (s, t)

Plugging into Renyi entropies gives

$$\geq \frac{1}{\alpha-1} \log \left\{ F^{\alpha} s^{1-\alpha} + (1-F)^{\alpha} t^{1-\alpha} \right\}$$ take $\alpha > 1$

$$\geq \frac{1}{\alpha-1} \log \left\{ F^{\alpha} s^{1-\alpha} \right\}$$

$$\geq \frac{1}{\alpha-1} \log \left\{ F^{\alpha} \left(\frac{1}{M}\right)^{1-\alpha} \right\}$$

$$= \frac{\alpha}{\alpha-1} \log F + \log M$$

the bound holds for any choice of $\tau_{R:B^n} \in \mathcal{T}(R:B^n)$ so take a minimum over all of them

$$\min_{\tau_{RB^n}} \tilde{D}_{\alpha}(\rho_{RB^n} \| \tau_{RB^n}) \geq \frac{\alpha}{\alpha-1} \log F + \log M$$

remove the dependence on any particular code by maximizing over all input states. We then get

$$F \leq 2^{-n\left(\frac{\alpha-1}{\alpha}\right)\left(Q - \frac{\tilde{R}_{\alpha}(\mathcal{N}^{\otimes n})}{n}\right)}$$

goal now becomes to show that $\tilde{R}_{\alpha}(\mathcal{N}^{\otimes n})$ obeys some kind of subadditivity

For this, consider that the channel is covariant w.r.t. permutations, i.e.,

$$\forall \pi \in S_n: \quad W^{\pi}_{B^n} \mathcal{N}^{\otimes n}(\rho_{A^n}) (W^{\pi}_{B^n})^{\dagger} =$$

$$\mathcal{N}^{\otimes n}\left(W^{\pi}_{A^n} \rho_{A^n} (W^{\pi}_{A^n})^{\dagger} \right)$$

so we can conclude that (from covariance lemma)

$$\tilde{R}_{\alpha}\left(\mathcal{N}_{A^n \to B^n}(\phi^{\rho}_{RA^n}) \right) \leq$$

$$\tilde{R}_{\alpha}\left(\mathcal{N}_{A^n \to B^n}(\phi^{\bar{\rho}}_{RA^n}) \right)$$

where $\phi^{\bar{\rho}}_{RA^n}$ is a purification of a permutation invariant state

$$\bar{\rho}_{A^n} \equiv \frac{1}{n!} \sum_{\pi \in S_n} W^{\pi}_{A^n} \rho_{A^n} (W^{\pi}_{A^n})^{\dagger}$$

$\phi^{\bar{\rho}}_{RA^n}$ is related by a unitary on the reference to $|\psi\rangle_{\hat{A}^n A^n} \in \mathrm{Sym}\left((\hat{A} \otimes A)^{\otimes n} \right)$

Since this is the case, we can apply the operator inequality

$$\psi_{\hat{A}^n A^n} \leq \Pi_{\mathrm{Sym}((\hat{A} \otimes A)^{\otimes n})} \leq \underbrace{n^{|A|^2} \int d\mu(\phi) \, (|\phi\rangle\langle\phi|_{\hat{A}A})^{\otimes n}}_{\text{de Finetti representation}}$$

work a bit, using properties of $\widetilde{D}_\alpha$, to arrive at

$$\widetilde{R}_\alpha(N^{\otimes n}) \leq n\widetilde{R}_\alpha(N) + \frac{\alpha |A|^2}{\alpha-1} \log n$$

So plugging into bound on fidelity, we get

$$F \leq 2^{-n\left(\frac{\alpha-1}{\alpha}\right)\left(Q - \widetilde{R}_\alpha(N) - \frac{\alpha|A|^2}{\alpha-1}\frac{\log n}{n}\right)}$$

$$= n^{|A|^2} \, 2^{-n\left(\frac{\alpha-1}{\alpha}\right)\left(Q - \widetilde{R}_\alpha(N)\right)}$$

Using fact that

$$\lim_{\alpha \to 1^+} \widetilde{R}_\alpha(N) = R(N)$$

if $Q > R(N)$ we can always find $\alpha > 1$ such that $Q > \widetilde{R}_\alpha(N)$ so that strong converse exponent

$$\left(\frac{\alpha-1}{\alpha}\right)\left(Q - \widetilde{R}_\alpha(N)\right) > 0$$

& fidelity decays exponentially fast

Main application is to establish strong converse for quantum capacity of all generalized dephasing channels.

$$\mathcal{N}(\rho) = \sum_{x,y} \langle x|_A \rho |y\rangle_A \langle \psi_y|\psi_x\rangle |x\rangle\langle y|_B$$

where $\{|x\rangle_A\}$ is O.N.

$\{|x\rangle_B\}$ is O.N. but

$\{|\psi_x\rangle\}$ is arbitrary

we get this b/c

$I_c(\mathcal{N}) = R(\mathcal{N})$ for these channels.