The Quantum Capacity of a Quantum Quannel

Francesco Battistel

TopMath-IMPRS Spring School
Quantum Entropy and its Use

31.03.2017

Fidelity

Recall the following facts:

- $F(\rho, \sigma) = \left(\operatorname{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)^2 = F(\sigma, \rho)$
- $0 \leq F(\rho, \sigma) \leq 1$
- $F(\rho, \sigma) = 1 \iff \rho = \sigma$
- $F(\rho, |\sigma\rangle\langle\sigma|) := F(\rho, |\sigma\rangle) = \langle\sigma|\rho|\sigma\rangle$

Definition of Capacity

We define the **rate** of a code as

$$\frac{1}{n}\log_2 \dim \mathcal{H}_{A'^{(n)}} := \frac{k^{(n)}}{n} \tag{1}$$

i.e. "the number of (logical) qubits sent per channel use".

Definition of Capacity

We define the **rate** of a code as

$$\frac{1}{n}\log_2 \dim \mathcal{H}_{A'^{(n)}} := \frac{k^{(n)}}{n} \tag{1}$$

i.e. "the number of (logical) qubits sent per channel use".

Q is said to be an **achievable rate** if $\forall \epsilon, \delta > 0$ there exist a sequence of codes such that, for n sufficiently large, the rate is at least $Q - \delta$ and

$$F\left(\mathcal{R} \circ \mathcal{N}^{\otimes n} \circ \mathcal{E}\left(|\psi^{RA'^{(n)}}\rangle\langle\psi^{RA'^{(n)}}|\right), |\psi^{RA'^{(n)}}\rangle\right) \geq 1 - \epsilon \tag{2}$$

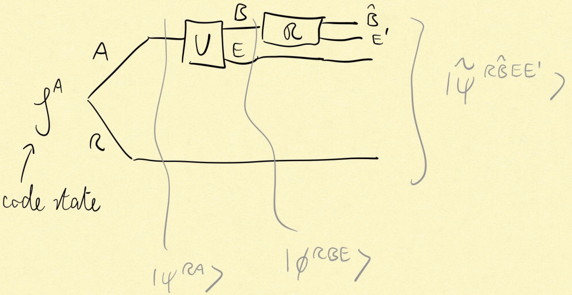
$\forall \rho^{A'^{(n)}}$ where $|\psi^{RA'^{(n)}}\rangle$ is its purification on the reference system.

The **quantum capacity** $Q(\mathcal{N})$ is the supremum of all achievable rates.

Some notation: $\mathcal{N}^{A\to B}$

Stinespring dilation $U_{\mathcal{N}}^{A\to BE}$

$\mathcal{R}^{B\to \hat{B}}$ with $V_{\mathcal{R}}^{B\to \hat{B}E'}$



Coherent Information

In our setting we define

$$
\begin{aligned}
I_c(R\rangle B)_\phi &:= -H(R|B)_\phi && (3)\\
&= -\big(H(RB) - H(B)\big) = H(B) - H(E) && (4)\\
&= \frac{1}{2}\big(I(R;B) - I(R;E)\big) && (5)
\end{aligned}
$$

Coherent Information

Coherent Information

In our setting we define

$$I_c(R\rangle B)_\phi := -H(R|B)_\phi \tag{3}$$
$$= -\big(H(RB) - H(B)\big) = H(B) - H(E) \tag{4}$$
$$= \frac{1}{2}\big(I(R;B) - I(R;E)\big) \tag{5}$$

Quantum data-processing inequality

$$I_c(R\rangle A) \geq I_c(R\rangle B) \geq I_c(R\rangle C) \tag{6}$$

given channels $\mathrm{id}_R \otimes \mathcal{M}_1^{A\to B}$ and $\mathrm{id}_R \otimes \mathcal{M}_2^{B\to C}$.

One-Shot Quantum Capacity

$$Q_1(\mathcal{N}) \coloneqq \max_A I_c(R\rangle B)_\phi \tag{7}$$

where the maximization is taken over all density matrices on A.

Lloyd-Shor-Devetak Theorem

$$Q(\mathcal{N}) = \lim_n \frac{1}{n} \max_{A^n} I_c(R^n\rangle B^n)_{\phi^{R^n B^n E^n}} \tag{8}$$

$$= \lim_n \frac{1}{n} Q_1(\mathcal{N}^{\otimes n}) \tag{9}$$

Outline

- Definition of Capacity
- Coherent Information
- Decoupling Principle
- An Upper Bound on the Quantum Capacity
- Coherent Information as an Achievable Rate
- Additivity Issues and Superactivation

Exact Recoverability

We say that Bob can **perfectly recover** $|\psi^{RA}\rangle$ prepared by Alice if

$$|\tilde{\psi}^{R\hat{B}EE'}\rangle = |\psi^{R\hat{B}}\rangle \otimes |\chi^{EE'}\rangle \tag{10}$$

for some χ, which is equivalent to the condition

$$F(R^{B\to\hat{B}}(\phi^{RB}), |\psi^{RA}\rangle) = 1 \tag{11}$$

Exact Recoverability

We say that Bob can **perfectly recover** $|\psi^{RA}\rangle$ prepared by Alice if

$$|\tilde{\psi}^{R\hat{B}EE'}\rangle = |\psi^{R\hat{B}}\rangle \otimes |\chi^{EE'}\rangle \tag{10}$$

for some χ, which is equivalent to the condition

$$F(R^{B\to\hat{B}}(\phi^{RB}), |\psi^{RA}\rangle) = 1 \tag{11}$$

Exact Decoupling

We say that the reference and the environment are **exactly decoupled** if

$$\phi^{RE} = \phi^{R} \otimes \phi^{E}. \tag{12}$$

Theorem: exact recoverability $\iff$ exact decoupling.

Proof " $\implies$ ": for the initial and final states we have

$$I_c(R\rangle A)_\psi = -H(R|A) = -H(RA) + H(R) = H(R) \quad (13)$$
$$I_c(R\rangle \hat{B})_{\tilde{\psi}} = -H(R|\hat{B}) = -H(R\hat{B}) + H(R) = H(R) \quad (14)$$

By the quantum data-processing inequality also the intermediate must have the same coherent information

$$\begin{aligned} H(R) &= I_c(R\rangle B)_\phi && (15)\\ &= H(B)_\phi - H(E)_\phi && (16)\\ &= H(RE)_\phi - H(E)_\phi && (17) \end{aligned}$$

$$\implies H(RE) = H(R) + H(E) \quad \implies \phi^{RE} = \phi^R \otimes \phi^E. \quad (18)$$

Approximate Recoverability

$|\psi^{RA}\rangle$ is ϵ-**recoverable** if there exist a recovery such that:

$$F(\mathcal{R}^{B\to\hat{B}}(\phi^{RB}), |\psi^{RA}\rangle) \geq 1-\epsilon. \tag{19}$$

Approximate Recoverability

$|\psi^{RA}\rangle$ is ϵ-**recoverable** if there exist a recovery such that:

$$F(\mathcal{R}^{B\to\hat{B}}(\phi^{RB}), |\psi^{RA}\rangle) \geq 1 - \epsilon. \tag{19}$$

Approximate Decoupling

We say that there's ϵ-**decoupling** between reference and environment if

$$||\phi^{RE} - \tilde{\phi}^R \otimes \tilde{\phi}^E||_1 \leq \epsilon \tag{20}$$

for some $\tilde{\phi}^R, \tilde{\phi}^E$.

Theorem: ϵ-decoupling $\implies$ ϵ-recoverability.

Proof: By Uhlmann's theorem $\exists\, |\tilde{\phi}^{RBE}\rangle$ purification of $\tilde{\phi}^R \otimes \tilde{\phi}^E$ such that:

$$F(\phi^{RE}, \tilde{\phi}^R \otimes \tilde{\phi}^E) = |\langle \phi^{RBE} | \tilde{\phi}^{RBE} \rangle|^2 \tag{21}$$

By the previous theorem, $|\tilde{\phi}^{RBE}\rangle$ is exactly recoverable. Moreover

$$\begin{aligned}
F(\mathcal{R}^{B\to\hat{B}}(\phi^{RB}), |\psi^{RA}\rangle) &= F(\mathcal{R}^{B\to\hat{B}}(\phi^{RB}), \mathcal{R}^{B\to\hat{B}}(\tilde{\phi}^{RB})) && (22)\\
&\geq F(\phi^{RB}, \tilde{\phi}^{RB}) && (23)\\
&\geq |\langle \phi^{RBE} | \tilde{\phi}^{RBE} \rangle|^2 && (24)\\
&= F(\phi^{RE}, \tilde{\phi}^R \otimes \tilde{\phi}^E) && (25)\\
&\geq (1 - \frac{1}{2}||\tilde{\phi}^{RE} - \tilde{\phi}^R \otimes \tilde{\phi}^E||_1)^2 && (26)\\
&\geq 1 - \epsilon. && (27)
\end{aligned}$$

Upper Bound on the Capacity

We want to show that

$$Q(\mathcal{N}) \leq \lim \frac{1}{n} \max_{A^n} I_c(R^n \rangle B^n)_\phi. \tag{28}$$

Sketch of the proof:

- Pick a sequence of codes and assume Q is achievable.
- Recall that it's enough to (approximately) send half of a maximally entangled state $|\Omega^{(n)}\rangle$ between R^n and a code subspace $\mathcal{C}_{A^n}^{(n)}$.

Coherent Information as an Achievable Rate

We want to show that, given some ρ^A with purification $|\psi^{RA}\rangle$, the coherent information is an achievable rate, i.e.

$$Q(\mathcal{N}) \geq I_c(R\rangle B)_\phi. \tag{29}$$

Key points in the proof:

- Decoupling inequality
- Random coding on typical subspaces

- We want to show that, discarding enough random subsystems from R, we get an almost maximally entangled state between A and what's left of R, with high probability.

- We want to show that, discarding enough random subsystems from R, we get an almost maximally entangled state between A and what's left of R, with high probability.
- Recall that the *Haar measure* is the only measure on the group of unitary matrices $D \times D$ such that

$$\mathbb{E}_W[\mathbb{1}] = 1 \tag{30}$$

$$\mathbb{E}_W[f(W)] = \mathbb{E}_W[f(W\tilde{W})] = \mathbb{E}_W[f(\tilde{W}W)] \tag{31}$$

for every fixed unitary $\tilde{W}$.

Decoupling inequality (I version)

Defined $\phi^{R_2 E}(W) := \mathrm{Tr}_{R_1}\left((W \otimes \mathbb{1})\phi^{RE}(W^\dagger \otimes \mathbb{1})\right)$ we have

$$\left(\mathbb{E}_W\left[\phi^{R_2 E}(W) - \frac{\mathbb{1}}{|R_2|} \otimes \phi^E\right]\right)^2 \leq \frac{|R_2||E|}{|R_1|}\mathrm{Tr}\left[(\phi^B)^2\right] \tag{32}$$

Decoupling inequality (I version)

Defined $\phi^{R_2E}(W) := \mathrm{Tr}_{R_1}\Big((W \otimes \mathbb{1})\phi^{RE}(W^\dagger \otimes \mathbb{1})\Big)$ we have

$$\left(\mathbb{E}_W\left[\phi^{R_2E}(W) - \frac{\mathbb{1}}{|R_2|} \otimes \phi^E\right]\right)^2 \leq \frac{|R_2||E|}{|R_1|}\,\mathrm{Tr}\left[(\phi^B)^2\right] \tag{32}$$

Decoupling inequality (II version)

Considering $W' := PW$ and renormalizing ϕ^{R_2E} afterwards we get

$$\left(\mathbb{E}_W\left[\phi^{R_2E}(W') - \frac{\mathbb{1}}{|R_2|} \otimes \phi^E\right]\right)^2 \leq |R_2||E|\,\mathrm{Tr}\left[(\phi^B)^2\right] \tag{33}$$

δ-Typicality

We define the δ-**typical subspace** $A_\delta \subseteq A^n$ as:

$$A_\delta := \operatorname{span}\left\{ |\bar{x}\rangle^{A^n} : \left| -\frac{1}{n} p(\bar{x}) - H(\rho^A) \right| \leq \delta \right\} \tag{34}$$

We define also the δ-**typical projector** Π_δ^A projecting A^n onto A_δ.

δ-Typicality

We define the δ-**typical subspace** $A_\delta \subseteq A^n$ as:

$$A_\delta := \text{span}\left\{ |\bar{x}\rangle^{A^n} : \left| -\frac{1}{n} p(\bar{x}) - H(\rho^A) \right| \leq \delta \right\} \tag{34}$$

We define also the δ-**typical projector** Π_δ^A projecting A^n onto A_δ.

- Project first $\{R^n, B^n, E^n\}$ onto δ-typical subspaces $\{R_\delta, B_\delta, E_\delta\}$

δ-Typicality

We define the δ-**typical subspace** $A_\delta \subseteq A^n$ as:

$$A_\delta := \text{span}\left\{ |\bar{x}\rangle^{A^n} : \left| -\frac{1}{n} p(\bar{x}) - H(\rho^A) \right| \leq \delta \right\} \tag{34}$$

We define also the δ-**typical projector** Π_δ^A projecting A^n onto A_δ.

- Project first $\{R^n, B^n, E^n\}$ onto δ-typical subspaces $\{R_\delta, B_\delta, E_\delta\}$
- Average with respect to random unitaries supported only inside R_δ

δ-Typicality

We define the δ-**typical subspace** $A_\delta \subseteq A^n$ as:

$$A_\delta := \text{span}\left\{ |\bar{x}\rangle^{A^n} : \left| -\frac{1}{n} p(\bar{x}) - H(\rho^A) \right| \leq \delta \right\} \qquad (34)$$

We define also the δ-**typical projector** Π_δ^A projecting A^n onto A_δ.

- Project first $\{R^n, B^n, E^n\}$ onto δ-typical subspaces $\{R_\delta, B_\delta, E_\delta\}$
- Average with respect to random unitaries supported only inside R_δ
- Project out some fixed subsystem $R_1 \subseteq R_\delta$, $R_\delta = R_1 R_2$, with $|R_2| = 2^{nQ}$ for some Q.

Lemma

Given $|\phi\rangle^{RBE}$, $\forall \delta > 0$ and sufficiently large n there exist δ-typical projectors $\Pi_\delta^{\{R,B,E\}}$ onto δ-typical subspaces $R_\delta \subseteq R^n$, $B_\delta \subseteq B^n$, $E_\delta \subseteq E^n$ such that

$$|\phi_\delta^{R^n B^n E^n}\rangle := (\Pi_\delta^R \otimes \Pi_\delta^B \otimes \Pi_\delta^E)\,|\phi^{R^n B^n E^n}\rangle \tag{35}$$

satisfies

$$|E_\delta| \leq 2^{nH(E)_\phi + n\delta} \tag{36}$$

$$\mathrm{Tr}\left[(\phi_\delta^{B_\delta})^2\right] \leq 2^{-nH(B)_\phi + n\delta} \tag{37}$$

$$||\phi^{R^n B^n E^n} - \phi_\delta^{R^n B^n E^n}||_1 \leq \epsilon \tag{38}$$

where $\epsilon = 2^{-nc\delta^2}$ for some c independent of n and δ.

Then by the decoupling inequality

$$\mathbb{E}_W\left(||\phi_\delta^{R_2E^n}(W') - \frac{\mathbb{1}}{|R_2|} \otimes \phi_\delta^{E^n}||_1\right) \le \sqrt{|R_2||E_\delta| \operatorname{Tr}\left[(\phi_\delta^{B_\delta})^2\right]} \tag{39}$$

$$\le \sqrt{2^{n(Q-H(B)+H(E)+3\delta}} \tag{40}$$

$$\le 2^{-n\delta} \le \epsilon \tag{41}$$

if $0 \le Q < H(B) - H(E) - 3\delta = I_c(R\rangle B)_\phi - 3\delta$.

$\Longrightarrow$ LSD Theorem is proved! :D

Outlook

- Strong converse
- Additivity for $Q_1(\mathcal{N})$
- Additivity for the capacity of *different* channels

Degradable Channels

Recall that given a channel $\mathcal{N}^{A\to B}$ with dilation $U_{\mathcal{N}}^{A\to BE}$, we can define the complementary channel $\widehat{\mathcal{N}}^{A\to E}$ by tracing out B instead of E. We say that $\mathcal{N}^{A\to B}$ is **degradable** if there exists a channel $\mathcal{T}^{B\to E}$ such that

$$\widehat{\mathcal{N}}^{A\to E} = \mathcal{T}^{B\to E} \circ \mathcal{N}^{A\to B}. \tag{42}$$

One can prove that in this case $Q_1(\mathcal{N}^{\otimes n}) \leq nQ_1(\mathcal{N})$ and get a single letter formula.

It has been proved that there exist an antidegradable channel $\mathcal{N}$ and a PPT channel $\mathcal{M}$ (both classes have 0 capacity) such that

$$Q(\mathcal{N} \otimes \mathcal{M}) > 0.1 \quad (!!!) \tag{43}$$

It has been proved that there exist an antidegradable channel $\mathcal{N}$ and a PPT channel $\mathcal{M}$ (both classes have 0 capacity) such that

$$Q(\mathcal{N} \otimes \mathcal{M}) > 0.1 \quad (!!!) \tag{43}$$

- Quantum capacity is not enough to characterize usefulness of a channel $\implies$ big problem in computing capacities!

It has been proved that there exist an antidegradable channel $\mathcal{N}$ and a PPT channel $\mathcal{M}$ (both classes have 0 capacity) such that

$$Q(\mathcal{N} \otimes \mathcal{M}) > 0.1 \quad \text{(!!!)} \tag{43}$$

- Quantum capacity is not enough to characterize usefulness of a channel $\implies$ big problem in computing capacities!
- We can combine apparently useless resources into something valuable.

Thanks for your attention!