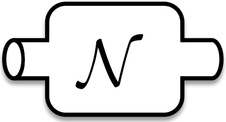
Unbounded number of channel uses are required to see quantum capacity

T. Cubitt, D. Elkouss, W. Matthews, M. Ozols, D. Pérez-García, S. Strelchuk

University of Cambridge, *Universidad Complutense de Madrid*

Motivation



1. Does $\mathcal{N}$ have capacity?
2. What is the capacity of $\mathcal{N}$?

Classical Channel

- Mutual information
- Single use of the channel

Quantum Channel

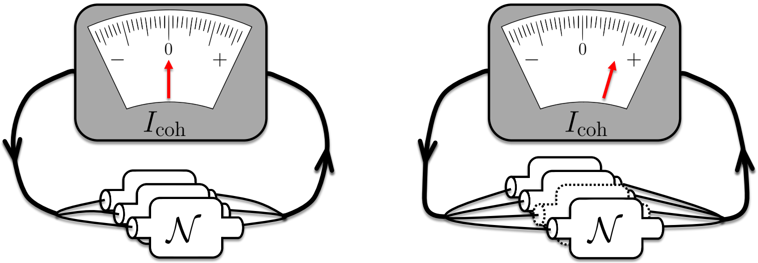
- Coherent information
- Unbounded number of channel uses

Do we need to consider an unbounded number of channel uses to detect quantum capacity?

Motivation

Main result

For any n, there exist a channel $\mathcal{N}$, for which the coherent information is zero for n copies of the channel, but has with positive capacity.



Outline

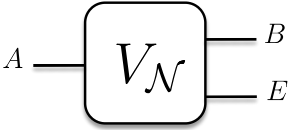
1. Introduction
2. Construction of $\mathcal{N}$ such that $Q^{(1)}(\mathcal{N}) = 0$ but $Q(\mathcal{N}) > 0$
3. Construction of $\mathcal{N}$ such that $Q^{(n)}(\mathcal{N}) = 0$ but $Q(\mathcal{N}) > 0$
4. Discussion

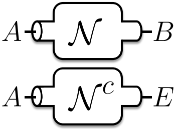
Outline

1. Introduction
2. Construction of $\mathcal{N}$ such that $Q^{(1)}(\mathcal{N}) = 0$ but $Q(\mathcal{N}) > 0$
3. Construction of $\mathcal{N}$ such that $Q^{(n)}(\mathcal{N}) = 0$ but $Q(\mathcal{N}) > 0$
4. Discussion

Quantum Channels 101

Isometric representation

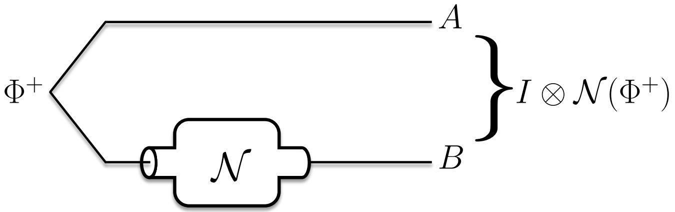




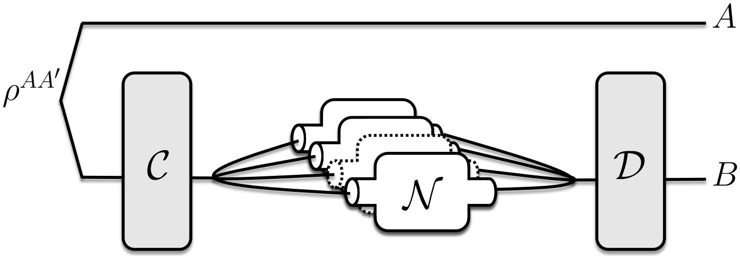
$$\mathcal{N}(\rho) = tr_E(V\rho V^\dagger)$$

$$\mathcal{N}^c(\rho) = tr_B(V\rho V^\dagger)$$

Channel-state duality



Quantum Communications



Definition

The capacity is the maximum rate at which arbitrarily faithful communication is possible.

Quantum Capacity

- Coherent information (Nielsen-Schumacher '96):

$$I_{coh}(\mathcal{N}, \rho) = H(\mathcal{N}(\rho)) - H(\mathcal{N}_c(\rho))$$

- Coherent information after n-uses of a channel:

$$Q^{(n)}(\mathcal{N}) = \frac{1}{n} \max_{\rho} I_{coh}(\mathcal{N}^{\otimes n}, \rho)$$

- **Quantum capacity of a channel**
(Lloyd '97, Shor '02, Devetak '05) :

$$Q(\mathcal{N}) = \lim_{n\to\infty} Q^{(n)}(\mathcal{N})$$

- Superadditivity of the coherent information
(DiVincenzo-Shor-Smolin '98):

$$Q(\mathcal{N}) > Q^{(1)}(\mathcal{N}) = 0$$

Other capacities

- Classical capacity (Hastings '09):

$$C(\mathcal{N}) > C^{(1)}(\mathcal{N})$$

- Private capacity (Smith-Renes-Smolin '08):

$$P(\mathcal{N}) > P^{(1)}(\mathcal{N})$$

- Classical zero-error capacity of a classical channel (Shannon '56):

$$C_0(\mathcal{N}) > C_0^{(1)}(\mathcal{N})$$

- Quantum zero-error capacity of a quantum channel (Shirokov '14):

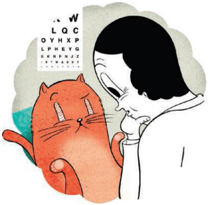
$$\forall n \exists \mathcal{N}; Q_0^{(n)}(\mathcal{N}) = 0, Q_0(\mathcal{N}) > 0$$

Outline

Superactivation

Theorem (Smith-Yard '08)

There exist two zero-capacity channels $\mathcal{E}_{1/2}, \Gamma$ s.t. $Q(\mathcal{E}_{1/2} \otimes \Gamma) > 0$.



'You appear to be blind in your left eye and blind in your right eye. Why you can see with both eyes is beyond me…" (Oppenheim '08)

Component channels

Erasure channel

$$\mathcal{E}_p(\rho^A) := (1-p)\rho^B + p|e\rangle\langle e|^B$$

if $p \geqslant 1/2$ $Q(\mathcal{E}_p) = 0$ $\left(\exists D; D \circ \mathcal{E}_p^c = \mathcal{E}_p\right)$.

$\mathcal{E}_{1/2}$ is an erasure channel with $p = 1/2$.

PPT channel

If the CJ of $\mathcal{N}$ has PPT then $Q(\mathcal{N}) = 0$
(P. Horodecki-M. Horodecki-R. Horodecki ′00).

Γ is a PPT channel with CJ close to a pbit.

Pbits

Definition

A bipartite **key** ab: $\phi^{\mathsf{ab}} = |\phi\rangle\langle\phi|^{\mathsf{ab}}$, $|\phi\rangle^{\mathsf{ab}} := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)^{\mathsf{ab}}$;
A **shield** AB ($\dim \mathsf{A} = \dim \mathsf{B}$) and state σ^{AB};
A **pbit** is a state of the form

$$\gamma^{\mathsf{abAB}} := U\left(\phi^{\mathsf{ab}} \otimes \sigma^{\mathsf{AB}}\right) U^{\dagger}$$

U is a *global* unitary of the form: $\sum_{i,j=0}^{1} |i\rangle\langle i|^{\mathsf{a}} \otimes |j\rangle\langle j|^{\mathsf{b}} \otimes U_{ij}^{\mathsf{AB}}$.

Properties

If we trace AB and Bob dephases locally: $\gamma^{\mathsf{ab}} = \frac{1}{2}\sum_{i=0}^{1} |ii\rangle\langle ii|_{\mathsf{ab}}$.
If Bob gets A he can "untwist" with a *local* unitary: ab become maximally entangled.

Plan: Γ distributes pbits, $\mathcal{E}_{1/2}$ is used to transmit the shield.

Approximate pbits

Theorem
(K. Horodecki-M. Horodecki-P. Horodecki-Oppenheim '09)

There exist PPT states arbitrarily close to a perfect pbit.

Beginning with:

$$\rho^{\mathsf{abAB}} = \frac{1}{2}\left(|\phi^+\rangle\langle\phi^+|^{\mathsf{ab}} \otimes \sigma^{+\,\mathsf{AB}} + |\phi^-\rangle\langle\phi^-|^{\mathsf{ab}} \otimes \sigma^{-\,\mathsf{AB}}\right)$$

obtain some $\tilde{\gamma}^{\mathsf{abAB}}$:

- Is PPT.
- Is ϵ-*close to* a perfect pbit.

Remark
The channel Γ with $\tilde{\gamma}^{\mathsf{abAB}}$ as CJ has zero capacity.

Proof of Smith-Yard

Protocol

- Send one half of the maximally entangled state through Γ.
- *Now Alice and Bob share a pbit (up to ϵ).*
- Alice sends her part of the shield through $\mathcal{E}_{1/2}$.

Evaluate for pbit, by continuity the result holds up to $f(\epsilon)$.

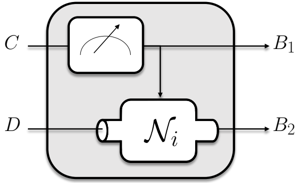
Coherent information

- With probability $\frac{1}{2}$, Bob gets the shield and he can untwist the pbit.
- With probability $\frac{1}{2}$, the channel erases (they are left with $\tilde{\gamma}_{\mathsf{ab}}$).
- This yields

$$Q^{(1)}(\mathcal{E}_{1/2} \otimes \Gamma) \geqslant \frac{1}{2} - f(\epsilon)$$

Switch channels

Direct sum channels (Fukuda-Wolf '07)



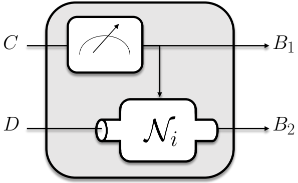
- The control input is measured in the computational basis
- The output of the measurement "chooses" the channel applied to the data input

Lemma (Fukuda-Wolf '07)

$$Q^{(1)}\left(\sum_i P_i \otimes \mathcal{N}_i\right) = \max_i Q^{(1)}(\mathcal{N}_i)$$

Corollary: $\mathcal{N}$ such that $Q^{(1)}(\mathcal{N}) = 0, Q(\mathcal{N}) > 0$

Channel $\mathcal{N}$



- Take $\mathcal{N}_1$ as the PPT channel with CJ state arbitrarily close to a pbit (Γ)
- Take $\mathcal{N}_2 = \mathcal{E}_{1/2}$

Proof

- Maximize coherent information of component channels.
- Clearly $Q^{(1)}(\mathcal{N}) = 0$.
- By taking $\mathcal{N} \otimes \mathcal{N}$ we have access to $\Gamma \otimes \mathcal{E}_{1/2}$. Hence $Q^{(2)}(\mathcal{N}) > 0$.

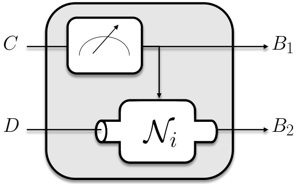
Outline

Plan

Use a switch with two component channels one can share a PPT pbit the other an erasure channel to send the shield.

- "Converse": $Q^{(n)} = 0$
  - Make pbit creation *unreliable* ($\Pr(\text{fail}) = \kappa$).
  - Boost the erasure probability of the erasure channel.
- "Achievable": $Q > 0$, via $Q^{(t+1)} > 0$ for some $t + 1 > n$:
  - Make the shield with t parts so that giving Bob any part of Alice's shield unlocks the entanglement in the key.
  - With the first use of channel (try to) establish this pbit between Alice and Bob. Send t pieces of the shield over t erasure channel uses.
  - Probability that at least one piece gets through: $1 - p^t$.

Channel



- Take $\mathcal{N}_1 = \mathcal{E}_p$
- Take $\mathcal{N}_2$ as a noisy PPT-pbit channel ($\tilde{\Gamma}_\kappa$)

where

$$\tilde{\Gamma}_\kappa := (1-\kappa)\Gamma + \kappa|e\rangle\langle e|$$

Requirement: even if we trace out all but one of the subsystems of the shield the reduced state should be close to a pbit. Proof similar to
(K. Horodecki-M. Horodecki-P. Horodecki-Oppenheim '09).

"Converse"

Lemma (Converse)

If $\kappa \in (0,1]$, *for* p *large enough* $Q^{(n)}(\mathcal{N}) = 0$.

Proof.

Restrict to $Q^{(1)}(\mathcal{N}_i)$. Let $I_l := I_{coh}\left(\tilde{\Gamma}_\kappa^{\otimes l} \otimes \mathcal{E}_p^{\otimes (n-l)}, \rho\right)$

$$\begin{aligned} I_l \leqslant & \kappa^l p^{n-l}(-S(\rho_l)) && \text{(all erase)} \\ & +(1-\kappa^l)p^{n-l} I_{coh}(\Gamma^{\otimes l} \otimes \mathcal{E}_1^{\otimes n-l}, \rho_l) && \text{(all } \mathcal{E}_p \text{ erase)} \\ & +(1-p^{n-l})S(\rho_l) && \text{(other cases)} \end{aligned}$$

$$I_l \leqslant (-\kappa^l p^{n-l} + 1 - p^{n-l})S(\rho_l) \leqslant (1-(1+\kappa^n)p^n)S(\rho_l),$$

We find that $I_l \leqslant 0$ if $p \geqslant (1+\kappa^n)^{-1/n}$.

$\square$

"Achievability"

Lemma (Achievability)

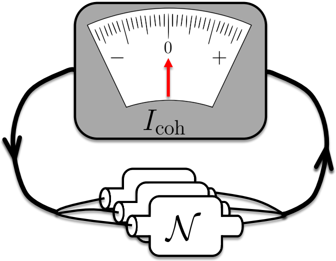
For $p \in (0,1)$, $\kappa \in (0,1/2)$, there exists a channel $\mathcal{N}$ and $t \in \mathbb{N}$ such that $Q^{(t+1)}(\mathcal{N}) > 0$.

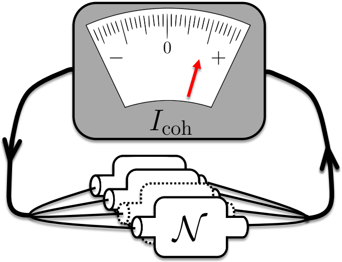
Protocol: Choose $\tilde{\Gamma}_\kappa$ for 1st use and (try) create pbit, choose $\mathcal{E}_p$ for uses $2 \ldots t+1$ and send Alice's t parts of the shield.

$$
\begin{aligned}
(t+1)Q^{(t+1)}(\mathcal{N}) \geqslant\ & I_{coh}(\tilde{\Gamma} \otimes \mathcal{E}_p^{\otimes t}, \rho) \\
\geqslant\ & \kappa I_{coh}(\mathcal{E}_1 \otimes \mathcal{E}_p^{\otimes t}, \rho) && \text{(no pbit)} \\
& + (1-\kappa) p^t I_{coh}(\Gamma \otimes \mathcal{E}_1^t, \rho) && \text{(got a pbit but no shield)} \\
& + (1-\kappa)(1-p^t) I_{coh}(\Gamma \otimes I \otimes \mathcal{E}_1^{t-1}, \rho) && \text{(got a pbit + shield)} \\
\geqslant\ & (1-\kappa)(1-p^t - f(\epsilon)) - \kappa
\end{aligned}
$$

$\forall n, \exists \mathcal{N}$ such that $Q^{(n)}(\mathcal{N}) = 0$ but $Q(\mathcal{N}) > 0$

- Given n, choose $\kappa = 1/3$ and $p = (1 + \kappa^n)^{-1/n}$ to comply with "Converse"
- Since κ, p are in the range of "Achievability" we can construct $\mathcal{N}$.





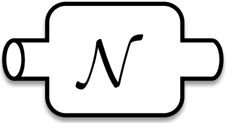
Outline

Discussion

Open questions

- ($t \gg n$) Identify m such that $Q^{(m)}(\mathcal{N}) = 0$ but $Q^{(m+1)}(\mathcal{N}) > 0$
- Same result with constant dimension?

Summary



1. Does $\mathcal{N}$ have capacity?
2. What is the capacity of $\mathcal{N}$?