Capacité Zéro-erreur quantique

Journées Codage et Cryptographie - 20 mars 2008 - Carcans, France

Rex A. C. Medeiros[1,2], Romain Alléaume[2], Hugues Randriam[2], Gérard Cohen[2], Francisco M. de Assis[1]

[1] Universidade Federal de Campina Grande

[2] Ecole Nationale Supérieure des Télécommunications

Outline

Outline

Motivation and Contributions

Motivation

- Generalize the notion of zero-error capacity (previously only defined for classical channels) to quantum channels.
- Find whether this “more general” problem, can help to shed new light on the theory of zero-error capacity, and on connex topics (combinatorics, graph theory).

Contributions

- A formal definition of a zero-error capacity and zero-error codes for quantum channels has been proposed.
- We have exhibited examples indicating that QZEC is not a trivial generalization of the classical problem.
- We have partially characterized the quantum states and the measurements attaining the QZEC

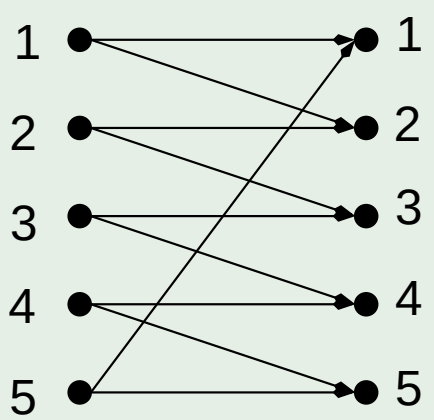
Outline

"Ordinary" Capacity of a classical channel

Shannon ordinary capacity of Discrete Memoryless Channel

DMC capacity: $C = \max_{p(x)} I(X;Y)$
For all rates $R < C$, by Shannon noisy coding theorem, one can find a code of length n presenting an asymptotically small but **non − vanishing** probability of error after decoding
$P_e \to 0$ when $n \to \infty$

Example (A DMC)



Example (Ordinary capaciy)

Assuming Prob $[i|i] =$ Prob $[i+1 \bmod 5|i] = \frac{1}{2}$

$$\begin{aligned} C &= \max_{p(x)} I(X;Y) \\ &= \max_{p(x)} H(X) - H(X|Y) \\ &= \log 5 - \log 2 \\ &\approx 1.32 \end{aligned}$$

Classical zero-error capacity

Definition:

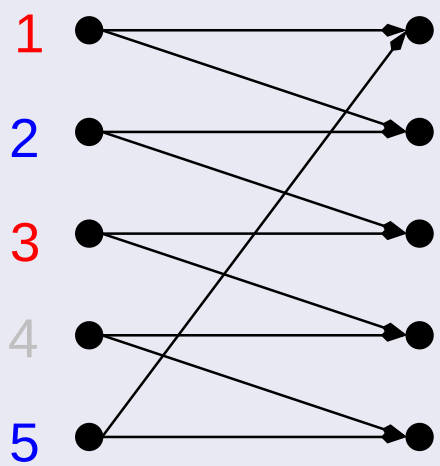
The zero-error capacity of a discrete memoryless channel $(\mathcal{X}, p(y|x), \mathcal{Y})$ is given by

$$C_0 = \limsup_{n\to\infty} \frac{1}{n} \log N(n), \tag{1}$$

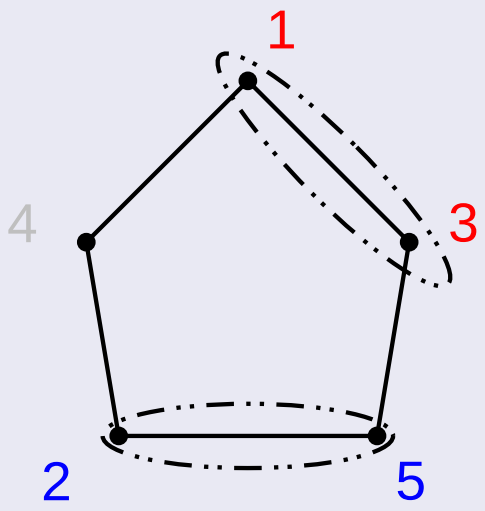
Where N(n) is the maximum number of $n-$ length messages that the system can transmit **without error**.

Relation with graph theory

Adjacency Graph of a channel



Characteristic graph



Notion of adjacency

Two input symbols and said to be adjacent with respect to the channel, iff they cannot be distinguished with certainty at the channel output, i.e. if there is a non-zero probability that the output of the channel is the same, for those two input state.

Zero-error'Capacity of a Discrete Memoryless Channels- Example

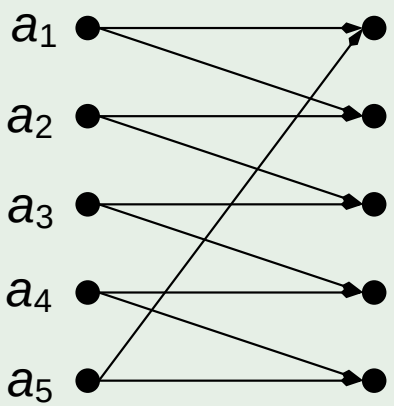
Definition of the ZEC, based on the characteristic graph

$$C_0 = \sup_n \frac{1}{n} \log \omega(G^n),$$

where G^n is the $n-$product of G and $\omega(G^n)$ stands for the clique number of G^n (clique number of a graph = cardinal of the largest completely connected subgraph of this graph).

Example

A DMC



Example

Zero-error code

$$\begin{aligned} a_1a_1 &\rightarrow \{a_1a_1, a_1a_2, a_2a_1, a_2a_2\} \\ a_2a_3 &\rightarrow \{a_2a_3, a_3a_3, a_2a_4, a_3a_4\} \\ a_3a_5 &\rightarrow \{a_3a_5, a_4a_5, a_3a_1, a_4a_1\} \\ a_4a_2 &\rightarrow \{a_4a_2, a_5a_2, a_4a_3, a_5a_3\} \\ a_5a_4 &\rightarrow \{a_5a_4, a_1a_4, a_5a_5, a_1a_5\} \end{aligned}$$

$R_{ze} = \frac{1}{2} \log 5 \approx 1.161 \qquad C = \log 5/2 \approx 1.322$

Classical Zero-error capacity

Some aspects of the zero-error capacity

- Finding the ZEC is a combinatorial problem
  - Indeed, it is a NP-Complete problem.
- The ZE-IT found application in areas like
  - Combinatorics
    - Functional and methods
    - Impact on graph theory
    - According to Claude Berge, Shannon's paper led him to introduce the class of perfect graphs

$$\omega(G) = \chi(G)$$

  - Computer science
    - Communication complexity

Outline

Classical and Quantum Information Theory

Classical versus quantum information theory

Classical Information Th.	Quantum Information Th.
Symbols a_i	Quantum states ρ_i
Input alphabet $\{a_1, \ldots, a_I\}$	Input quantum states $\{\rho_1, \ldots, \rho_I\}$
Codeword $\in \{a_1, \ldots, a_I\}^n$	Quantum codeword $\in \{\rho_1, \ldots, \rho_I\}^{\otimes n}$
DMC channel $[p(y\|x)]$ Stochastic matrix	Quantum channel $\mathcal{E}(\rho)$ Positive trace-preserving map
Shannon entropy $H(\mathbf{X})$	von Neumann $S(\rho) = -\mathrm{tr}\,[\rho \log \rho]$
Shannon capacity	Holevo capacity, Adaptive capacity Entanglement-assisted capacity
Decoding	POVM Measurements + decoding

Quantum states and measurements

Pure states

(normalized vector) $|\psi\rangle \in \mathcal{H}_d$

$\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \Rightarrow$ basis $\mathcal{H}_d$

$$|0\rangle \equiv \begin{bmatrix} 1 & 0 & \ldots & 0 \end{bmatrix}^T$$

$$|d-1\rangle \equiv \begin{bmatrix} 0 & 0 & \ldots & 1 \end{bmatrix}^T$$

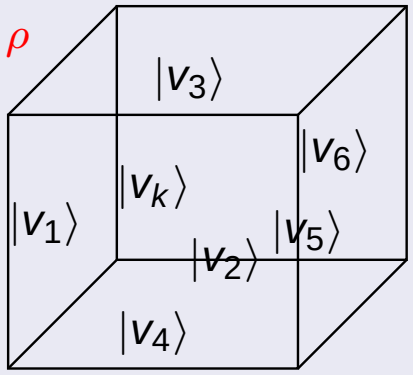
$$|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Mixed states

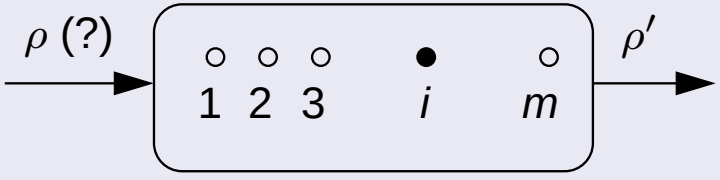
The system may be in $|v_i\rangle$ with probability p_i

Density matrix

$$\rho = \sum_{i=1}^{k} p_i |v_i\rangle\langle v_i|$$



POVM Measurements



POVM Apparatus

POVM $\mathcal{P} = \{M_1, \ldots, M_m\}$; $\sum_i M_i = \mathbb{1}$

$Prob[\text{get output } i] = \text{tr}\,[\rho M_i]$

von Neumann: $M_i \Rightarrow$ projectors

Quantum channels

Quantum channel model

Mathematically represented by a positive trace-preserving map:

$$\mathcal{E}(\rho) = \sum_a E_a \rho E_a^\dagger,$$

where $\sum_a E_a^\dagger E_a = \mathbb{1}$.

Example

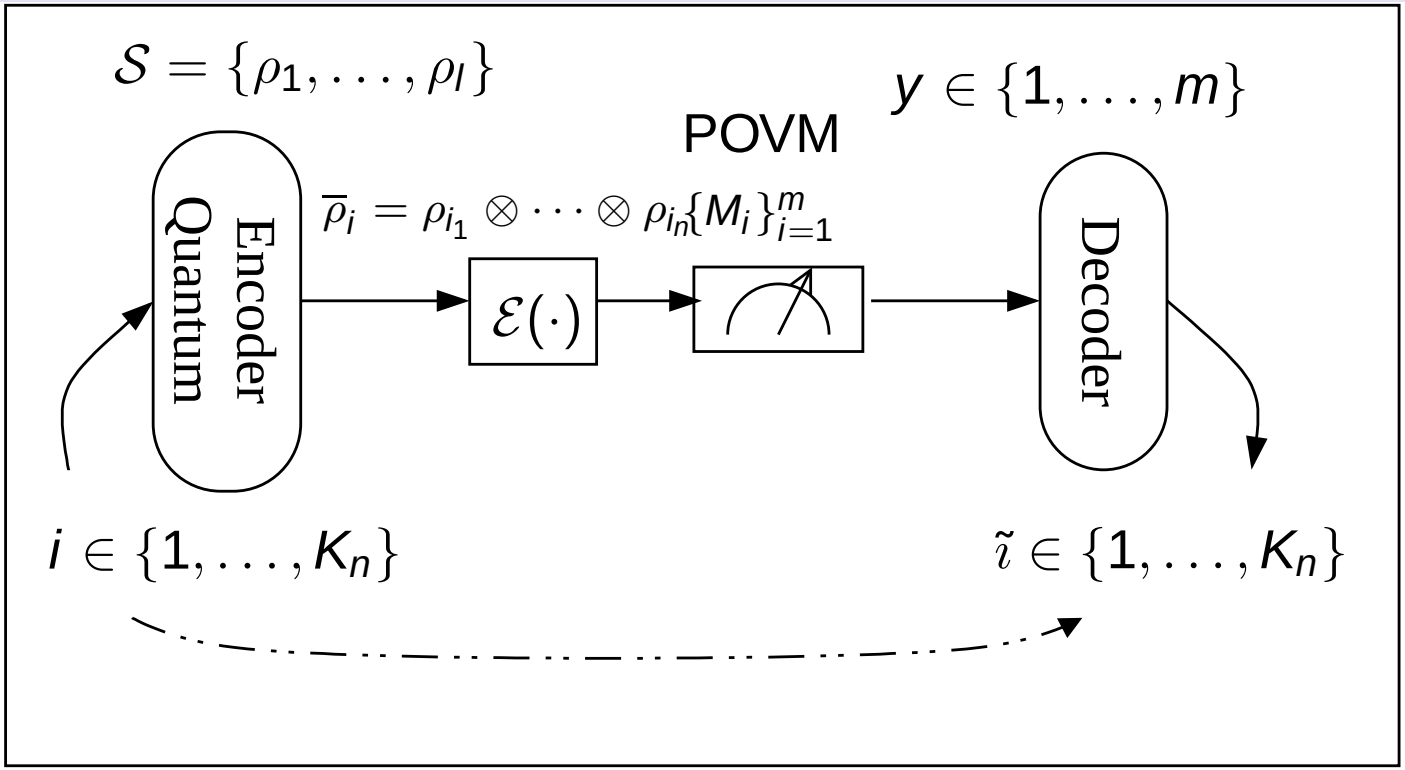
Amplitude damping channel (energy dissipation)

$$\mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger,$$

where $E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$ and $E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$.

Outline

Zero-error quantum communication system



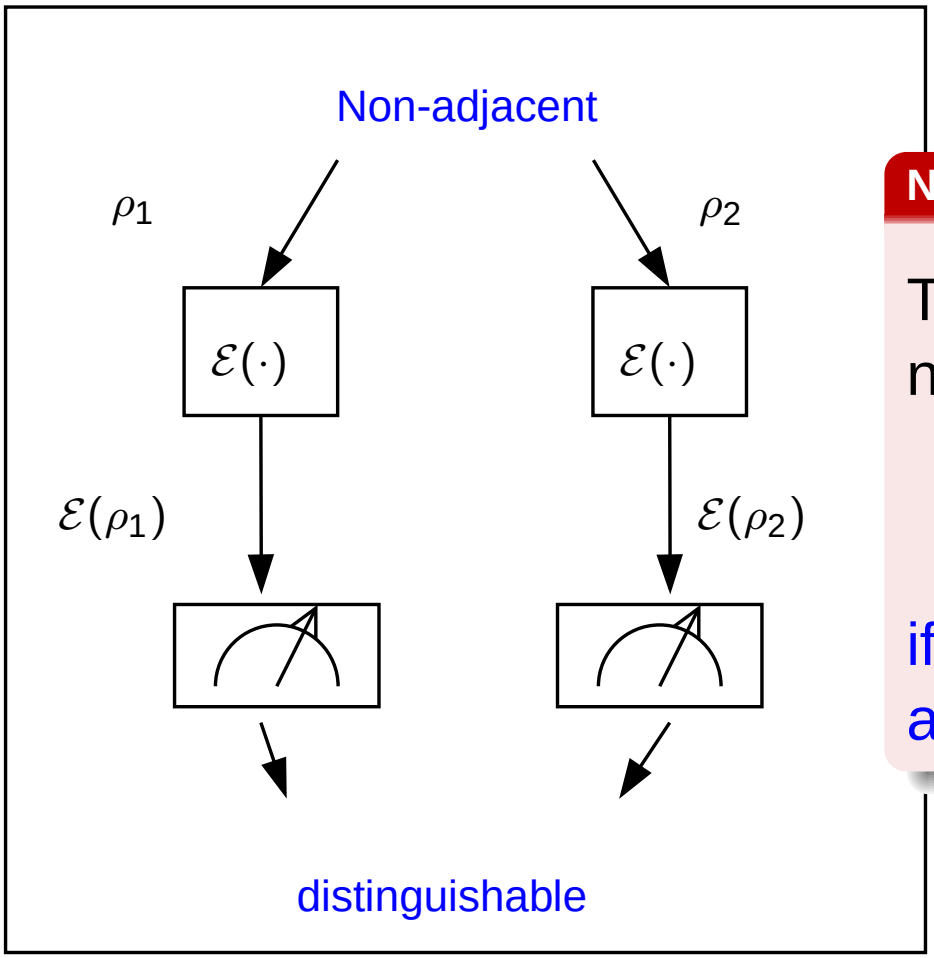
Definition

The zero-error capacity of a noisy quantum channel is

$$C^{(0)}(\mathcal{E}) = \sup_n \frac{1}{n} \log K_n, \qquad \text{(with } P_e = 0\text{)}$$

where K_n stands for the maximum number of classical messages that the system can transmit without error, when a quantum block code of length n is used.

Adjacency of input symbols in the quantum context



Non-adjacent input states

Two quantum states ρ_1 and ρ_2 are non-adjacent

$$\mathcal{E}(\rho_1) \perp \mathcal{E}(\rho_2) \qquad \rho_1 \perp_{\mathcal{E}} \rho_2$$

if they are completely distinguishable at the channel output.

Relation with graph theory

Set-up

Given a quantum channel $\mathcal{E}$ and a subset $\mathcal{S}$, we can construct a characteristic graph $\mathcal{G}$ as follows:

- Take as many vertices as $|\mathcal{S}|$
- Connect two vertices if the corresponding quantum states are non-adjacent with respect to $\mathcal{E}$

QZEC: freedom in the choice of the set $\mathcal{S}$

- Let $\mathcal{S} = \{\rho_1, \ldots, \rho_l\}$ be a set of input states,

$$\begin{aligned} V(\mathcal{G}) &= \{1, \ldots, l\}, \\ E(\mathcal{G}) &= \{(i,j); \rho_i \perp_{\mathcal{E}} \rho_j;\ \rho_i, \rho_j \in \mathcal{S}; i \neq j\}. \end{aligned}$$

For a given quantum channel, there is an infinity of possible sets $\mathcal{S}$, the sets $\mathcal{S}$ for which the QZEC is reached are said to be optimum.

Graph-based definition of the QZEC

Equivalent definition

The zero-error capacity of a quantum channel is given by

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_{n} \frac{1}{n} \log \omega\left(\mathcal{G}^n\right),$$

The supremum is attained for the optimum $\mathcal{S}$.

Note that:

For an optimum $\mathcal{S}$ and n attaining the capacity:

1. $K_n = \omega(\mathcal{G}^n)$
2. Codebook: sequences indexed by the vertex of the largest clique in $\mathcal{G}^n$

Outline

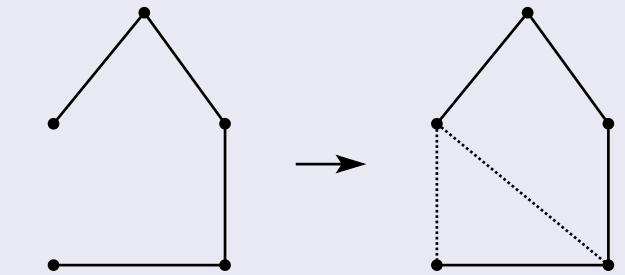
Pure states reach the capacity

Input quantum states

- In principle, the set $\mathcal{S}$ of the optimum $(\mathcal{S}, \mathcal{P})$ may contain both pure and mixed states
- We demonstrated that $C_0(\mathcal{E})$ can be reached using only pure states

Proof Sketch:

- Suppose an optimum $\mathcal{S} = \{\rho_1, \ldots, \rho_l\}$ containing mixed states giving rise to $\mathcal{G}$
- We show that $\mathcal{S}' = \{|v_i\rangle, \ldots, |v_l\rangle\}$, where $|v_i\rangle \in$ supp ρ_i, is also optimum:
  - $\mathcal{G}'$ is obtained from $\mathcal{G}$ by probably adding edges
  - Adding edges never decreases the clique number



Example of $\mathcal{G}$ Example of $\mathcal{G}'$

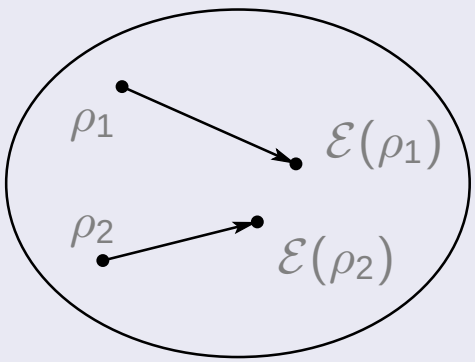
Non-adjacent states are necessarily orthogonal

Distinguishable states at channel output have orthogonal supports

Beigi, Shor quant-ph 07092090

ρ_i is non-adjacent to ρ_j, iff $Tr(\mathcal{E}(\rho_i)\,\mathcal{E}(\rho_j)) = 0$

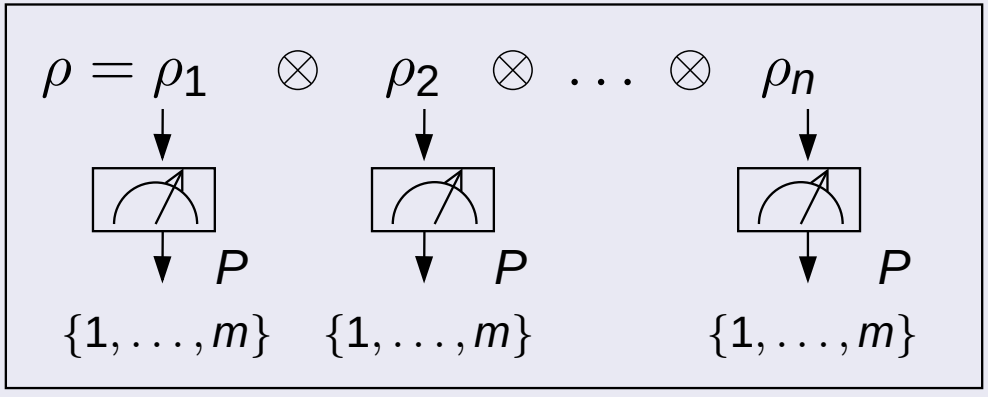
AND : Quantum Channels are contractive



$\Rightarrow$ Non-adjacent states, $\rho_i \perp_{\mathcal{E}} \rho_j$ have orthogonal support at channel input, $Tr(\rho_i\,\rho_j) = 0$

Individual or collective measurements needed ?

Individual measurements



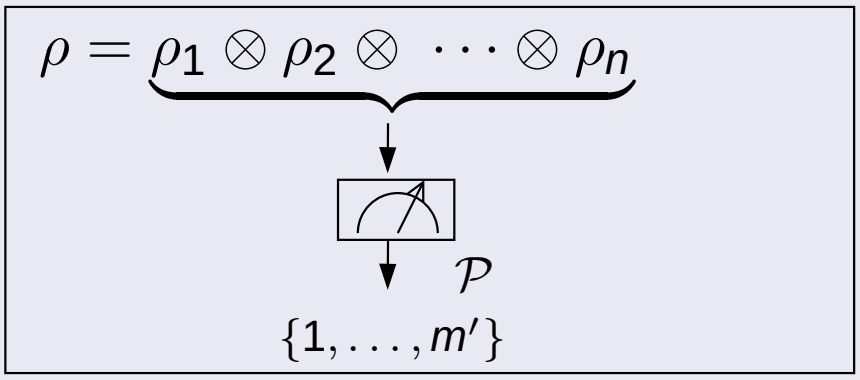
$$\rho_i \in \mathcal{H}_d$$

$$P = \{M_1, \ldots, M_m\}$$

M_i are $d \times d$ matrices

$$y \in \{1, \ldots, m\}^n$$

Collective measurements



$$\rho_i \in \mathcal{H}_d$$

$$\mathcal{P} = \{M_1, \ldots, M_{m'}\}$$

M_i are $d^n \times d^n$ matrices

$$y \in \{1, \ldots, m'\}$$

Measurements reaching the capacity

Projective measurements

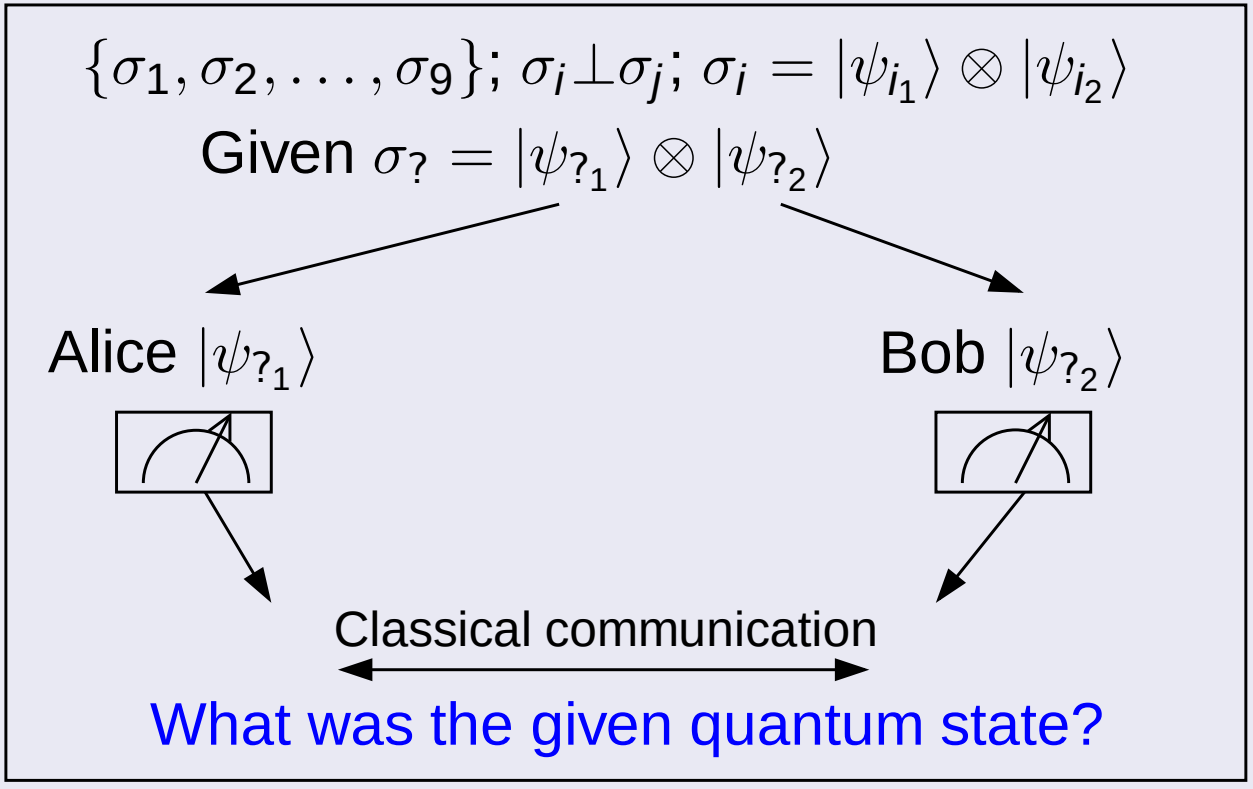
- Because non-adjacent states have orthogonal supports at the channel output, collective projective measurements are sufficient

$$\begin{aligned}
\mathcal{E}(\overline{\rho}_1) &= \underbrace{\mathcal{E}(\rho_{1_1}) \otimes \mathcal{E}(\rho_{1_2}) \otimes \cdots \otimes \mathcal{E}(\rho_{1_n})}_{P_1} \\
\mathcal{E}(\overline{\rho}_2) &= \underbrace{\mathcal{E}(\rho_{2_1}) \otimes \mathcal{E}(\rho_{2_2}) \otimes \cdots \otimes \mathcal{E}(\rho_{2_n})}_{P_2} \\
&\vdots \qquad\quad \vdots \\
\mathcal{E}(\overline{\rho}_{K_n}) &= \underbrace{\mathcal{E}(\rho_{K_{n_1}}) \otimes \mathcal{E}(\rho_{K_{n_2}}) \otimes \cdots \otimes \mathcal{E}(\rho_{K_{n_n}})}_{P_{K_n}}
\end{aligned}$$

- $\mathcal{P} = \{P_1, P_2, \ldots, P_{K_n}, P_{K_{n+1}}\}$, where $P_{K_{n+1}} = \mathbb{1} - \sum_{i=1}^{K_n} P_i$.
- Are collective measurements necessary?

Collective measurement are necessary

Distinguishing quantum states



- In the general case, collective measurements are necessary to distinguish orthogonal tensor product states (Bennett et. al.)

Is the QZEC a trivial generalization of the Shannon ZEC?

What could be definitions of "trivial" ?

- (1) The characteristic graph of $\mathcal{E}$, induced by S is either completely connected or completely disconnected.
- (2) The QZEC is achieved using "trivial" codes of length one.
- (3) QZEC problem reduces to the ZEC problem (in particular, QZEC reached for orthogonal input states).

Example (Trivial examples)

- Qubit channels have $C^{(0)}(\mathcal{E}) = 0$ or $C^{(0)}(\mathcal{E}) = 1$
  - bit flip channel, phase flip, ...
- The depolarizing channel in a $d-$dimensional Hilbert space,

$$\mathcal{E}(\rho) = p\rho + (1-p)\mathbb{1},$$

has $C^{(0)}(\mathcal{E}) = 0$

There are quantum channels with non-trivial graphs

Example (Finding a quantum channel giving rise to the pentagon as characteristic graph)

Consider the quantum channel $\mathcal{E} \equiv \{E_1, E_2, E_3\}$ in $\mathcal{H}_5$ where

$$E_1 = \begin{bmatrix} 0.5 & 0 & 0 & 0 & 0.04 \\ 0.5 & 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & -0.12 & 0.12 \\ 0 & 0 & 0 & 0.7 & 0.5 \end{bmatrix} \quad E2 = \begin{bmatrix} 0.5 & 0 & 0 & 0 & -0.04 \\ 0.5 & -0.5 & 0 & 0 & 0 \\ 0 & 0.5 & -0.5 & 0 & 0 \\ 0 & 0 & 0.5 & 0.12 & -0.12 \\ 0 & 0 & 0 & 0.7 & -0.4 \end{bmatrix}$$

$$E3 = 0.72|4\rangle\langle 4|$$

One can verify that

$$\sum_{i=1}^{3} E_i E_i^{\dagger} = \mathbb{1}$$

Let $\{|0\rangle, \ldots, |4\rangle\}$ be the computational basis of $\mathcal{H}_5$. Consider the subset

$$\mathcal{S} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |v_{34}\rangle\}, |v_{34}\rangle = \frac{|3\rangle + |4\rangle}{\sqrt{2}}$$

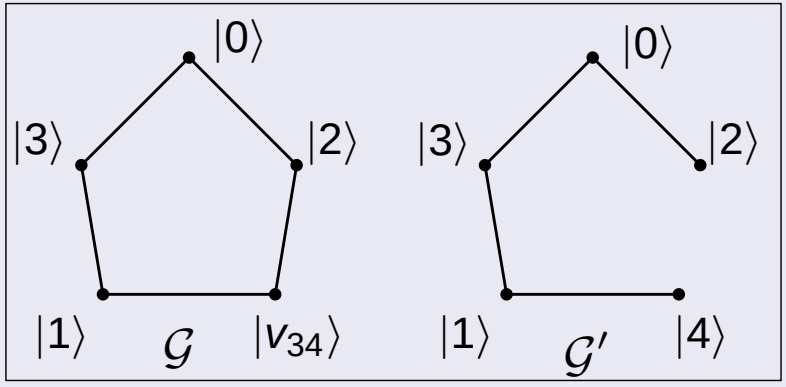
Optimum $\mathcal{S}$ may not be an orthogonal set

As illustrated by our pentagon example

Adjacency relation are:

$$|0\rangle \perp_{\mathcal{E}} |2\rangle, \quad |0\rangle \perp_{\mathcal{E}} |3\rangle, \quad |1\rangle \perp_{\mathcal{E}} |3\rangle, \quad |1\rangle \perp_{\mathcal{E}} |v_{34}\rangle, \quad |2\rangle \perp_{\mathcal{E}} |v_{34}\rangle,$$

giving rise to the pentagon as characteristic graph:



- Suppose we take

$$\mathcal{S}' = \{|0\rangle, \ldots, |4\rangle\}.$$

The characteristic graph $\mathcal{G}'$ has Shannon capacity $C_0 = 1$ bits/use.

- We conjecture that the zero-error capacity is reached by $\mathcal{S}$

$$C^{(0)}(\mathcal{E}) = \frac{1}{2} \log 5 \textit{ bits per use}.$$

What can we say about sets S of orthogonal states ?

What happens under unitary transformations ?

For $\mathcal{E}$ fixed, is the QZEC conserved when one applies a unitary transform U to S ? (*)

Surprise ?

The answer to (*) is **NO** !

Counter Example :

$\mathcal{E} : \rho \rightarrow p\rho + (1-p)\rho X \rho X$

$S = \{|0\rangle, |1\rangle\} \Rightarrow QZEC(S, \mathcal{E}) = 0$ unless p=0 or p=1.

$S' = HS = \{|0\rangle + |1\rangle/\sqrt{2}, \{|0\rangle - |1\rangle/\sqrt{2}\} \Rightarrow QZEC(S, \mathcal{E}) = 1$

Outline

Summary

Summary of our contributions

- We have proposed a new kind of capacity to quantum channels:
  - We generalized the classical zero-error capacity to include quantum channels
- We formally defined an error-free quantum code
- Necessary and sufficient condition to $C^{(0)} > 0$
- We developed an graph theoretic approach to the problem of finding the quantum ZEC.

Summary

Summary of our contributions

- We studied quantum states and measurements reaching the QZEC:
  - The capacity can always be reached using an ensemble of pure states
  - Collective von Neumann measurements are required to attain the QZEC
    - The QZEC with individual measurements is less than or equal to $C^{(0)}$.
- We have exhibited some examples of channels whose QZEC is claimed to be non-trivial:
  - It is reached using non-orthogonal quantum states
  - Quantum codes of length $n > 1$
- The QZEC is upper bounded by the HSW capacity

References

- R. A. C. Medeiros and F. M. de Assis, Quantum Zero-error capacity *Int. J. Quant. Inf.*, 3(1):135–139, 2005.
- R. A. C. Medeiros and F. M. de Assis, Quantum Zero-error capacity and HSW capacity, *in Proc. QCMC'04*, 734, p52-54, 2004.
- R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis. Quantum States Characterization of the zero-error capacity, *quant-ph/0611042.*
- S. Beigi, P. Shor, On the Complexity of Computing Zero-error and Holevo Capacity of Quantum Channels, *quant-ph/07092090*, 2007.
- R. A. C. Medeiros, R. Alléaume, H. Randriam, G. Cohen, and F. M. de Assis. *In preparation* (on C-Q channels in particular)

Perspectives

Perspectives - non-exhaustive list

- Find an upper bound of the QZEC, based on properties of the quantum channel itself.
- Investigate whether new or alternative derivations of ZEC computation, for some graphs (in particular for the pentagon) are possible.
- Link with the theory of decoherence free subspaces and noiseless subsystems.

Thank you!