Positivity, Discontinuity and Finite Resources for Arbitrarily Varying Quantum Channels

Holger Boche,
(TU München, Germany)
joint work with Janis Nötzel

JWCC 2014
Barcelona

Topics (all with respect to AVQCs:)

1. CLASSICAL MESSAGE TRANSMISSION (CONTINUITY)
2. ENTANGLEMENT TRANSMISSION
3. STRONG SUBSPACE TRANSMISSION

Things you can do with a quantum channel

Let **n** be a quantum channel with input system S and an outputsystem R for some legitimate receiver.

The channel can be used to transmit particles carrying information.

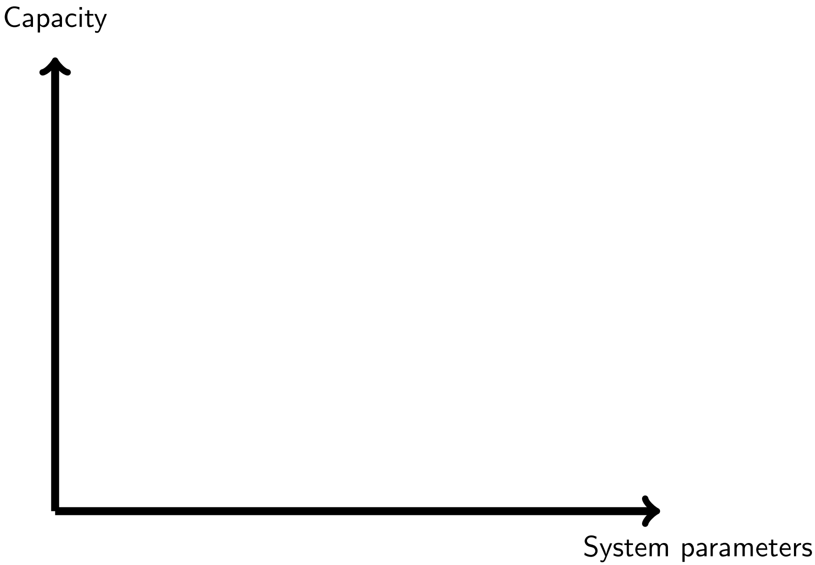
Different tasks can be carried out, leading to different mathematical criteria of 'successful transmission:

- message transmission (under average error criterion[1])
- message transmission (under maximal error criterion[2])
- entanglement transmission
- strong subspace transmission
- corresponding security criteria

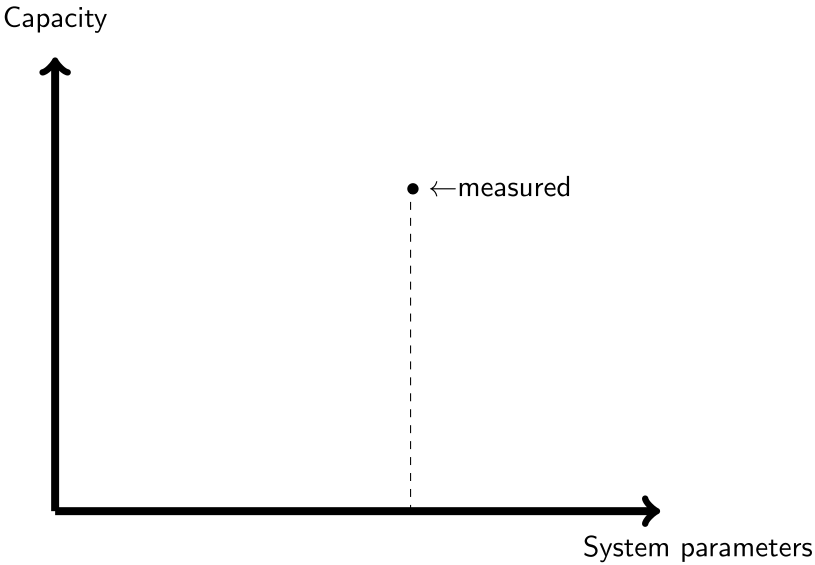
[1] solved for AVCs in [CS89]

[2] connected to zero-error capacity [Ahl70]

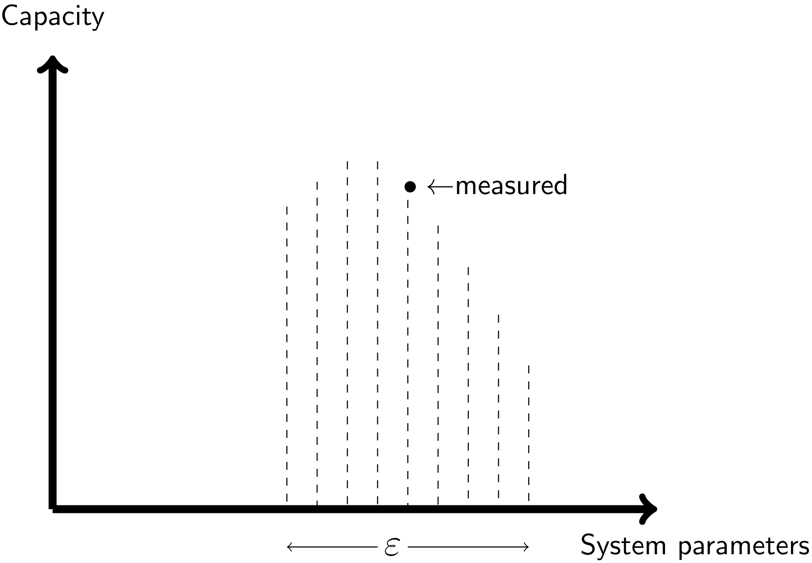
Remarks on continuity of capacities



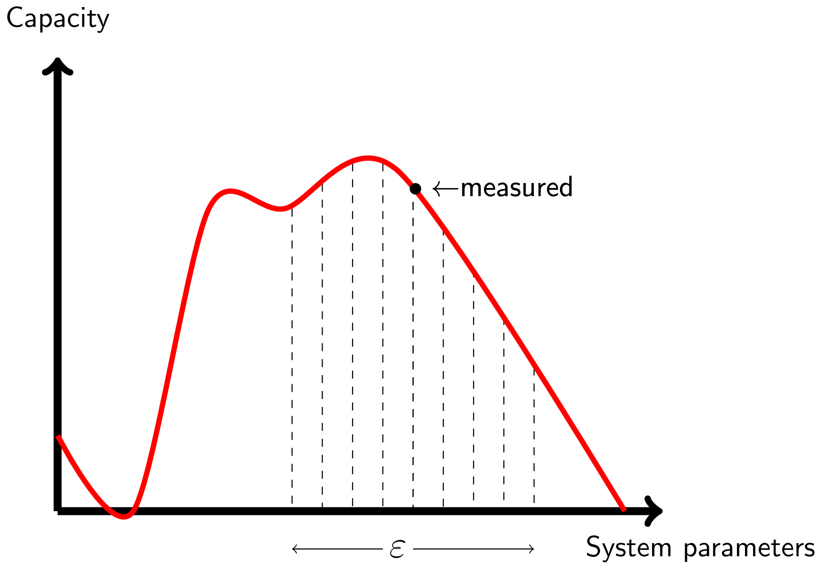
Remarks on continuity of capacities



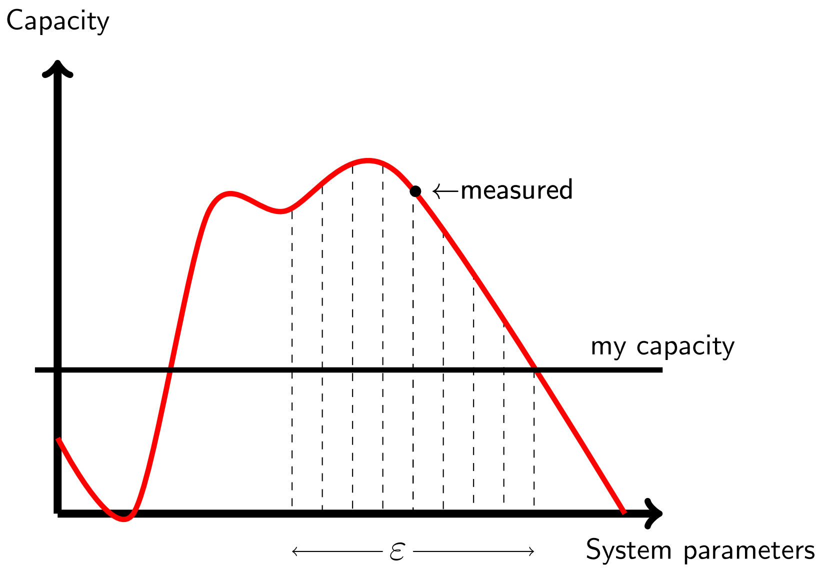
Remarks on continuity of capacities



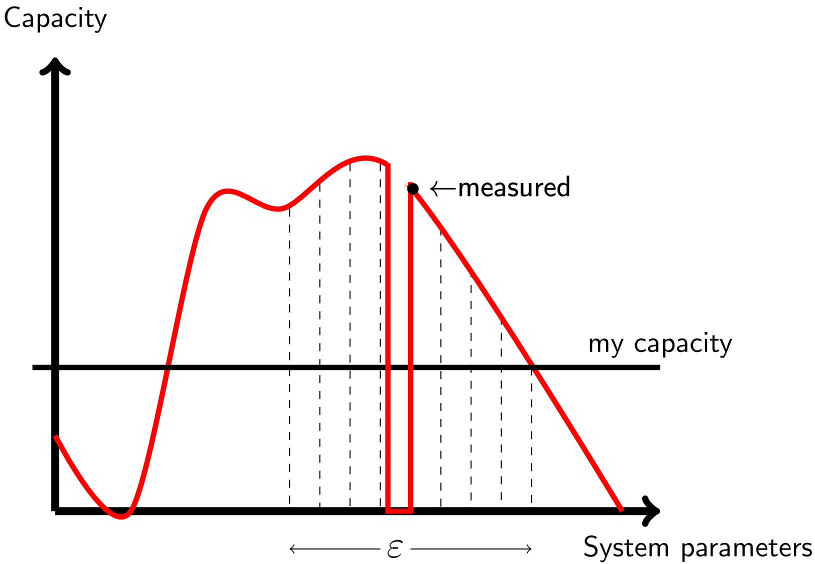
Remarks on continuity of capacities



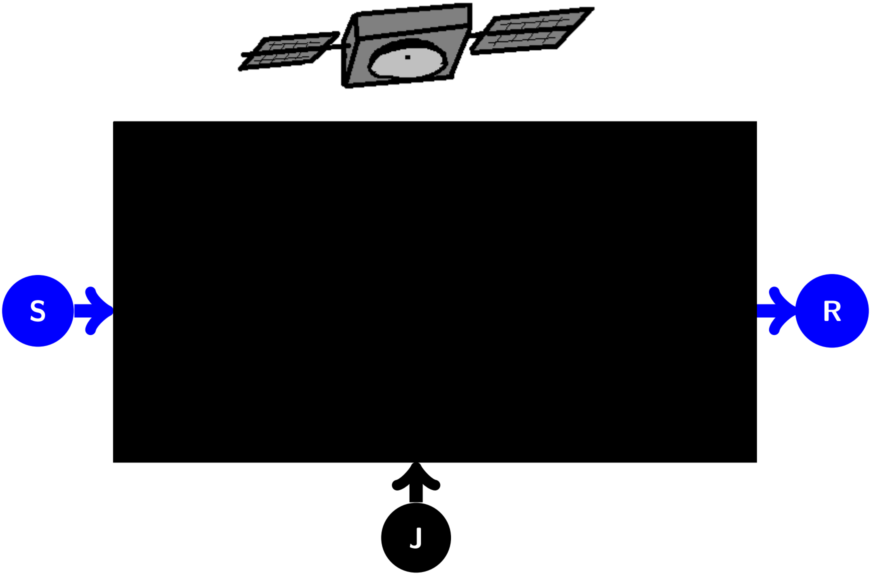
Remarks on continuity of capacities



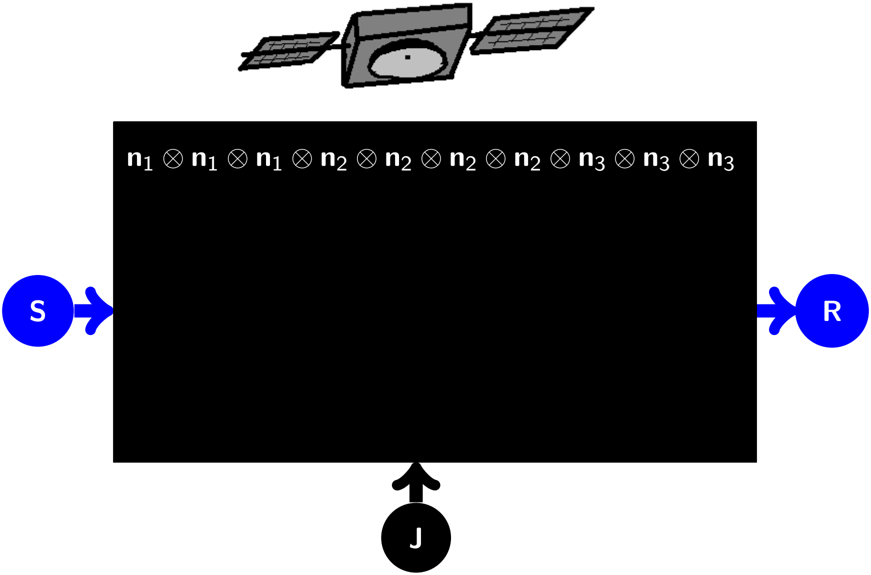
Remarks on continuity of capacities



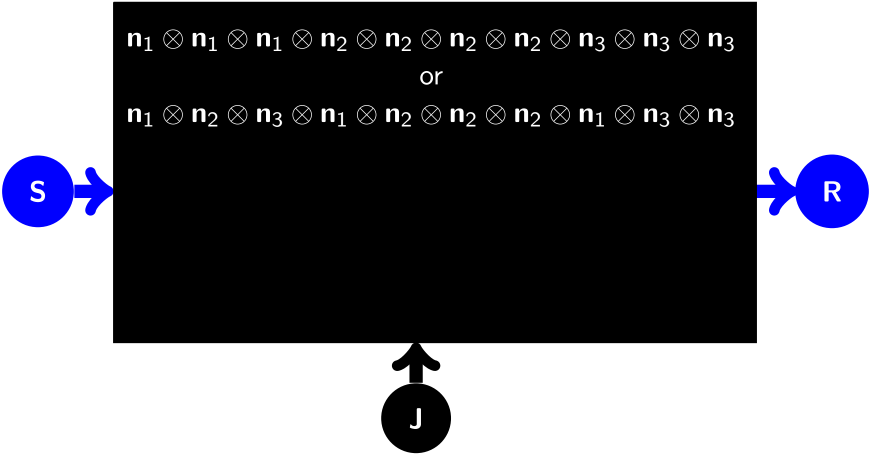
AVQC $\mathfrak{J} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses



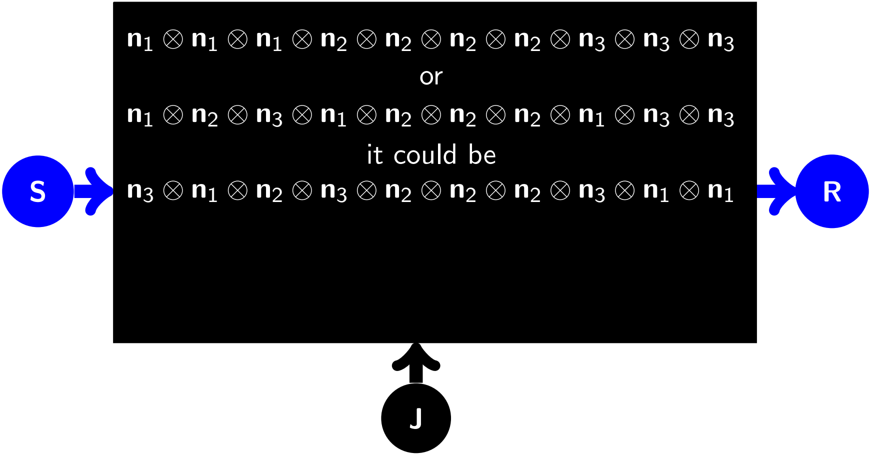
AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses



AVQC $\mathfrak{J} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses



AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses



AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

or

$\mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_1 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

it could be

S $\rightarrow$ $\mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$ $\rightarrow$ R

or something completely different?

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$

$\uparrow$

J

AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses

$$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$$

or

$$\mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_1 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$$

it could be

S

$$\mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$$

R

or something completely different?

$$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$$

$$\vdots$$

J

S

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

or

$\mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_1 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

it could be

$\mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$

or something completely different?

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$

$\vdots$

R

J

AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$, no randomness, 10 channel uses

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

or

$\mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_1 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

it could be

S $\rightarrow$ $\mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$ $\rightarrow$ R

or something completely different?

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$

$\vdots$

$\uparrow$

J

AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$ with randomness, 10 channel uses

S

$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

or

$\mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_1 \otimes \mathbf{n}_3 \otimes \mathbf{n}_3$

it could be

$\mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_2 \otimes \mathbf{n}_3 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$

or something completely different?

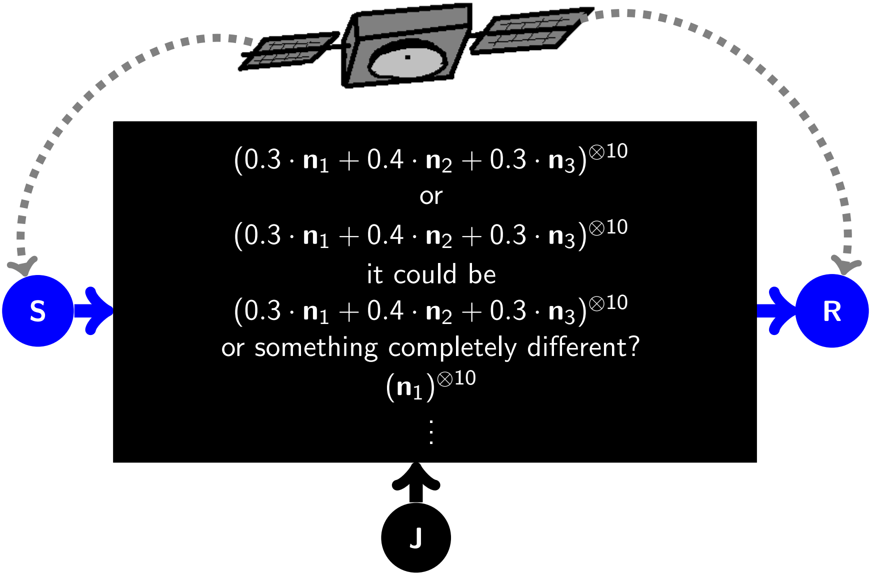
$\mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1 \otimes \mathbf{n}_1$

$\vdots$

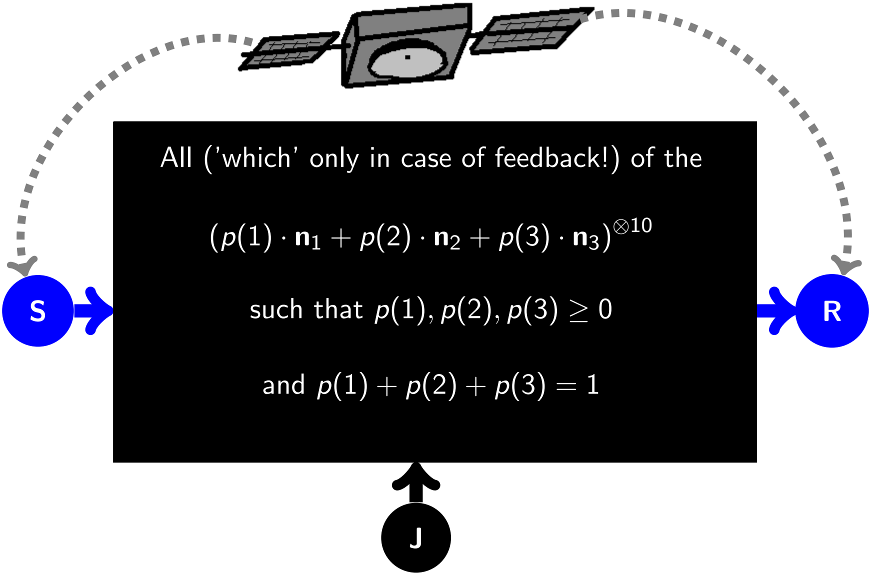
R

J

AVQC $\mathfrak{I} = \{\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3\}$ with randomness, 10 channel uses



Shared randomness: AVQC → compound channel



Basics

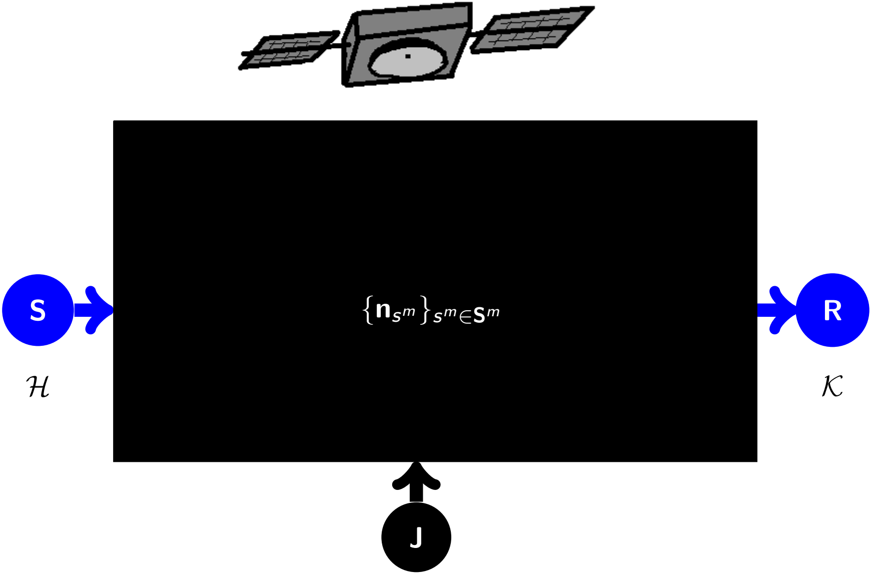
- The quantum systems $\mathcal{H}, \mathcal{K}$ under consideration are modeled on finite dimensional Hilbert spaces labelled by the same letters $\mathcal{H}, \mathcal{K}$.
- Quantum channels from $\mathcal{H}$ to $\mathcal{K}$ are modeled by completely positive trace preserving maps. The set of all channels from $\mathcal{H}$ to $\mathcal{K}$ is written $CPTPM(\mathcal{H}, \mathcal{K})$.
- If the input system is a finite set $\mathbf{X}$ instead of a quantum system, the channel is called a 'cq-channel'. The set of all channels with input set $\mathbf{X}$ and output system $\mathcal{H}$ is labeled $CQ(\mathbf{X}, \mathcal{H})$.

Basics

- The quantum systems $\mathcal{H}, \mathcal{K}$ under consideration are modeled on finite dimensional Hilbert spaces labelled by the same letters $\mathcal{H}, \mathcal{K}$.
- Quantum channels from $\mathcal{H}$ to $\mathcal{K}$ are modeled by completely positive trace preserving maps. The set of all channels from $\mathcal{H}$ to $\mathcal{K}$ is written $CPTPM(\mathcal{H}, \mathcal{K})$.
- If the input system is a finite set $\mathbf{X}$ instead of a quantum system, the channel is called a 'cq-channel'. The set of all channels with input set $\mathbf{X}$ and output system $\mathcal{H}$ is labeled $CQ(\mathbf{X}, \mathcal{H})$.
- Throughout, $\mathfrak{I}$ denotes a finite subset: $\mathfrak{I} \subset CPTPM(\mathcal{H}, \mathcal{K})$.
- Throughout, $\mathfrak{I} = \{\mathbf{n}_s\}_{s \in \mathbf{S}}$ also denotes the arbitrarily varying quantum channel which is generated by it: $(\{\mathbf{n}_{s^m}\}_{s^m \in \in \mathbf{S}^m})_{m \in \mathbb{N}}$.
- For m channel uses, the possible channels are $\{\mathbf{n}_{s^m}\}_{s^m \in \mathbf{S}^m}$, where

$$\mathbf{S}^m := \mathbf{S} \times \ldots \times \mathbf{S}, \qquad \mathbf{n}_{s^m} := \mathbf{n}_{s_1} \otimes \ldots \otimes \mathbf{n}_{s_m}$$

AVQC, no shared randomness, m channel uses



Message transmission under channel uncertainty

- For the moment: No 'arbitrarily varying' channel.

Message transmission under channel uncertainty

- For the moment: No 'arbitrarily varying' channel.
- Sender S has message set $[M] = \{1, \dots, M\}$. He wants to send them to receiver R. Transmission takes place over one of the channels from the set $\{\mathbf{n}_s\}_{s \in \mathbf{S}} \subset CPTPM(\mathcal{H}, \mathcal{K})$. Neither sender nor receiver knows the index $s \in \mathbf{S}$.
- S uses the encoding $\mathcal{P} \in CQ([M], \mathcal{H})$, R tries to guess the message - he measures the output system with a POVM $\mathbf{D} \in \mathcal{M}_M$:

$$\mathcal{M}_M := \{(D(1), \dots, D(M)) : D(k) \geq 0 \ \forall k, \ \sum_k D(k) = \mathbb{1}_{\mathcal{K}}\}.$$

- Probability of (perhaps wrongly) guessing k when k' was sent over channel $\mathbf{n}_s$:

$$\mathrm{tr}\{ \ D(k) \cdot \mathbf{n}_s(\mathcal{P}(k')) \ \}.$$

- Measure of successful transmission:

$$\min_{s \in \mathbf{S}} \frac{1}{M} \sum_k \mathrm{tr}\{D(k)\mathbf{n}_s(\mathcal{P}(k))\} \ \in [0, 1].$$

Entropic quantities

Asymptotic system performance is described by entropic quantities:

Definition (Von Neumann Entropy)

Let $\rho \in \mathcal{S}(\mathcal{H})$ be a state. Its von Neumann entropy is

$$S(\rho) := -\mathrm{tr}\,\rho \log \rho$$

Definition (Ensemble)

Any finite alphabet $\mathcal{X}$, probability distribution p on $\mathcal{X}$ and set $\{\rho_x\}_{x \in \mathcal{X}} \subset \mathcal{S}(\mathcal{H})$ defines an ensemble $E := \{p(x), \rho_x\}_{x \in \mathcal{X}}$

Definition (Holevo Quantity)

Let $\mathbf{n}$ be a channel and $E = \{p(x), \rho_x\}_{x \in \mathcal{X}}$ an ensemble. Then

$$\chi(E, \mathbf{n}) := S(\mathbf{n}(\rho)) - \sum_x p(x) S(\mathbf{n}(\rho_x)),$$

Definition: Message transmission capacities

- Let $m \in \mathbb{N}$. An (m, M_m) random code for message transmission over $\mathfrak{I}$ is a probability distribution γ_m on a finite subset $\{\mathcal{P}_i\}_{i=1}^{\Gamma_m} \times \{\mathbf{D}_j\}_{j=1}^{\Gamma_m}$ of $CQ([M_m], \mathcal{H}^{\otimes m}) \times \mathcal{M}_{M_m}$.
- $R \geq 0$ is called achievable with random codes if there exists a sequence $(\gamma_m)_{m\in\mathbb{N}}$ of random codes satisfying both

$$1) \quad \liminf_{m\to\infty} \min_{s^m \in \mathbf{S}^m} \sum_{i,j=1}^{|\Gamma_m|} \gamma_m(i,j) \frac{1}{M_m} \sum_{k=1}^{M_m} \mathrm{tr}\{D_j(k) \mathbf{n}_{s^m}(\mathcal{P}_i(k))\} = 1$$

$$2) \quad \liminf_{m\to\infty} \frac{1}{m} \log M_m \geq R.$$

- The corresponding random message transmission capacity is

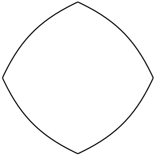
$$\overline{C}_{\mathrm{ran}}(\mathfrak{I}) := \sup\{R : R \text{ is achievable with random codes}\}$$

- The capacity without randomness is

$$\overline{C}_{\mathrm{det}}(\mathfrak{I}) := \sup\left\{ R : \begin{array}{l} \text{R is achievable with random codes} \\ \text{such that } |\Gamma_m| = 1 \ \forall m \in \mathbb{N} \end{array} \right\}$$

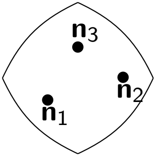
Old results

For every finite $\mathfrak{I} = \{\mathbf{n}_s\}_{s\in\mathbf{S}}$, define
$conv(\mathfrak{I}) := \{\mathbf{n}_p = \sum_{s\in\mathbf{S}} p(s)\mathbf{n}_s |\ p \in \mathfrak{P}(\mathbf{S})\}$.



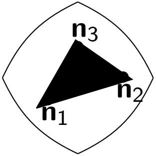
Old results

For every finite $\mathfrak{I} = \{\mathbf{n}_s\}_{s\in\mathbf{S}}$, define
$conv(\mathfrak{I}) := \{\mathbf{n}_p = \sum_{s\in\mathbf{S}} p(s)\mathbf{n}_s |\ p \in \mathfrak{P}(\mathbf{S})\}$.



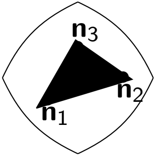
Old results

For every finite $\mathfrak{I} = \{\mathbf{n}_s\}_{s\in\mathbf{S}}$, define
$conv(\mathfrak{I}) := \{\mathbf{n}_p = \sum_{s\in\mathbf{S}} p(s)\mathbf{n}_s |\ p \in \mathfrak{P}(\mathbf{S})\}$.



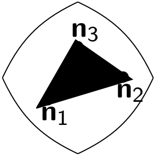
Old results

For every finite $\mathfrak{I} = \{\mathbf{n}_s\}_{s\in\mathbf{S}}$, define
$conv(\mathfrak{I}) := \{\mathbf{n}_p = \sum_{s\in\mathbf{S}} p(s)\mathbf{n}_s |\ p \in \mathfrak{P}(\mathbf{S})\}$.
A It is proven in [BN–] that



Old results

For every finite $\mathfrak{J} = \{\mathbf{n}_s\}_{s\in\mathbf{S}}$, define
$conv(\mathfrak{J}) := \{\mathbf{n}_p = \sum_{s\in\mathbf{S}} p(s)\mathbf{n}_s |\ p \in \mathfrak{P}(\mathbf{S})\}$.
A It is proven in [BN–] that



Theorem (Dichotomy for Message Transmission)

For every finite AVQC $\mathfrak{J}$ we have

1. $\overline{C}_{\mathrm{ran}}(\mathfrak{J}) = \lim_{m\to\infty} \frac{1}{m} \max_E \min_{\mathbf{n}\in conv(\mathfrak{J})} \chi(E, \mathbf{n}^{\otimes m})$
2. *Either* $\overline{C}_{\mathrm{det}}(\mathfrak{J}) = 0$ *or else* $\overline{C}_{\mathrm{det}}(\mathfrak{J}) = \overline{C}_{\mathrm{ran}}(\mathfrak{J})$.

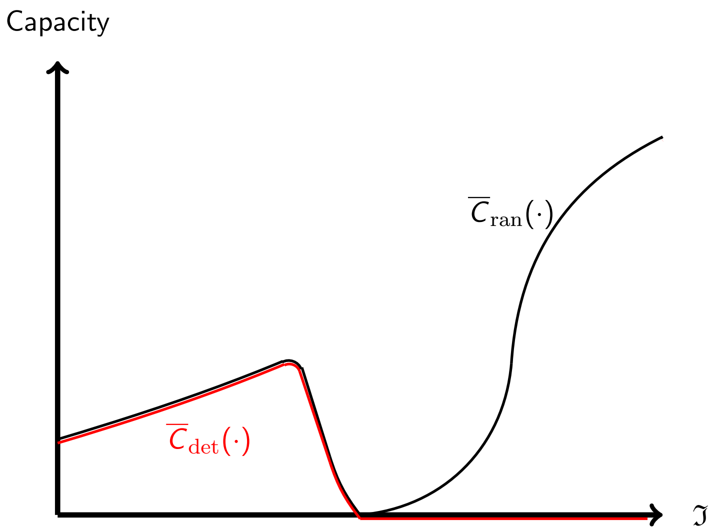
Theorem ([ABBN13])

A finite AVQC $\{\mathbf{n}_s\}_{s\in\mathbf{S}}$ has $\overline{C}_{\mathrm{det}}(\mathfrak{J}) = 0$ if and only if it satisfies for all $m \in \mathbb{N}$: For all $\rho, \sigma \in \mathcal{S}(\mathcal{H}^{\otimes m})$ there is $p, q \in \mathfrak{P}(\mathbf{S}^m)$ such that

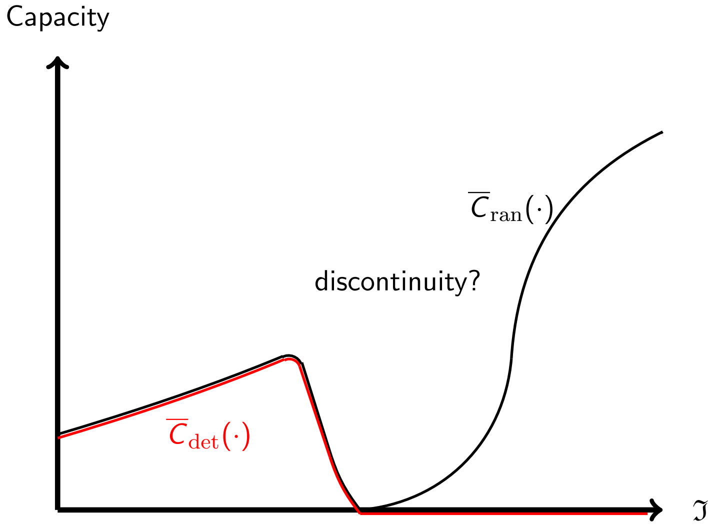
$$\sum_{s^m\in\mathbf{S}^m} p(s^m)\mathbf{n}_{s^m}(\rho) = \sum_{s^m\in\mathbf{S}^m} q(s^m)\mathbf{n}_{s^m}(\sigma) \qquad (*)$$

$(*)$ An AVQC with this property is called 'm-symmetrizable'

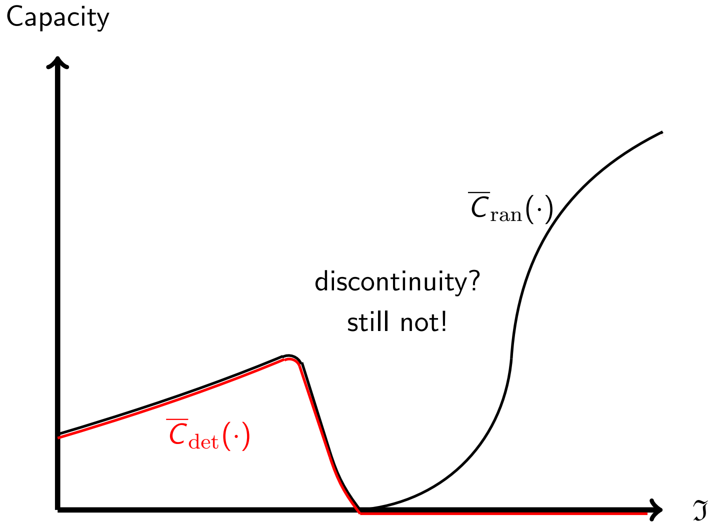
New Result I: Randomness helps!



New Result I: Randomness helps!



New Result I: Randomness helps!



New result I: Randomness helps!

Theorem

❶ *Let $\mathfrak{I}$ consist of entanglement breaking channels that have the special form $\mathbf{n}_s(\rho) := \sum_{x\in\mathbf{X}} \mathrm{tr}\{\rho M_x\}\rho_{s,x}$, $s \in \mathbf{S}$, for some finite set $\mathbf{S}$ and POVM $\{M_i\}_{i=1}^{M}$ on $\mathcal{H}$. The following is true:*

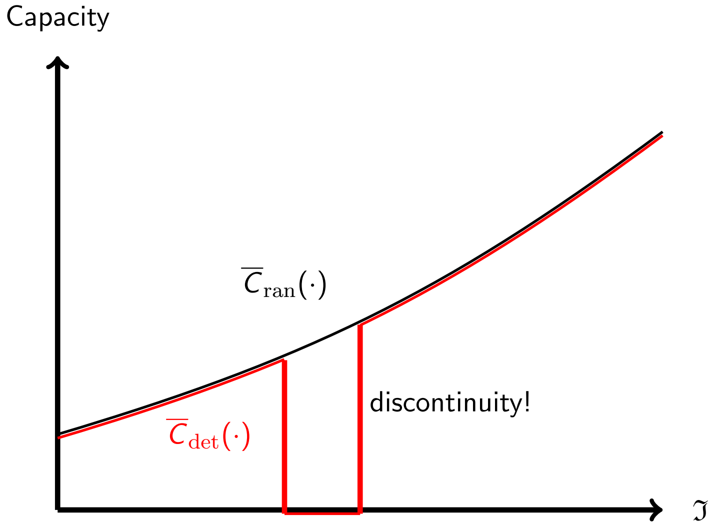
If there are probability distributions $\{p_x\}_{x\in\mathbf{X}} \subset \mathfrak{P}(\mathbf{S})$ such that

$$\sum_{s\in\mathbf{S}} p_{x'}(s)\rho_{s,x} = \sum_{s\in\mathbf{S}} p_x(s)\rho_{s,x'} \qquad \forall x, x' \in \mathbf{X},$$

then it holds $\overline{C}_{\mathrm{det}}(\mathfrak{I}) = 0$.

❷ *There exists an example of an AVQC satisfying the above conditions which additionally has the property $\overline{C}_{\mathrm{ran}}(\mathfrak{I}) > 0$.*

New result II: Discontinuity



New result II: $\overline{C}_{\mathrm{det}}$ is discontinuous

Theorem (Discontinuity of $\overline{C}_{\mathrm{det}}$)

The function $\overline{C}_{\mathrm{det}}$ is discontinuous on $\{\mathfrak{I} \subset \mathcal{C}(\mathcal{H}, \mathcal{K}) : |\mathfrak{I}| < \infty\}$.

New result III: The property $C_{\mathrm{det}}(\mathfrak{I}) > 0$ is stable

(the set where $C_{\mathrm{det}} > 0$ is open)

Theorem (Positivity of $\overline{C}_{\mathrm{det}}$ is stable)

Let $\mathfrak{I}$ be a finite AVQC satisfying $\overline{C}_{\mathrm{det}}(\mathfrak{I}) > 0$. There exists $\delta_0 > 0$ such that for all finite AVQCs $\mathfrak{I}'$ satisfying $D_{\Diamond}(\mathfrak{I}, \mathfrak{I}') \leq \delta_0$ it holds $\overline{C}_{\mathrm{det}}(\mathfrak{I}') > 0$.

($D_{\Diamond}$ denotes the Hausdorff-distance induced by the diamond norm)

Randomness helps: Idea of proof

$$\mathcal{H} \xrightarrow[\text{(entanglement breaking)}]{\text{measurement}} \mathbf{X} \xrightarrow[\text{classical-quantum channel}]{\text{arbitrarily varying}} \mathcal{K}$$

- Entanglement breaking channel $\Rightarrow$ one-shot random capacity
- Entangled signal states from $\mathcal{H}$ $\rightarrow$ random encoding for *cq* part
- Message transmission capacity of an AVcqC does not benefit from randomization at the encoder (proof: straightforward as in [AB07])
- It follows $\overline{C}_{\mathrm{det}}(\mathfrak{I}) = 0$ (by symmetrizability of the cq-part).
- To prove that $\overline{C}_{\mathrm{ran}}(\mathfrak{I}) > 0$: Take fixed product state encoding. Use results of [AB07] again $\Rightarrow$ for specific choice $\rho_{1,1} = |e_1\rangle\langle e_1|$, $\rho_{1,2} = \rho_{2,1} = |e_3\rangle\langle e_3|$, $\rho_{2,2} = |e_2\rangle\langle e_2|$, $\mathbf{X} = \mathbf{S} = \{1, 2\}$, $M_1 = |e_1\rangle\langle e_1|$, $M_2 = |e_2,\rangle\langle e_2|$:

$$\overline{C}_{\mathrm{ran}}(\mathfrak{I}) \geq \min_{\mathbf{n} \in \mathrm{conv}(\mathfrak{I})} \chi(\{\tfrac{1}{2}, \{|e_i\rangle\langle e_i\}_{i=1}^{2}\}, \mathbf{n}) \geq 1/2$$

Discontinuity: Idea of proof

- Take the same channel $\mathfrak{I}$ as before. Augment it by a tiny bit of 'identity': $Id(X) = X$ embeds the matrices from $\mathbb{C}^2$ into those on $\mathbb{C}^3$.

$$\mathbf{n}_{s,\lambda} := (1-\lambda)Id + \lambda \mathbf{n}_s, \qquad \mathfrak{I}_\lambda := \{\mathbf{n}_{s,\lambda}\}_{s \in \mathbf{S}}$$

- Obviously, $\lim_{\lambda \to 1} D_\Diamond(\mathfrak{I}_\lambda, \mathfrak{I}) = 0$
- We know that $\mathfrak{I}_1 = \{\mathbf{n}_{s,\lambda}\}_{s \in \mathbf{S}}$ satisfies $C_{\mathrm{det}}(\mathfrak{I}_1) = 0$.
- It is easy to show that $\mathfrak{I}_\lambda$ is non-symmetrizable for all $\lambda \in [0, 1)$
- It follows $\overline{C}_{\mathrm{ran}}(\mathfrak{I}_\lambda) = C_{\mathrm{det}}(\mathfrak{I}_\lambda)$ for all $\lambda \in [0, 1)$ (here, one uses the dichotomy-result!)
- But $C_{\mathrm{ran}}(\mathfrak{I}_1) \geq 1/2$, whence $C_{\mathrm{ran}}(\mathfrak{I}_\lambda) \geq 1/4$ for $\lambda \approx 1$
- Thus $C_{\mathrm{det}}(\mathfrak{I}_\lambda) \geq 1/4$ for $\lambda \approx 1$, but $C_{\mathrm{det}}(\mathfrak{I}_1) = 0$

Stability: Idea of proof

- For every $m \in \mathbb{N}$ define, on finite sets $\{\mathbf{n}_i\}_{i\in\mathcal{I}} \subset \mathcal{C}(\mathcal{H}^{\otimes m}, \mathcal{K}^{\otimes m})$ of channels, a function F_m through

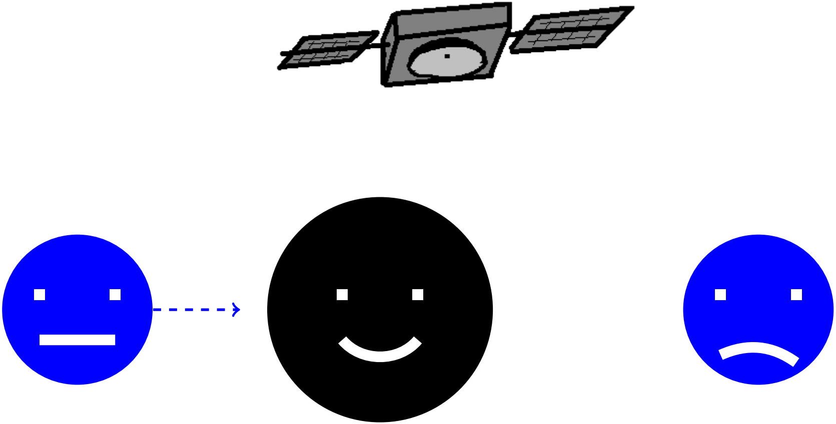
$$\{\mathbf{n}_i\}_{i\in\mathcal{I}} \mapsto \max_{\rho,\sigma\in\mathcal{S}(\mathcal{H}^{\otimes m})} \min_{q,p\in\mathfrak{P}(\mathcal{I})} \|\sum_{i\in\mathcal{I}}(p(i)\mathbf{n}_i(\rho) - q(i)\mathbf{n}_i(\sigma))\|_1.$$

- It holds $\overline{C}_{\mathrm{det}}(\mathfrak{I}) > 0 \Leftrightarrow \exists\ m \in \mathbb{N}: \ F_m(\mathfrak{I}) > 0$.
  (Use the connection between symmetrizability and $\overline{C}_{det}$)

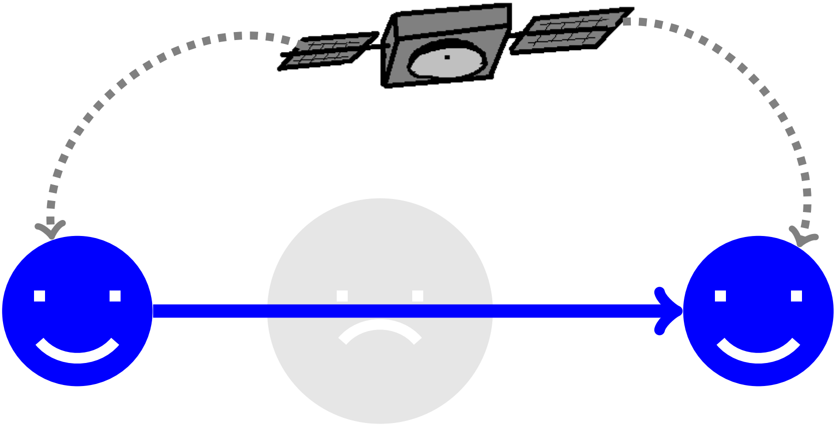
- Show that $F_m(\mathfrak{I}) \approx F_m(\mathfrak{I}')$ if $\mathfrak{I} \approx \mathfrak{I}'$.

- If $C_{\mathrm{det}}(\mathfrak{I}) > 0$ then there is $m \in \mathbb{N}$ such that $F_m(\mathfrak{I}) > 0$, but then choosing $\mathfrak{I}' \approx \mathfrak{I}$ ensures $F_m(\mathfrak{I}') > 0$, whence $C_{\mathrm{det}}(\mathfrak{I}') > 0$.

Conclusion



Shared randomness:
Can increase the capacity and stabilize the system



Finite error, finite resources

If instead of

$$\liminf_{m\to\infty} \min_{s^m\in\mathbf{S}^m} \sum_{i,j=1}^{|\Gamma_m|} \gamma_m(i,j)\frac{1}{M_m}\sum_{k=1}^{M_m} \mathrm{tr}\{D_j(k)\mathbf{n}_{s^m}(\mathcal{P}_i(k))\} = 1$$

on requires for some $\lambda \in (0,1)$ only

$$\liminf_{m\to\infty} \min_{s^m\in\mathbf{S}^m} \sum_{i,j=1}^{|\Gamma_m|} \gamma_m(i,j)\frac{1}{M_m}\sum_{k=1}^{M_m} \mathrm{tr}\{D_j(k)\mathbf{n}_{s^m}(\mathcal{P}_i(k))\} \geq 1-\lambda$$

then the corresponding capacity $\overline{C}_{\mathrm{ran}}(\mathfrak{I},\lambda)$ can be achieved using only a finite amount K of shared random bits, and K scales as $K \approx 1/\lambda$.
The number of channel uses needed to achieve an error smaller than λ scales as $\log(1/\lambda)$.

See our paper for an exact statement.

Entanglement fidelity (entanglement transmission)

- Sender $\mathfrak{S}$ has access to one part of pure entangled state $|\psi\rangle\langle\psi| \in \mathcal{S}(\mathcal{F} \otimes \mathcal{F})$.
- He wishes to transmit his half to receiver $\mathfrak{R}$ by use of the channel $\mathbf{n} \in CPTPM(\mathcal{H}, \mathcal{K})$.
- $\mathfrak{S}$ uses the encoding map $\mathcal{P} \in CPTPM(\mathcal{F}, \mathcal{H})$
- and $\mathfrak{R}$ the decoding map $\mathcal{R} \in CPTPM(\mathcal{K}, \mathcal{F})$.
- Measure of success:

$$\langle \psi, Id_{\mathcal{F}} \otimes \mathcal{R} \circ \mathbf{n} \circ \mathcal{P}(|\psi\rangle\langle\psi|)\psi\rangle =: F_e(\rho, \mathcal{R} \circ \mathbf{n} \circ \mathcal{P}) \in [0, 1],$$

where $\rho := Id_{\mathcal{F}} \otimes \mathrm{tr}_{\mathcal{F}}(|\psi\rangle\langle\psi|)$ (the marginal state).

Remark: For arbitrary (sub) spaces $\mathcal{F}$, $\pi_{\mathcal{F}}$ denotes the state supported only on $\mathcal{F}$ satisfying $\mathrm{spec}(\mathcal{F}) = \frac{1}{\dim \mathcal{F}}$.

Minimum fidelity (strong subspace transmission)

- Sender $\mathfrak{S}$ controls the system $\mathcal{F}$.
- He wants to make sure that he can send arbitrary states $\rho \in \mathcal{S}(\mathcal{F})$ to the receiver $\mathfrak{R}$ by use of a channel $\mathbf{n} \in CPTPM(\mathcal{H}, \mathcal{K})$.
- $\mathfrak{S}$ uses the encoding $\mathcal{P} \in CPTPM(\mathcal{F}, \mathcal{H})$
- and $\mathfrak{R}$ the decoding $\mathcal{R} \in CPTPM(\mathcal{K}, \mathcal{F})$.
- Measure describing how well the channel $\mathcal{R} \circ \mathbf{n} \circ \mathcal{P}$ preserves the states sent by $\mathfrak{S}$:

$$\min_{x \in S(\mathcal{F})} \langle x, \mathcal{R} \circ \mathbf{n} \circ \mathcal{P}(|x\rangle\langle x|)x\rangle =: F_{\min}(\mathcal{F}, \mathcal{R} \circ \mathbf{n} \circ \mathcal{P}) \ \in [0, 1].$$

Remark: $S(\mathcal{F}) = \{x \in \mathcal{F} : \|x\| = 1\}$ is the unit sphere on $\mathcal{F}$.

Coherent information

- Measure of how much noise is induced by $\mathbf{n}$: For arbitrary $\rho \in \mathcal{S}(\mathcal{H})$, $\mathbf{n} \in CPTPM(\mathcal{H}, \mathcal{K})$ it is given by

  $$I_c(\rho, \mathbf{n}) := S(\mathbf{n}(\rho)) - S(Id \otimes \mathbf{n}(|\psi\rangle\langle\psi|)).$$

  Here, and only for a brief moment, S denotes von Neumann Entropy.

Entanglement transmission

- A (deterministic) (m, k_m)-code for the AVQC $\mathfrak{I} = \{\mathbf{n}_s\}_{s\in\mathbf{S}}$ is a triple $(\mathcal{F}_m, \mathcal{P}^m, \mathcal{R}^m)$, where

$$\begin{aligned} \mathcal{F}_m \quad &- \quad \text{Hilbert space of dimension } \dim \mathcal{F}_m = k_m \\ \mathcal{P}^m \in CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \quad &- \quad \text{the encoding} \\ \mathcal{R}^m \in CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m) \quad &- \quad \text{the decoding} \end{aligned}$$

- $R \geq 0$ is a an achievable rate for entanglement transmission over the AVQC $\mathfrak{I}$ if there is a sequence of (m, k_m)-codes with

$$\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R,$$
$$\lim_{m\to\infty} \inf_{s^m\in\mathbf{S}^m} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathbf{n}_{s^m} \circ \mathcal{P}^m) = 1.$$

- Entanglement transmission capacity $\mathcal{A}_{\text{det}}(\mathfrak{I})$ of $\mathfrak{I}$:

$$\mathcal{A}_{\text{det}}(\mathfrak{I}) := \sup \left\{ R : \begin{array}{l} R \text{ is achievable entanglement} \\ \text{transmission rate for } \mathfrak{I} \end{array} \right\}$$

Entanglement transmission using random codes

- A (random) (m, k_m)-random code for the AVQC $\mathfrak{I} = \{\mathbf{n}_s\}_{s \in \mathbf{S}}$ is a probability distribution μ on a finite set Γ together with a set of triples $(\mathcal{F}_m, \mathcal{P}^m_\gamma, \mathcal{R}^m_\gamma)$ for each $\gamma \in \Gamma$, where

$$\begin{aligned} \mathcal{F}_m \quad &- \quad \text{Hilbert space of dimension } \dim \mathcal{F}_m = k_m \\ \mathcal{P}^m_\gamma \in CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \quad &- \quad \text{the encoding} \\ \mathcal{R}^m_\gamma \in CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m) \quad &- \quad \text{the decoding} \end{aligned}$$

- $R \geq 0$ achievable: $\exists$ sequence of (m, k_m)-random codes with

$$\liminf_{m \to \infty} \frac{1}{m} \log k_m \geq R,$$

$$\lim_{m \to \infty} \inf_{s^m \in \mathbf{S}^m} \sum_{\gamma \in \Gamma} \mu(\gamma) F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m_\gamma \circ \mathbf{n}_{s^m} \circ \mathcal{P}^m_\gamma) = 1.$$

- Randomness-assisted entanglement transmission capacity of $\mathfrak{I}$:

$$\mathcal{A}_{\text{rand}}(\mathfrak{I}) := \sup \left\{ R : \begin{array}{l} R \text{ is achievable entanglement transm.} \\ \text{rate for } \mathfrak{I} \text{ (with random codes)} \end{array} \right\}$$

Strong subspace transmission

- A (deterministic) (m, k_m)-code for the AVQC $\mathfrak{I} = \{\mathbf{n}_s\}_{s \in \mathbf{S}}$ is a triple $(\mathcal{F}_m, \mathcal{P}^m, \mathcal{R}^m)$, where

$$\begin{aligned} \mathcal{F}_m &\ - \ \text{Hilbert space of dimension } \dim \mathcal{F}_m = k_m \\ \mathcal{P}^m &\in CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \ - \ \text{the encoding} \\ \mathcal{R}^m &\in CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m) \ - \ \text{the decoding} \end{aligned}$$

- $R \geq 0$ is a an achievable rate for strong subspace transmission over the AVQC $\mathfrak{I}$ if there is a sequence of (m, k_m)-codes with

$$\liminf_{m \to \infty} \frac{1}{m} \log k_m \geq R,$$
$$\lim_{m \to \infty} \inf_{s^m \in \mathbf{S}^m} F_{\min}(\mathcal{F}_m, \mathcal{R}^m \circ \mathbf{n}_{s^m} \circ \mathcal{P}^m) = 1.$$

- Strong subspace transmission capacity $\mathcal{A}_{s,\mathrm{det}}(\mathfrak{I})$ of $\mathfrak{I}$:

$$\mathcal{A}_{s,\mathrm{det}}(\mathfrak{I}) := \sup \left\{ R : \begin{array}{l} R \text{ is achievable strong subspace} \\ \text{transmission rate for } \mathfrak{I} \end{array} \right\}$$

An equivalence

Theorem

For every arbitrarily varying quantum channel defined through a subset $\mathfrak{I} \subset CPTPM(\mathcal{H}, \mathcal{K})$ it holds:

$$\mathcal{A}_{\mathsf{s},\mathrm{det}}(\mathfrak{I}) = \mathcal{A}_{\mathrm{det}}(\mathfrak{I}), \qquad \mathcal{A}_{\mathsf{s},\mathrm{rand}}(\mathfrak{I}) = \mathcal{A}_{\mathrm{rand}}(\mathfrak{I})!$$

Comparison to classical quantities

Strong subspace transmission is considered an analogue to the maximal error[1] criterion,

entanglement transmission as the analogue to the average error[2] criterion.

For classical arbitrarily varying channels, the capacities for message transmission under average -and maximal error probability criterion are NOT identical!
(There, at least one has to explicitly assume that randomized encoding schemes are used in order to get identical capacities)

[1] average error of a code is given by $$\frac{1}{M}\sum_{i=1}^{M}\mathrm{tr}\{D_i\mathbf{n}(\rho_i)\},$$

[2] maximal error of a code is given by $$\max_{1\le i\le M}\mathrm{tr}\{D_i\mathbf{n}(\rho_i)\}.$$

Why THAT analogue?

- For every $\mathcal{M} \in CPTPM(\mathcal{F}_m, \mathcal{F}_m)$, $\dim(\mathcal{F}_m)$ arbitrary, it holds

$$1 - \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} F_e(\rho, \mathcal{M}) \leq 4\sqrt{1 - F_{\min}(\mathcal{F}_m, \mathcal{M})} \leq 4\sqrt{\|\mathcal{M} - id_{\mathcal{F}_m}\|_\infty}$$

$$\leq 4\sqrt{\|\mathcal{M} - id_{\mathcal{F}_m}\|_{cb}} \leq 8(1 - \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} F_e(\rho, \mathcal{M}))^{1/4}$$

[KW04]

Why THAT analogue?

- For every $\mathcal{M} \in CPTPM(\mathcal{F}_m, \mathcal{F}_m)$, $\dim(\mathcal{F}_m)$ arbitrary, it holds

$$1 - \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} F_e(\rho, \mathcal{M}) \leq 4\sqrt{1 - F_{\min}(\mathcal{F}_m, \mathcal{M})} \leq 4\sqrt{\|\mathcal{M} - id_{\mathcal{F}_m}\|_\infty}$$
$$\leq 4\sqrt{\|\mathcal{M} - id_{\mathcal{F}_m}\|_{cb}} \leq 8(1 - \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} F_e(\rho, \mathcal{M}))^{1/4}$$

[KW04]

- For the normalized Haar measure μ on $S(\mathcal{F}_m)$:

$$\int \langle x, \mathcal{M}(|x\rangle\langle x|)x\rangle d\mu(x) = \frac{\dim(\mathcal{F}_m) \cdot F_e(\pi_{\mathcal{F}_m}, \mathcal{M}) + 1}{\dim(\mathcal{F}_m) + 1}.$$

[HHH99, N02]

Why THAT analogue?

- For every $\mathcal{M} \in CPTPM(\mathcal{F}_m, \mathcal{F}_m)$, $\dim(\mathcal{F}_m)$ arbitrary, it holds

$$1 - \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} F_e(\rho, \mathcal{M}) \leq 4\sqrt{1 - F_{\min}(\mathcal{F}_m, \mathcal{M})} \leq 4\sqrt{\|\mathcal{M} - id_{\mathcal{F}_m}\|_\infty}$$
$$\leq 4\sqrt{\|\mathcal{M} - id_{\mathcal{F}_m}\|_{cb}} \leq 8(1 - \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} F_e(\rho, \mathcal{M}))^{1/4}$$

[KW04]

- For the normalized Haar measure μ on $S(\mathcal{F}_m)$:

$$\int \langle x, \mathcal{M}(|x\rangle\langle x|) x\rangle d\mu(x) = \frac{\dim(\mathcal{F}_m) \cdot F_e(\pi_{\mathcal{F}_m}, \mathcal{M}) + 1}{\dim(\mathcal{F}_m) + 1}.$$

[HHH99, N02]

- And *no* function $f : [0,1] \to [0,1]$ with $\lim_{x \to 1} f(x) = 0$ satisfies

$$\|\mathcal{M} - id_{\mathcal{F}_m}\|_\infty \leq f(F_e(\pi_{\mathcal{F}_m}, \mathcal{M})) \qquad \forall\ \mathcal{M}$$

[KW04]

Quantum-Ahlswede dichotomy for AVQCs

Theorem (Quantum - Ahlswede[3] dichotomy (proven in [ABBN13]))

For the AVQC defined by $\mathfrak{I} = \{\mathbf{n}_s\}_{s\in\mathbf{S}} \subset CPTPM(\mathcal{H},\mathcal{K})$:

$$\mathcal{A}_{\text{random}}(\mathfrak{I}) = \lim_{m\to\infty}\frac{1}{m}\max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes m})}\inf_{\mathbf{n}\in conv(\mathfrak{I})} I_c(\rho,\mathbf{n}^{\otimes m})$$

Either $C_{\text{det}}(\mathfrak{I}) = 0$ *or* $\mathcal{A}_{\text{det}}(\mathfrak{I}) = \mathcal{A}_{\text{random}}(\mathfrak{I})$.

$$conv(\mathfrak{I}) = \left\{\mathbf{n}_{\mathfrak{q}} \,\middle|\, \mathbf{n}_{\mathfrak{q}} = \sum_{s\in\mathbf{S}'}\mathfrak{q}(s)\mathbf{n}_s,\ \mathfrak{q}\in\mathfrak{P}(\mathbf{S}'),\ \mathbf{S}'\subset\mathbf{S},\ |\mathbf{S}'|<\infty\right\}.$$

$\mathfrak{P}(\mathbf{S}')$ - set of probability distributions on $\mathbf{S}'$.

[3] Find its ancestor, the classical Ahlswede-Dichotomie, in [Ahl78]

Conjectures

Conjecture ([ABBN13, BN13])

First, there exist AVQVs $\mathfrak{I}$ *for which*

$$\overline{C}_{\mathrm{random}}(\mathfrak{I}) > \overline{C}_{\mathrm{det}}(\mathfrak{I}).$$

Second, for every AVQC $\mathfrak{I}$ *it holds*

$$\mathcal{A}_{\mathrm{random}}(\mathfrak{I}) = \mathcal{A}_{\mathrm{det}}(\mathfrak{I}).$$

- First conjecture: Solved in [BN–]
- Second conjecture: Still open.

Conclusion

- Message transmission: Shared randomness assisted capacity is continuous
- Message transmission: Shared randomness assisted capacity can be strictly larger than unassisted capacity
- Message transmission: $\overline{C}_{\mathrm{det}}$ is discontinuous
- Entanglement transmission is equivalent to strong subspace transmission
- If our conjecture turns out to be true then the unassisted entanglement transmission capacity is continuous

THANK YOU

[Ahl70] R. Ahlswede, "*A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity*" The Annals of Mathematical Statistics, Vol. 41, No. 3. (1970)

[ABBN13] R. Ahlswede, I. Bjelakovic, H. Boche, J. Nötzel "*Quantum capacity under adversarial noise: arbitrarily varying quantum channels*", Comm. Math. Phys., Vol. 317, Iss. 1, 103-156 (2013)

[AB07] R. Ahlswede, V. Blinovsky, "*Classical capacity of classical-quantum arbitrarily varying channels*", IEEE Trans. Inf. Theory, Vol. 53, No. 2, 526-533 (2007)

[Ahl78] R. Ahlswede, "*Elimination of Correlation in Random Codes for Arbitrarily Varying Channels*", Z. Wahrscheinlichkeitstheorie verw. Gebiete 44, 159-175 (1978)

References II

[BN–] H. Boche, J. Nötzel, "*Positivity, Discontinuity, Finite Resources and Nonzero Error for Arbitrarily Varying Quantum Channels*", accepted for publication in J. Math. Phys. (2014)

[BN13] H. Boche, J. Nötzel, "*Arbitrarily small amounts of correlation for arbitrarily varying quantum channels*" J. Math. Phys. 54, 112202 (2013)

[CS89] I. Csiszar, P. Narayan, "*The Capacity of the Arbitrarily Varying Channel Revisited: Positivity, Constraints*", IEEE Trans. Inf. Th. Vol. 34, No. 2, 181-193 (1989)

[HHH99] M. Horodecki, P. Horodecki, R. Horodecki, "*General teleportation channel, singlet fraction, and quasidistillation*", Phys. Rev. A 60, 1888–1898 (1999)

References III

[KW04] D. Kretschman, R.F. Werner, "*Tema con variazioni: quantum channel capacity*", New Journal of Physics, Vol. 6, 26-59 (2004)

[N02] M.A. Nielsen, "*A simple formula for the average gate fidelity of a quantum dynamical operation*", Phys. Lett. A 303, 249 (2002)