Private Capacity and Subfactors

Carolina Dias Alexiou

The University of Tokyo

Virtual LPQ

2020/06/19

work in progress

Yasuyuki Kawahigashi's group

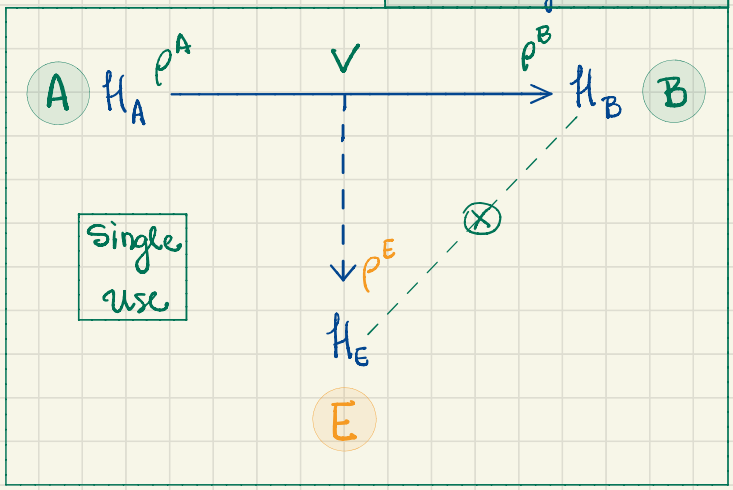
Outline

- Wiretap channels
- Beyond type I
- Private quantum subalgebras

Wiretap Channels : send classical information using quantum channels

(finite dimension)

Schrödinger Picture



$V : \mathcal{H}_A \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_E$ isometry map

$\rho_A \longmapsto \rho_{BE} = \Phi(\rho_A) \doteq V \rho_A V^*$

channel

classical – quantum state

ρ_{BE}

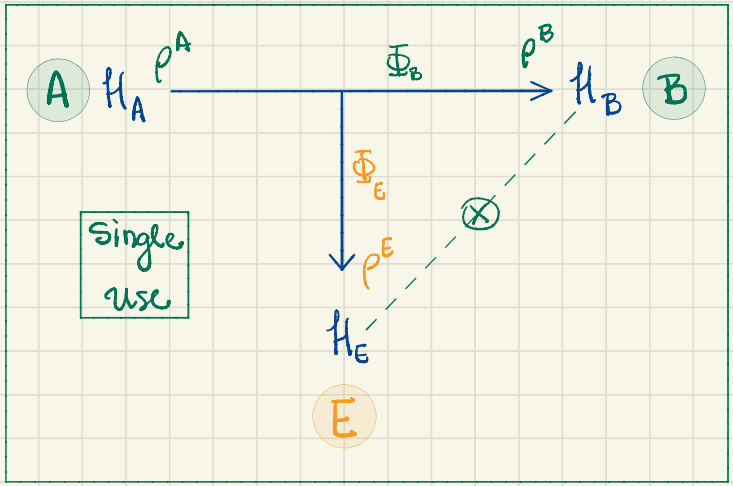
$\begin{cases} \rho_B = Tr_E \rho_{BE} \\ \rho_E = Tr_B \rho_{BE} \end{cases}$

Complementary channels

$$\left.\begin{array}{l} \rho_B = \Phi_B(\rho_A) \;;\; \Phi_B \doteq Tr_E \circ \Phi \\ \rho_E = \Phi_E(\rho_A) \;;\; \Phi_E \doteq Tr_B \circ \Phi \end{array}\right\} \Phi = \Phi_B \otimes \Phi_E$$

Wiretap Channels : send classical information using quantum channels

(finite dimension)



(classical) Shannon Mutual information

$$I(X;Y) = H(Y) - H(Y|X)$$

Shannon entropy

"formal quantum analog"

Holevo χ quantity

given $\mathcal{E} = \{p_x, \rho_x\}_x$ ensemble

$\rho = \mathbb{E}_x(\rho_x) = \sum_x p_x \rho_x$ expected state

$$\chi(\mathcal{E}) = S(\rho) - \sum_x p_x S(\rho_x)$$

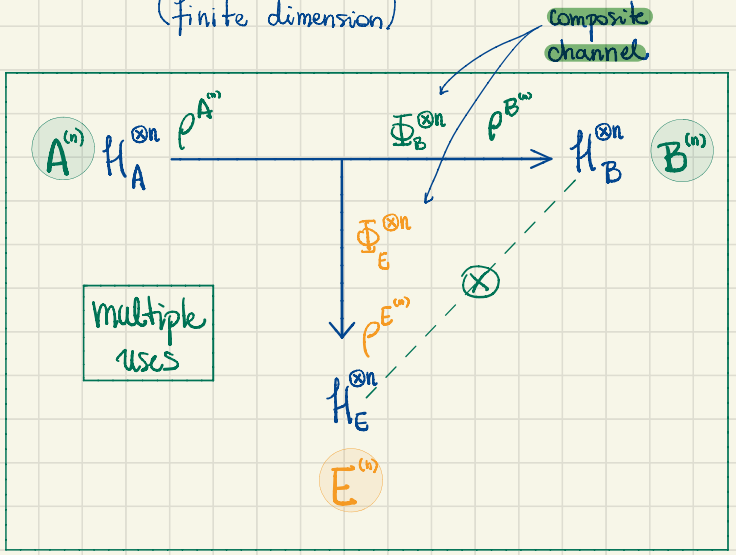
"formal quantum analog" $\quad \mathcal{E} = \{p_x, \rho_x^B\}$

classical – quantum state

$$\sigma_{XA} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x^B \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B) \Rightarrow \boxed{\chi(\mathcal{E}) = I(X;B)_\sigma} = S(B)_\sigma - S(B|X)_\sigma$$

Wiretap Channels : send classical information using quantum channels

(finite dimension)



Holevo χ quantity $\quad \chi(\mathcal{E}) = S(\rho) - \sum_x p_x S(\rho_x)$

- How well can we send information reliably ?
- How can we minimize the leaking of information ?

What is the private (classical) capacity of the channel ? $P(\Phi)$

"amount of information" received by B $-$ "amount of information" received by E

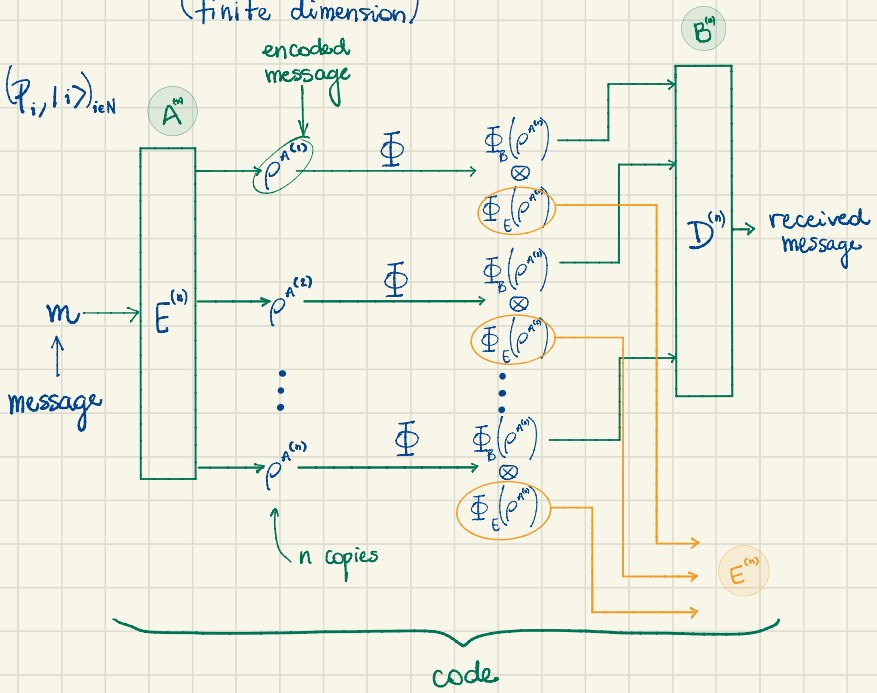
"Definition"

$$P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \left\{ \chi(\mathcal{E}_{B^{(n)}}) - \chi(\mathcal{E}_{E^{(n)}}) \right\}$$

$$\mathcal{E} = \{p_x, \rho_x^{A^{(n)}}\} \; ; \; \mathcal{E}_{B^{(n)}} = \{p_x, \Phi_B^{\otimes n}(\rho_x^{A^{(n)}})\} \; ; \; \mathcal{E}_{E^{(n)}} = \{p_x, \Phi_E^{\otimes n}(\rho_x^{A^{(n)}})\}$$

Wiretap Channels : send classical information using quantum channels

(finite dimension)



number of blocks — number of codewords

A code $(E^{(n)}, D^{(n)})$ with length n and size N for the composite channel

$$\Phi^{\otimes n}: \mathcal{S}(\mathcal{H}_A^{\otimes n}) \to \mathcal{S}(\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E^{\otimes n})$$

consists of an encoding $E^{(n)}$ and a decoding $D^{(n)}$

such that $E^{(n)} = \{E_i^{(n)}\}_{i=1}^N$ in $\mathcal{H}_A^{\otimes n}$

and $D^{(n)} = \{D_i^{(n)}\}_{i=1}^N$ in $\mathcal{H}_B^{\otimes n}$

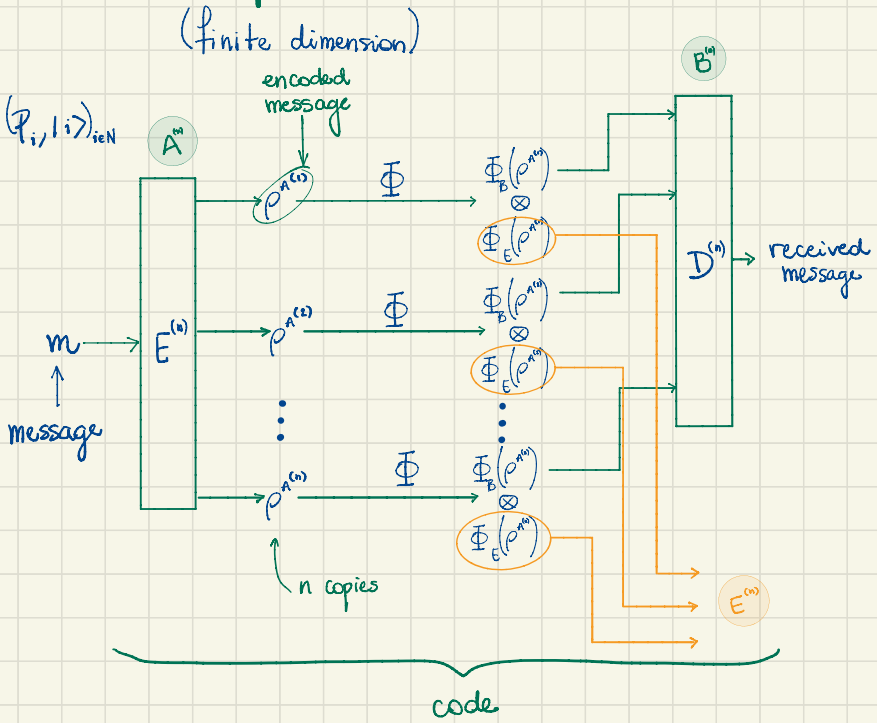
The maximum error probability of a code is

$$P_e(E^{(n)}, M^{(n)}) = \max_m P_r\{D^{(n)}(\Phi^{\otimes n}(E^{(n)}(m))) \neq m\}$$

$$= \max_{i=1,\dots,N} \mathrm{Tr}\left[\left(\mathbb{1} - D_i^{(n)}\right)\left(\Phi^{\otimes}(\rho_i^{A^{(n)}})\right)\right]$$

Wiretap Channels : send classical information using quantum channels

(finite dimension)



- The **maximum error probability** of a code is

$$P_e(E^{(n)}, M^{(n)}) = \max_m \Pr\{D^{(n)}(\Phi^{\otimes n}(E^{(n)}(m))) \neq m\}$$

$$= \max_{i=1,\dots,N} \mathrm{Tr}\left[\left(\mathbb{1} - D_i^{(n)}\right)\left(\Phi^{\otimes}(\rho_i^{A^{(n)}})\right)\right]$$

- The **variability** of a wiretap channel is the quantity

$$\nu_E(E^{(n)}) = \max_{\substack{i,k \\ 1,\dots,N}} \| \rho_{E^{(n)}}^{i} - \rho_{E^{(n)}}^{k} \|_1$$

- $R \geq 0$ is called an **achivable rate** if there exist a sequence of codes $(E^{(n)}, D^{(n)})$ of sizes $N = 2^{nR}$ such that

$$\lim_{n\to\infty} P_e(E^{(n)}, D^{(n)}) = 0$$

and

$$\lim_{n\to\infty} \nu_E(E^{(n)}) = 0$$

Definition : The **private classical capacity** $P(\Phi)$ is the least upper bound of the achievable rates

Wiretap Channels : send classical information using quantum channels

Definition: The private classical capacity $P(\Phi)$ is the least upper bound of the achievable rates

→ average amount of information that can A send to B in a way that the amount E can recover is negligible

$$P(\Phi) \leq \text{"amount of information received by } B\text{"} - \text{"amount of information received by } E\text{"}$$

Theorem (Devetak '03, Cai – Winter – Yeung '04)

$$P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \left\{ \chi(\mathcal{E}_B^{(n)}) - \chi(\mathcal{E}_E^{(n)}) \right\}$$

$$\mathcal{E} = \{p_x, \rho_x^{A^{(n)}}\} \; ; \; \mathcal{E}_B^{(n)} = \{p_x, \Phi_B^{\otimes n}(\rho_x^{A^{(n)}})\} \; ; \; \mathcal{E}_E^{(n)} = \{p_x, \Phi_E^{\otimes n}(\rho_x^{A^{(n)}})\}$$

Wiretap Channels : send classical information using quantum channels

Definition: The **private classical capacity** $P(\Phi)$ is the least upper bound of the achievable rates → average amount of information that can A send to B in a way that the amount E can recover is negligible

Theorem (Devetak '03, Cai – Winter – Yeung '04)

$$P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \left\{ \chi(\mathcal{E}_B^{(n)}) - \chi(\mathcal{E}_E^{(n)}) \right\}$$

$$\mathcal{E} = \{p_x, \rho_x^{A^{(n)}}\} \; ; \; \mathcal{E}_B^{(n)} = \{p_x, \Phi_B^{\otimes n}(\rho_x^{A^{(n)}})\} \; ; \; \mathcal{E}_E^{(n)} = \{p_x, \Phi_E^{\otimes n}(\rho_x^{A^{(n)}})\}$$

Problems • **How to compute $P(\Phi)$?**

Let $C_\chi(\Phi) = \max_{\mathcal{E}} \{\chi(\mathcal{E}_B) - \chi(\mathcal{E}_E)\}$

if $C_\chi(\Phi^{\otimes n}) = n\, C_\chi(\Phi)$, then $P(\Phi) = C_\chi(\Phi)$

(additivity)

(2009) Ke Li et al : Example when is $>$ (superadditive)

Motivation

Can we find families of channels that are additive?

Wiretap Channels : send classical information using quantum channels

Definition: The **private classical capacity** $P(\Phi)$ is the least upper bound of the achievable rates

→ average amount of information that can A send to B in a way that the amount E can recover is negligible

Theorem (Devetak '03, Cai – Winter – Yeung '04)

$$P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \left\{ \chi(\mathcal{E}_B^{(n)}) - \chi(\mathcal{E}_E^{(n)}) \right\}$$

$$\mathcal{E} = \left\{ p_x, \rho_x^{A^{(n)}} \right\} \; ; \; \mathcal{E}_B^{(n)} = \left\{ p_x, \Phi_B^{\otimes n}\left(\rho_x^{A^{(n)}}\right) \right\} \; ; \; \mathcal{E}_E^{(n)} = \left\{ p_x, \Phi_E^{\otimes n}\left(\rho_x^{A^{(n)}}\right) \right\}$$

Problems

- How to compute $P(\Phi)$?
- How to deal with infinite dimension ?
  - Not everything is $\mathcal{B}(\mathcal{H})$ [type I]
  - Entropy can be infinite
  - etc...

Beyond type I

ultraweak
strongly
weakly
⋮

Quick review to define notation

Concrete von Neumann algebras

Def 1 : (insert favorite topology here) closed $*$-algebra of $\mathcal{B}(\mathcal{H})$ with $\mathbb{1}$

von Neumann double commutant theorem

Def 2 : $M \subset \mathcal{B}(\mathcal{H})$ closed under involution such that $M = M''$

Abstract von Neumann algebra (Sakai '71) M a C^*-algebra with a predual M_*

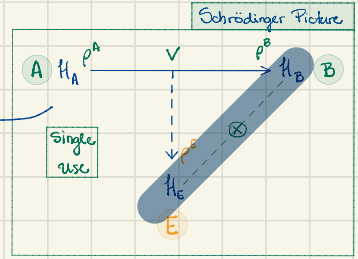
Factors : $\mathcal{Z}(M) = M \cap M' = \mathbb{C}\mathbb{1}$

classification → $\mathcal{B}(\mathcal{H})$

- type I
- type II
- type III

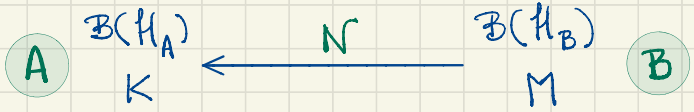
(Von Neumann '49) every von Neumann is isomorphic to a direct integral of factors

$$\mathcal{B}(\mathcal{H}_B \otimes \mathcal{H}_E) = \mathcal{B}(\mathcal{H}_B) \otimes \mathcal{B}(\mathcal{H}_E)$$



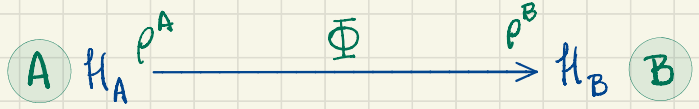
Beyond type I

Heisenberg Picture



Normal Unital Completely Positive map

Schrödinger Picture



Completely Positive Trace Preserving map

Abstract von Neumann algebra (Sakai '71)

M a C^*-algebra with a predual M_*

$N : M \to K$

$N_* : K_* \to M_*$

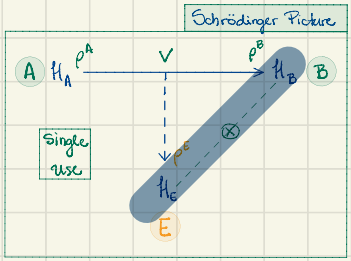
$\rho \mapsto \rho \circ N$

thm (Sherman '50, Takeda '54) Any C^*-algebra has a universal enveloping von Neumann algebra

Beyond type I

$\mathcal{B}$ and $\mathcal{E}$ mutually commuting von Neuman algebras

before: $\mathcal{B}(\mathcal{H}_B) \otimes \mathbb{1}$, $\mathbb{1} \otimes \mathcal{B}(\mathcal{H}_E)$



Will consider $\mathcal{E} \subset \mathcal{B}$ subfactors and that the communication between A and B is perfect and that A only ensemble states ρ such that $\rho = \rho \circ N$ (following Naaijkens '17)

Since $\mathcal{E} \subset \mathcal{B}$ subfactor, we have a notion of relative size: $[\mathcal{B} : \mathcal{E}]$ Jones index

Definition: • $\chi(\mathcal{E}) \doteq \sum_x{}' p_x S(\rho_x, \rho)$ where $\rho = \sum_x{}' p_x \rho_x$ and $S(\cdot,\cdot)$ is the relative entropy

↑ Holevo χ-quantity

↑ can be $+\infty$!

$$P(\$) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \left\{ \chi(\mathcal{E}_{\mathcal{B}^{(n)}}) - \chi(\mathcal{E}_{\mathcal{E}^{(n)}}) \right\}$$

• $S_{\mathcal{B}|\mathcal{E}}(\{p_x\}, \{\rho_x\}) \doteq \chi(\{p_x\}, \{\rho_x\}) - \chi(\{p_x\}, \{\rho_x|_{\mathcal{E}}\})$

restriction is a channel: $|_{\mathcal{E}} : \mathcal{B} \to \mathcal{E}$ is the adjoint of $i : \mathcal{E} \hookrightarrow \mathcal{B}$ (inclusion map)

Beyond type I

$$\chi(\mathcal{E}) \doteq \sum_x p_x S(\rho_x, \rho) \qquad \mathcal{E} = \{p_x, \rho_x\}_x$$

$$S_{B|E}(\{p_x\}, \{\rho_x\}) \doteq \chi(\{p_x\}, \{\rho_x\}) - \chi(\{p_x\}, \{\rho_x|_E\})$$

thm (Pimsner–Popa '86, Hiai '91)

If $E \subset B$ is irreducible (ie $E' \cap B = \mathbb{C}\mathbb{1}$), then

$$\sup_{\substack{\rho \circ N = \rho \\ \rho \text{ f.n.}}} \sup_{\mathcal{E}} \{ S_{B|E}(\mathcal{E}) \} = \log [B:E] \qquad \mathcal{E} = \{p_x, \rho_x\}_x$$

with $N : E \longrightarrow B$ the conditional expectation. And

$$\sup_{\rho \circ N^{\otimes n} = \rho} \sup_{\mathcal{E}^{(n)}} \{ S_{B|E}(\mathcal{E}^{(n)}) = n \log [B:E]$$

$\mathcal{E}^{(n)} = \{p_x^{(n)}, \rho_x^{(n)}\}$; $N^{\otimes n} = N \otimes N \otimes \cdots \otimes N : E^{\bar{\otimes} n} \longrightarrow B^{\bar{\otimes} n}$

$+$ (Longo '89) $\longrightarrow$ $[B^{\otimes n} : E^{\otimes n}] = [B:E]^n$

n copies of the channel

Theorem (Devetak '03, Cai–Winter–Yeung '04)

$$P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \{ \chi(\mathcal{E}_{\Phi^{(n)}}) - \chi(\mathcal{E}_{\Phi^{(n)}}) \}$$

$\mathcal{E} = \{p_x, \rho_x^{\Phi^{(n)}}\}$; $\mathcal{E}_{\Phi^{(n)}} = \{p_x, \Phi_B^{\otimes n}(\rho_x^{\Phi^{(n)}})\}$; $\mathcal{E}_{\Phi^{(n)}} = \{p_x, \Phi_E^{\otimes n}(\rho_x^{\Phi^{(n)}})\}$

$$\Rightarrow \quad P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \sup_{\mathcal{E}^{(n)}} S_{B|E}(\mathcal{E}^{(n)})$$

$+$ thm above $\longrightarrow$ <u>additivity</u> !

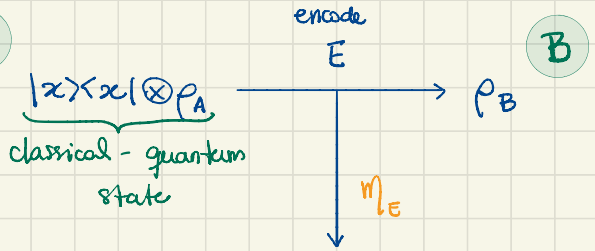
Beyond type I

- Many assumptions, definitely not general.
- Suggests that **Theorem** (Devetak '03, Cai – Winter – Yeung '04)
$$P(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\varepsilon} \{ \chi(\mathcal{E}_{\Phi^{\otimes n}}) - \chi(\mathcal{E}_{\Phi^{\otimes n}}) \}$$
cannot be extended.
- Highlights the difficulty of translate the wiretap model to more general von Neumann algebras.
- Suggests that there might be a class of channels which are additive

Maybe a different approach?

Private Subalgebras

M. Mosca et al. (2000)



Private Quantum Channel

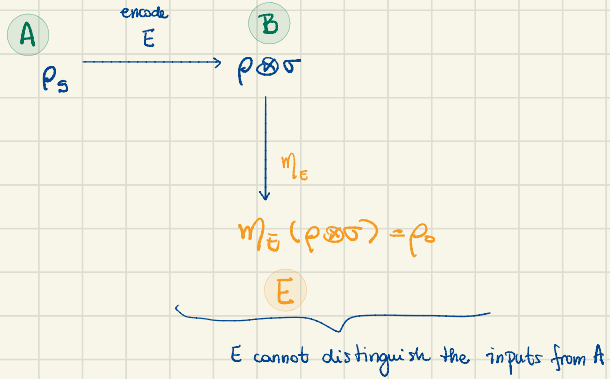
- encoder E has an inverse
- $\eta_E(E(\sigma_{xA})) = \rho_0 \quad \forall \sigma_{xA}$

$\eta_E(E(|x\rangle\langle x| \otimes \rho_A)) = \rho_0$ (fix)

E cannot distinguish the inputs from A

2. private spaces?

Private Subalgebras



S. D. Barlett et. al. (2004)

$E : \mathcal{H}_S \longrightarrow \mathcal{H}_A \otimes \mathcal{H}_{A'} \subset \mathcal{H}$, $\dim \mathcal{H}_S = \dim \mathcal{H}_A$ (ancilla space)

$\eta_E : \mathcal{H} \longrightarrow \mathcal{H}$

If for a fixed $\sigma \in \mathcal{H}_{A'}$, $\eta_E(\rho \otimes \sigma) = \rho_0 \ \forall \rho \in \mathcal{H}_A$ fixed $\rho_0 \in \mathcal{H}$

then the **subsystem** $\mathcal{H}_A$ is said to be **completely private** with respect to η_E

Moreover, if $\eta_E(\rho \otimes \sigma) = \frac{1}{d_A} \mathbb{1} \otimes \sigma'$ and σ' independent of ρ, then

$\mathcal{H}_A$ is said to be a **decoherence-full subsystem**.

Private Subalgebras

J. Crann et. al. (2015)

Given S a Hilbert space, M a von Neumann algebra, $\eta : M \to B(S)$, and P a projection in $\mathcal{P}(S)$.

We say that $N \subset B(PS)$ is **private** with respect to P if $C_P \circ \eta(M) \subset N'$ (where $C_P(\cdot) = P \cdot P^*$)

---

main References

Devetak '03 — arXiv: quant-ph/0304127

Cai-Winter-Yeung '04 — Probl. Inf. Transm 40, 318-336

Naaijkens '17 — arXiv: 1704.05562 [math-ph]

M. Mosca et. al. (2000) — arXiv: quant-ph/0003101

S.D. Barlett et. al. (2004) — arXiv: quant-ph/0403161

J. Crann et. al. (2015) — arXiv: 1510.06672 [quantum-ph]