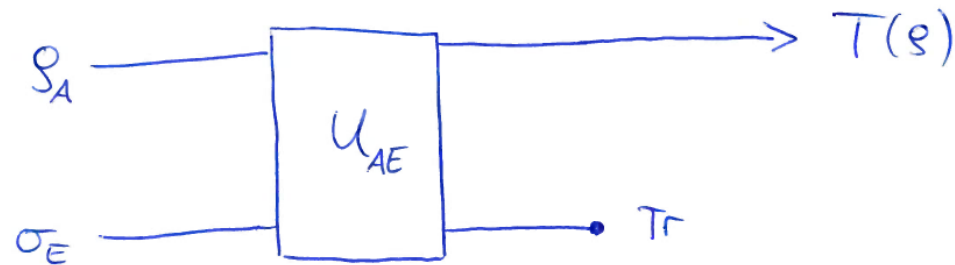


The mathematics of useless quantum channels

Alexander Müller-Hermes

Uio Math

Quantum channels: Model noise in open quantum systems



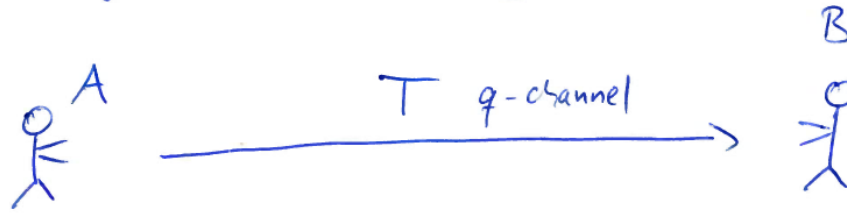
$$T(\rho) = \text{Tr}_E [U_{AE} (\rho \otimes \sigma_E) U_{AE}^\dagger]$$

for unitary evolution U_{AE} of system + environment.

Mathematically: $T: M_{d_A} \rightarrow M_{d_B}$ completely positive & trace-preserving

$\downarrow$
 $\text{id}_k \otimes T$ positive $\forall k$.

Quantum information processing:



Possible goals:

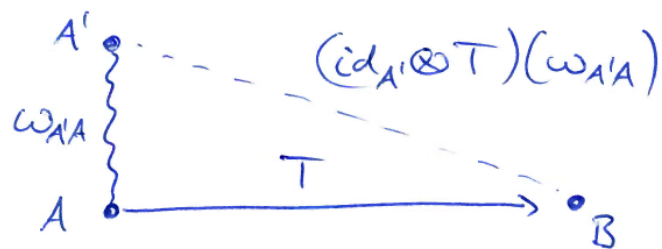
- (1) Share entanglement
- (2) Communicate qbits
- (3) Private communication
- ⋮ and more.

Which channels are
useless for these tasks?

What are their properties?

(1) Sharing entanglement

Easy strategy: Alice prepares maximally ent. state (EPR pair) $\omega_{A'A}$ and sends system A to Bob.



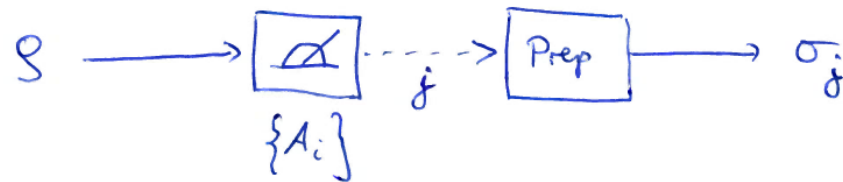
Entanglement breaking (EB) channels: Channels $T: M_{d_A} \rightarrow M_{d_B}$ s.t.
 $(id_{A'} \otimes T)(\omega_{A'A})$ separable.

Thm: No entanglement can be shared using EB channels.

Structure of EB channels

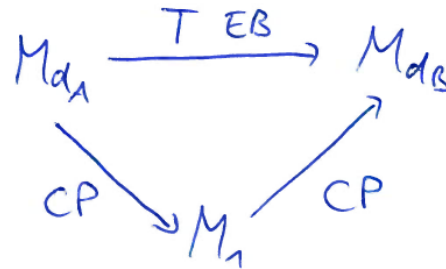
Holevo form : $T(\rho) = \sum_i \text{Tr} [A_i \rho] \sigma_i$

for POVM $\{A_i\}$ and q -states σ_i .



Measurement - prepare channel

Mathematical interpretation :



T factors through
a 1-dimensional system.

(2) Communication tasks



Goal: Using T multiple times, send a

- quantum bit $\rightsquigarrow$ quantum communication
- private bit $\rightsquigarrow$ private communication

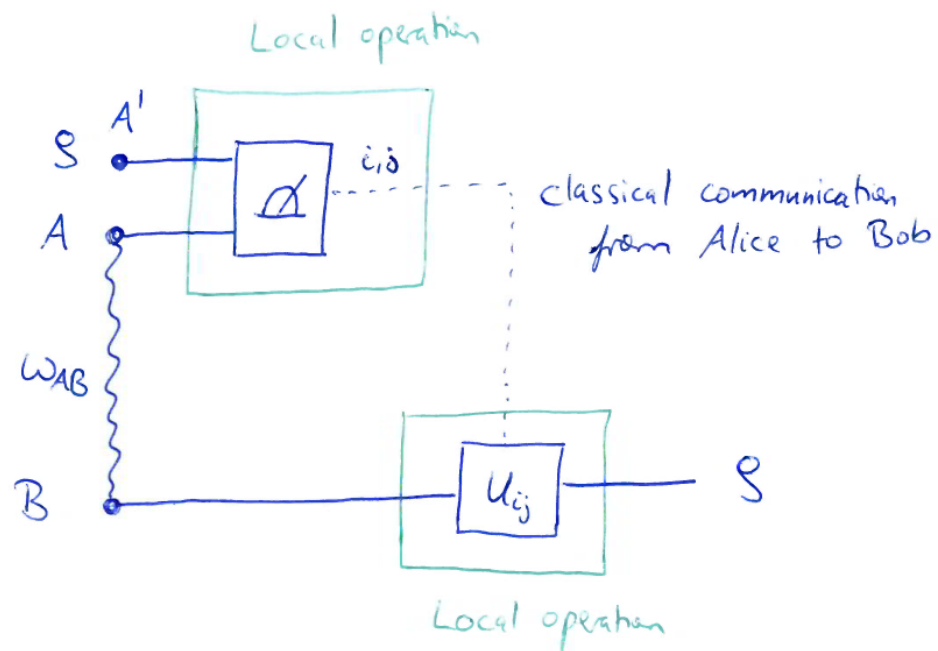
from Alice to Bob.

Common additional assumption: Alice and Bob may

- act locally on their own systems
- communicate classically

LOCC

Example: Teleportation protocol



With LOCC sharing maximally entangled state
is equivalent to being able to send a quantum system.

Equivalent formulation as state preparation



Define $\Delta_n^{AB}[T] = \left\{ \rho_{AB} \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^{d'}) : \begin{array}{l} d, d' \in \mathbb{N} \\ \rho_{AB} \text{ preparable using} \\ T \text{ } n\text{-times and} \\ \text{using LOCC} \end{array} \right\}$

Then: T is useful for q -communication / p -communication



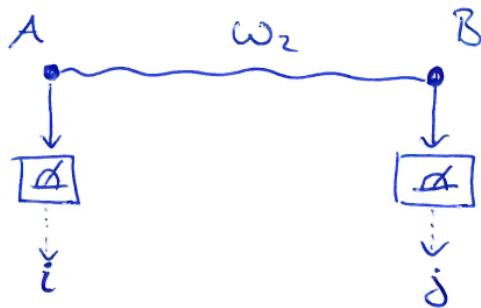
$\exists$ sequence $\rho^{(n)} \in \Delta_n^{AB}[T]$ s.t.

$\rho^{(n)} \longrightarrow \tau_{AB}$ as $n \rightarrow \infty$,

where τ_{AB} is EPR pair / private state.

Private states: Fundamental resource for q -cryptography

Easiest example: EPR pair $\omega_2 \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$



Assume Alice & Bob pick same measurement basis

- $i=j \rightsquigarrow$ perfectly correlated random bits (uniform)
- No other party can know these bits!
 $\rightsquigarrow$ since any extension of ω_2 (pure!) is product $\omega_2 \otimes \sigma_E$.
- One-time-pad $\Rightarrow$ Can send a private bit!

For which states does this work?

Private states:

$$\gamma_2^{ABA'B'} = U_{tw}^{ABA'B'} (\omega_2^{AB} \otimes \sigma_{A'B'}) (U_{tw}^{ABA'B'})^\dagger$$

for so-called twisting unitary

$$U_{tw}^{ABA'B'} = \sum_{ij} |v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j| \otimes U_{ij}^{A'B'}$$

Equivalent formulation as state preparation



Define $\Delta_n^{AB}[T] = \left\{ \rho_{AB} \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^{d'}) : \left. \begin{array}{l} d, d' \in \mathbb{N} \\ \rho_{AB} \text{ preparable using} \\ T \text{ } n\text{-times and} \\ \text{using LOCC} \end{array} \right\} \right\}$

Then: T is useful for q -communication / p -communication



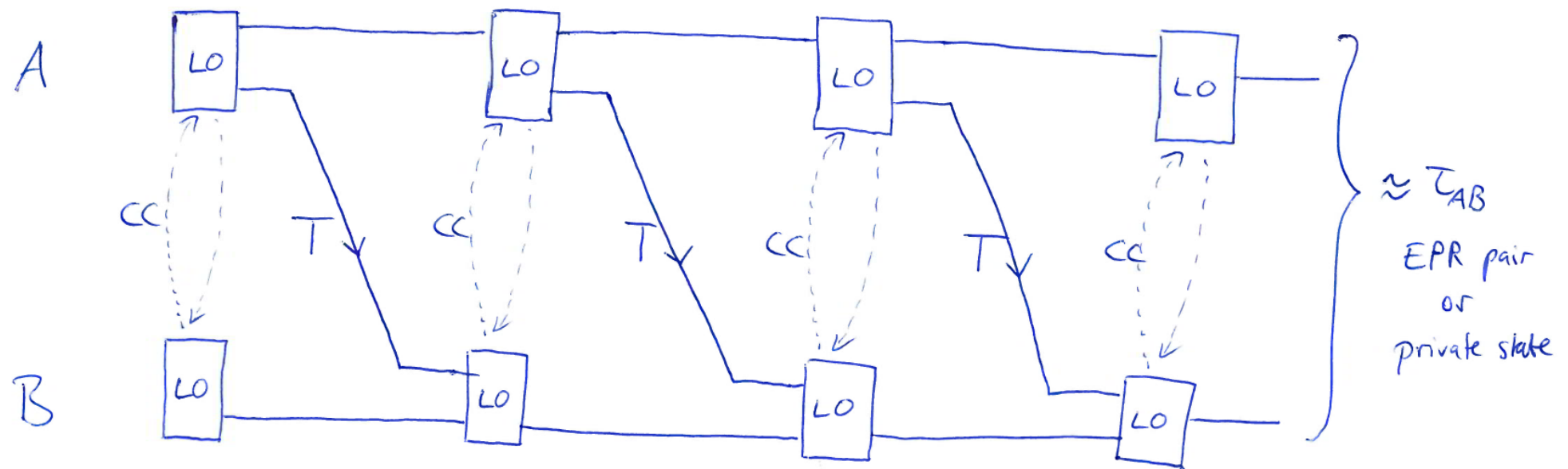
$\exists$ sequence $\rho^{(n)} \in \Delta_n^{AB}[T]$ s.t.

$\rho^{(n)} \longrightarrow \tau_{AB}$ as $n \rightarrow \infty$,

where τ_{AB} is EPR pair / private state.

Communication protocols assisted by LOCC

Schematic of a general protocol (using q -channel T three times) :



→ These protocols can involve feedback and are quite complicated !

Q-communication with LOCC assistance



Goal: Create ω_2 using LOCC and T multiple times.

PPT channels: $T: M_A \rightarrow M_B$ s.t. $\mathcal{U}_B \circ T$ is q -channel

$\leadsto$ Here $\mathcal{U}_A(X) = X^T$ is transpose map (not a q -channel!)

Thm: PPT channels are useless for q -communication.

Proof: If T is PPT, then we have

$$S_{AB}^\Gamma = (\text{id} \otimes \mathcal{U}_B)(S_{AB}) \geq 0$$

for any $S_{AB} \in \mathcal{L}_n^{AB}[T]$. But $\omega_2^\Gamma = \frac{1}{2}I_2 \not\geq 0$.

$\Rightarrow$ Cannot approximate ω_2 using $\mathcal{L}_n^{AB}[T]$

Remark: $EB \Rightarrow PPT$

but there are PPT channels $T: M_{d_A} \rightarrow M_{d_B}$
for $(d_A, d_B) \notin \{(2,2), (2,3), (3,2)\}$ that are not EB.



Open problem: Are there any other examples of useless channels for q -comm. under LOCC assist?

→ NPPT bound entanglement problem.

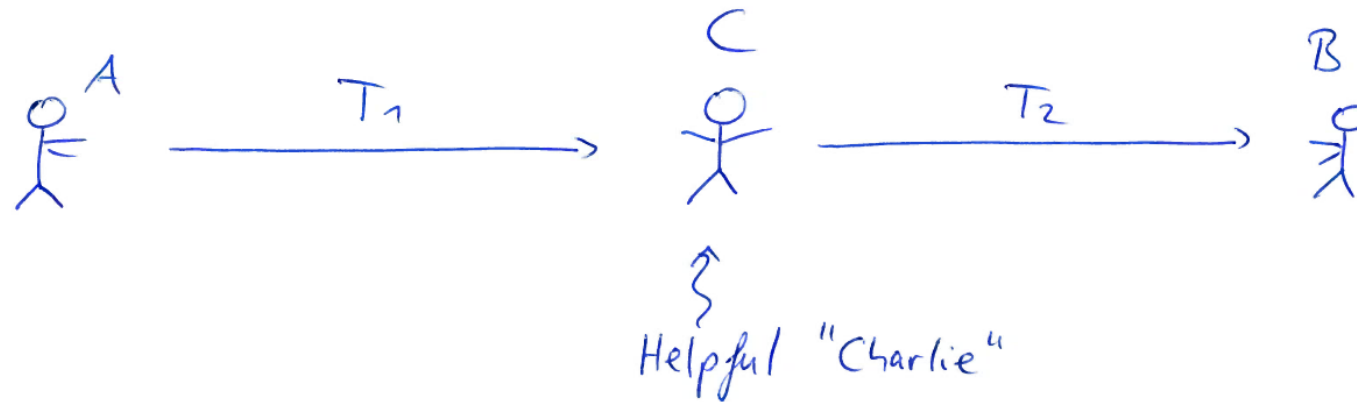
P-communication with LOCC assistance

Conjecture: Only EB channels are useless for private comm.

→ There are PPT channels allowing for private communication!

Q-channels can be useless for q-communication
but useful for private communication!

Communication over repeaters



Goals: (1) Share entanglement between Alice and Bob.

(2) Using LOCC (between all three parties) and T_1, T_2 multiple times generate (approx.)

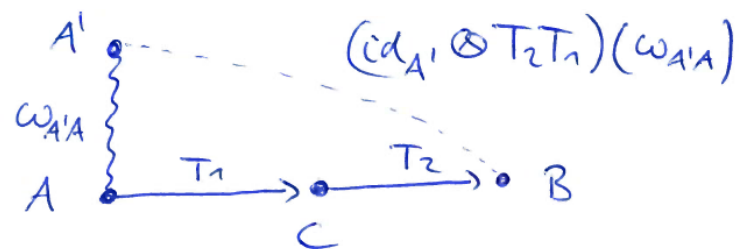
- EPR pair $\omega_2^{AB} \rightsquigarrow q$ -repeater

- Private state $\gamma_2^{ABA'B'} \rightsquigarrow$ key repeater

between Alice & Bob.

Sharing entanglement via repeaters

Strategy: Alice prepares maximally ent. state $\omega_{A'A}$ and sends system A to Charlie who sends it to Bob.



Conjecture (PPT² conjecture, Christandl 2012)

If T_1, T_2 PPT, then $T_2 T_1$ is EB.

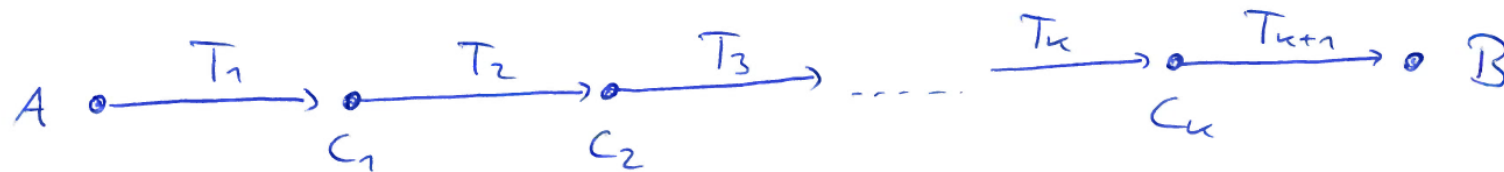
Thm: (Christandl, AMH, Wolf 2019)

$T_1, T_2 : M_3 \rightarrow M_3$ PPT, then $T_2 T_1$ is EB.

↑
First non-trivial case!

Sharing entanglement via repeater chains

More generally:



Question: When is composition $T_{k+1}T_k \dots T_1 \in \mathcal{EB}$?

Breaking entanglement with qubit:

T is called 2-EB if
 $(\text{id}_2 \otimes T)(\rho)$ separable
 for any $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^{d_A})$



Thm: (Christandl, AMH, Wolf 2019)
 Composition of $(d-1)$ 2-EB channels
 $T_i: M_d \rightarrow M_d$ is EB.

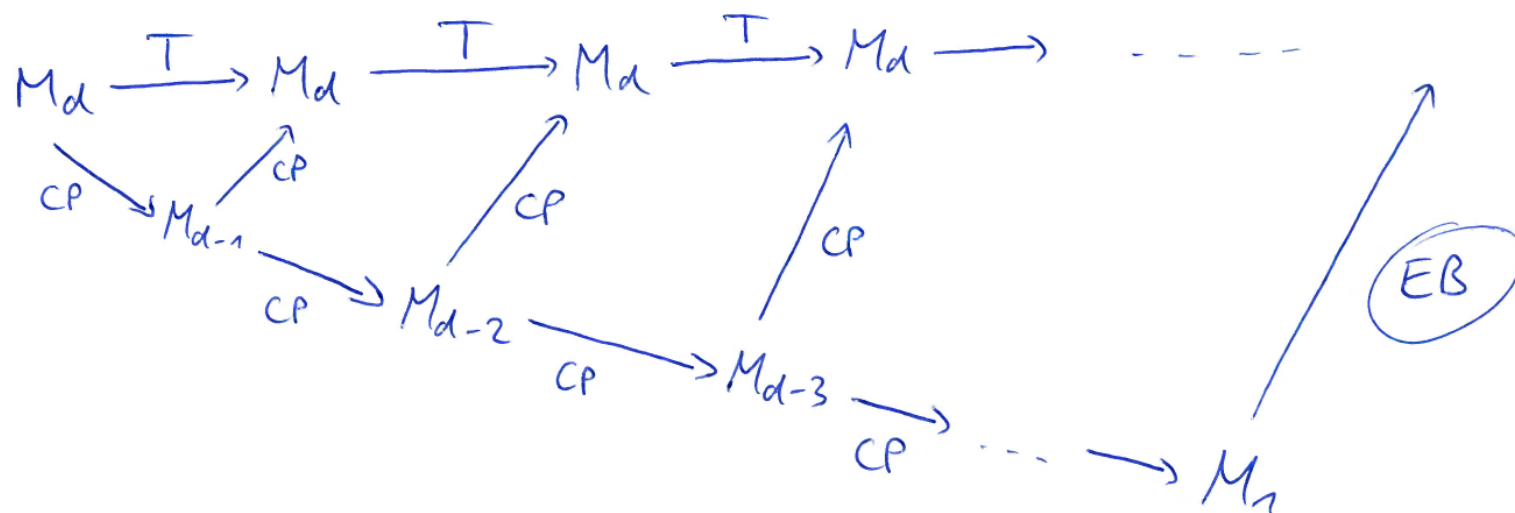
2-EB channels — Properties

Thm: (Christandl, AMH, Wolf 2019)

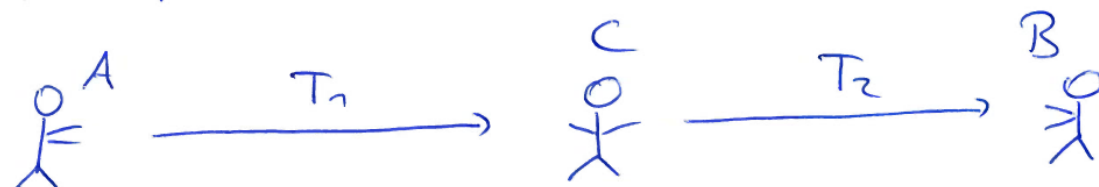
If $T: M_d \rightarrow M_d$ is 2-EB, then



This theorem can be iterated:



Key repeaters



Goal: Create private state between A and B
using T_1, T_2 multiple times and LOCC.

PPT^2 -conjecture $\implies$ T_1 and T_2 might allow for
private communication but together
they are useless in a key repeater.

Can we get this result
without relying on PPT^2 -conjecture?

More quantitative:

$P_{\leftrightarrow}(T)$: Supremum of achievable rates
for generating private states (pbits)
using LOCC & T

$\frac{\# \text{ private bits}}{\# \text{ channel uses}}$

$P_{A \leftrightarrow C \leftrightarrow B}(T_1, T_2)$: Analogous quantity
for repeater scenario.

Thm: (Christandl, AMH 2017)

There is q -channel $T_d: M_2 \otimes M_d \longrightarrow M_2 \otimes M_d$ s.t.

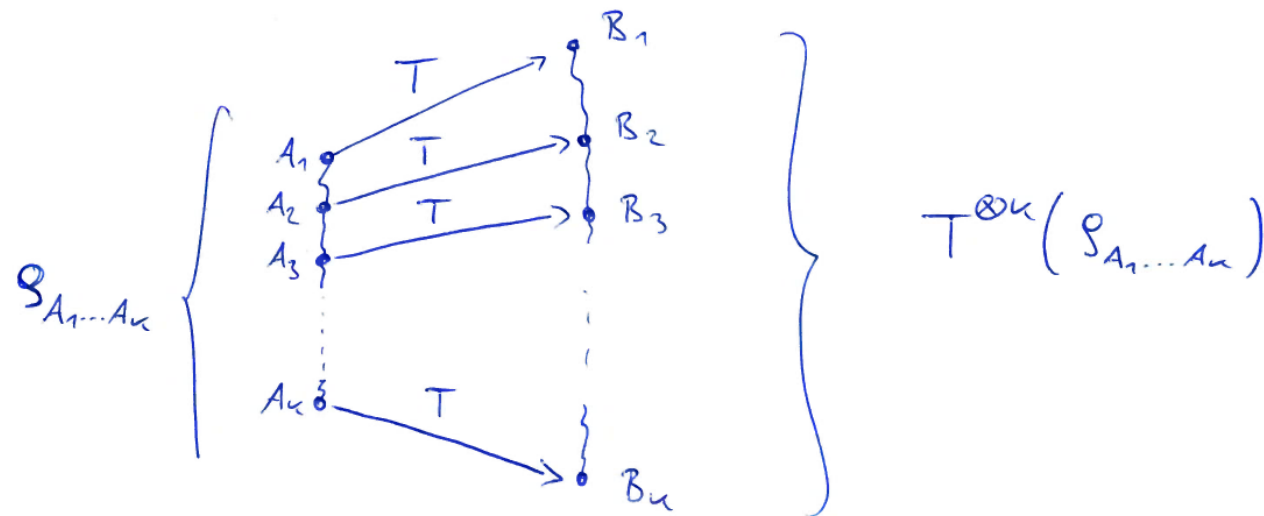
$$P_{\leftrightarrow}(T_d) \geq 1 - h_2\left(\frac{1}{\sqrt{d}+1}\right) \longrightarrow 1 \quad \text{as } d \rightarrow \infty.$$

but

$$P_{A \leftrightarrow C \leftrightarrow B}(T_d, T_d) \leq \log\left(1 + \frac{1}{\sqrt{d}+1}\right) \longrightarrow 0 \quad \text{as } d \rightarrow \infty.$$

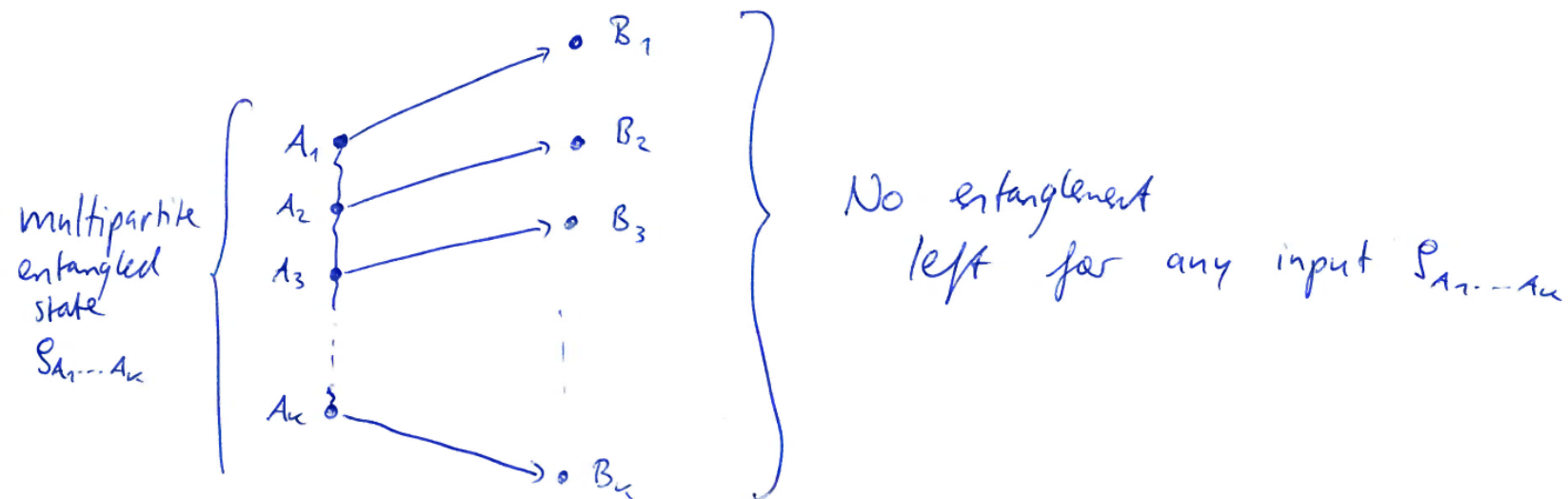
Multipartite entanglement sharing

Strategy: Alice prepares multipartite entangled state $\rho_{A_1 \dots A_k}$ and sends each system to one of the Bobs.



Challenge: No universal resource state (like EPR pair) for multipartite entanglement!

Useless channels for multipartite entanglement sharing



Clear: EB channels are useless!

Thm: (Aubrun, AMH 2023)

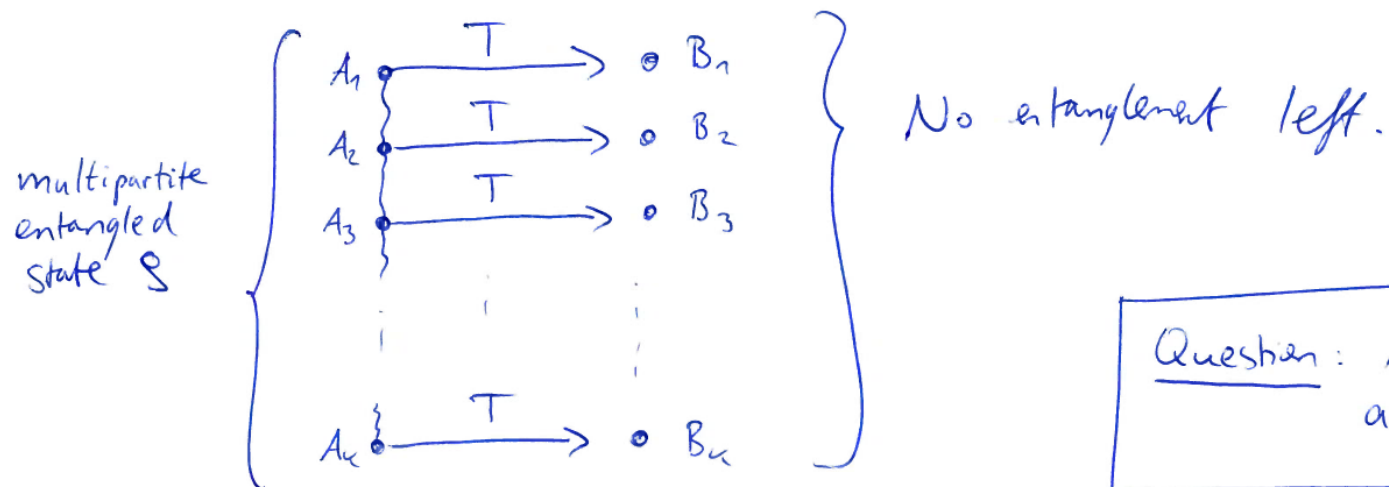
For any $k \in \mathbb{N}$, there are useless channels that are not EB.

~~~~~ What about  $k \rightarrow \infty$ ?

## Local vs. global uselessness

Quantum channel  $T: M_A \rightarrow M_B$  is entanglement annihilating (EA) if for any  $\rho \in D((\mathbb{C}^{d_A})^{\otimes K})$  for any  $K \in \mathbb{N}$  we have

$T^{\otimes K}(\rho)$  fully separable.



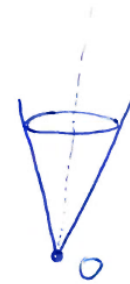
Question: Are EA channels always EB?

⋮  
If no, then this solves NPPT-bound ent. problem

& PPT<sup>2</sup>-conjecture.

Version of this question in ordered vector spaces

Proper cones:  $C_A \subseteq V_A$       e.g. PSD cones (quantum)  
 $C_B \subseteq V_B$       Lorentz cones  
 ⋮



Tensor products:  $C_A \otimes_{\min} C_B = \text{conv} \{ x \otimes y : x \in C_A, y \in C_B \}$   
 $\longrightarrow$  like separable states!

$$C_A \otimes_{\max} C_B = (C_A^* \otimes_{\min} C_B^*)^*$$

$\longrightarrow$  like entanglement witnesses!

$$C^* = \left\{ f: V \rightarrow \mathbb{R} : \begin{array}{l} f(x) \geq 0 \\ \forall x \in C \end{array} \right\}$$

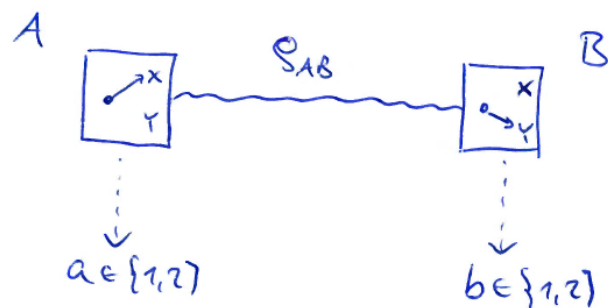
Question: EA:  $\bigcap_{\forall k} P^{\otimes k}(C_A^{\otimes_{\max} k}) \subseteq C_B^{\otimes_{\min} k}$       vs.      EB:  $P = \sum_i \gamma_i \alpha_i$   
 $\alpha_i \in C_A^*$   
 $\gamma_i \in \mathbb{R}_0$

# Why study ordered vector spaces?

Motivation for physicists: Nonlocality

Pair of 2-outcome POVMs:  $X = \{X_1, X_2\}$   $X_1, X_2 \geq 0, X_1 + X_2 = \mathbb{1}$   
 $Y = \{Y_1, Y_2\}$   $Y_1, Y_2 \geq 0, Y_1 + Y_2 = \mathbb{1}$

Typical setup:



Correlation:  $P(a, b \mid \text{Settings})$

↳ How to understand those?

## Formulation in language of ordered vector spaces

POVMs

$$X = \{X_1, X_2\} \quad X_1, X_2 \geq 0, \quad X_1 + X_2 = \mathbb{1}$$

$$Y = \{Y_1, Y_2\} \quad Y_1, Y_2 \geq 0, \quad Y_1 + Y_2 = \mathbb{1}$$

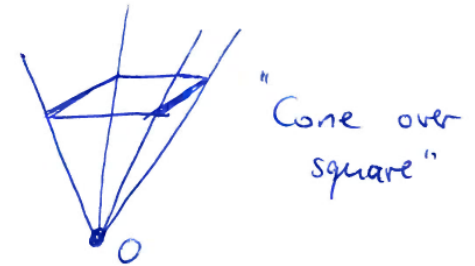
Define:

$$E_x = X_1 - X_2 \quad \text{and linear map} \quad \begin{cases} P: M_d \rightarrow \mathbb{R}^3 \\ P(\rho) = \begin{pmatrix} \text{Tr}[\rho] \\ \text{Tr}[E_x \rho] \\ \text{Tr}[E_y \rho] \end{pmatrix} \end{cases}$$

$$E_y = Y_1 - Y_2$$

Map  $P$  captures the pair of POVMs.

Note:  $P(M_d^+) \subseteq C_{\ell_\infty^2} = \left\{ (t, x, y) : \begin{matrix} |x| \leq t \\ |y| \leq t \end{matrix} \right\}$



Correlations correspond to  $(P \otimes P)(\rho_{AB}) \in C_{\ell_\infty^2} \otimes_{\max} C_{\ell_\infty^2}$

## EA vs. EB

We have the following correspondences:

$$C_{\ell_\infty}^2 \otimes_{\max} C_{\ell_\infty}^2 \quad \longleftrightarrow \quad \text{non-signalling correlations}$$

$$C_{\ell_\infty}^2 \otimes_{\min} C_{\ell_\infty}^2 \quad \longleftrightarrow \quad \text{local correlations}$$

EA:  $P^{\otimes k}((M_d^+)^{\otimes_{\max} k}) \subseteq C_{\ell_\infty}^2{}^{\otimes_{\min} k}$  "all multipartite correlations local"  
for any  $k \in \mathbb{N}$

EB:  $P$  is EB iff POVMs  $X, Y$  are jointly measurable.

Question: If POVMs  $X, Y$  are not jointly measurable, can they be used to generate multipartite correlations?

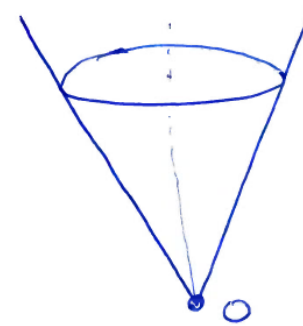
## Partial results:

Thm: (Aubrun, AMH, 2023)

If  $C_A$  or  $C_B$  is Lorentz cone  
then  
 $EA(C_A, C_B) = EB(C_A, C_B)$

Lorentz cones

$$L_n = \{(t, x) : \|x\|_2 \leq t\} \subseteq \mathbb{R}^{n+1}$$



Consequence: Any EA map  $T: M_d \rightarrow M_d$   
breaks entanglement with all Lorentz cones

$$(\text{id}_{n+1} \otimes T)(L_n \otimes_{\max} M_d^+) \subseteq L_n \otimes_{\min} M_d^+$$

for any  $n \in \mathbb{N}$ .

$\leadsto$  In particular, they break entanglement with qubits!

$\Rightarrow$  If  $T: M_d \rightarrow M_d$  is EA channel,  
then  $T^{d-1}$  is EB

---

Thank you for your attention!

Are there any questions?

