12th lecture, 10/11/2023

Reminder: we talked about CP maps.

- We say that a linear operator $\rho \in B(\mathcal{H})$ is positive iff $\langle\varphi|\rho|\varphi\rangle \geq 0 \ \forall \ |\varphi\rangle \in \mathcal{H}$.
- We say that a linear operater $T : B(\mathcal{H}) \to B(\mathcal{K})$ is positive/positivity preserving if
$$T(\rho) \geq 0 \quad \forall \rho \geq 0.$$
- We say that $T : B(\mathcal{H}) \to B(\mathcal{K})$ is CP if $\forall \ \mathcal{H}'$ Hilb-space
$$(T \otimes id_{\mathcal{H}'})(\rho) \geq 0 \quad \forall \rho \in B(\mathcal{H}) \otimes B(\mathcal{H}'), \ \rho \geq 0.$$
- We have seen that CP maps are exactly the ones that admit Kraus representation,
$$T(\rho) = \sum_i A_i \rho A_i^{+}.$$
- We can check whether T is CP: enough $\mathcal{H}' = \mathcal{H}$, and $\rho = |\Omega\rangle\langle\Omega|$, $|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_i |ii\rangle$:
T is CP iff $(T \otimes id)(|\Omega\rangle\langle\Omega|) \geq 0$.
(Choi-Jamiolkowsky)

We have also seen that

- $\forall$ CP maps are positive
- there are positive, not CP map.

Eg: Transposition is positive, but

$$(T\otimes id)(|\Omega\rangle\langle\Omega|) \ngeq 0.$$

Entanglement

Consider a composite system $\mathcal{H}_A\otimes\mathcal{H}_B$.

Thm Consider density matrices $\rho_i\in S(\mathcal{H}_A)$, $\eta_i\in S(\mathcal{H}_B)$, and a probability distribution p.

Then

$$\rho = \sum_i p_i\, \rho_i\otimes\eta_i \in B(\mathcal{H}_A)\otimes B(\mathcal{H}_B)$$

is a density matrix.

Proof: As $\rho_i\geq 0$, we can write $\rho_i = X_i^\dagger X_i$.
As $\eta_i\geq 0$, we can write $\eta_i = Y_i^\dagger Y_i$.

Then

$$\rho = \sum_i \left(\sqrt{p_i}\, X_i^\dagger\otimes Y_i^\dagger\right)\cdot\left(\sqrt{p_i}\, X_i\otimes Y_i\right)$$

and thus, if $Z = \sum_i \sqrt{p_i}\, |i\rangle \otimes X_i \otimes Y_i$,

$Z \in B(\mathcal{H}) \otimes B(\mathcal{H}) \otimes \mathbb{C}^n$, or equivalently,

$$Z = \begin{pmatrix} \sqrt{p_1}\, X_1 \otimes Y_1 \\ \sqrt{p_2}\, X_2 \otimes Y_2 \\ \vdots \\ \sqrt{p_n}\, X_n \otimes Y_n \end{pmatrix}, \quad \text{then}$$

$$Z^\dagger Z = \left(\sqrt{p_1}\, X_1^\dagger \otimes Y_1^\dagger,\ \sqrt{p_2}\, X_2^\dagger \otimes Y_2^\dagger, \dots \right) \begin{pmatrix} \sqrt{p_1}\, X_1 \otimes Y_1 \\ \vdots \\ \sqrt{p_n}\, X_n \otimes Y_n \end{pmatrix} =$$

$$= \sum_i p_i\, X_i^\dagger X_i \otimes Y_i^\dagger Y_i = \rho. \qquad \square$$

That is, the convex combination of tensor product of density matrices is a density matrix.

<u>Thm</u>: Not every density matrix in $B(\mathcal{H}_A) \otimes B(\mathcal{H}_B)$ is of this form.

<u>Proof</u>: Proof by contradiction.

Take a positive, but not CP map (e.g. transposition). Then $\exists\, \rho \in B(\mathcal{H}) \otimes B(\mathcal{H})$ s.t.

$(T \otimes id)(\rho)$ is not positive, e.g. $\rho = |\Omega\rangle\langle\Omega|$.

If $\rho = \sum_i p_i\, \eta_i \otimes \nu_i$, w/ $p_i, \eta_i, \nu_i \geq 0$, then

$$(T\otimes \mathrm{id})(\rho) = \sum_i p_i \, T(\eta_i) \otimes \nu_i \geq 0 \; \lightning .$$

$\square$

<u>Def</u>: A density matrix $\rho \in B(\mathcal{H}) \otimes B(\mathcal{K})$ that can be written as

$$\rho = \sum_i p_i \, \eta_i \otimes \nu_i \quad \text{w/ } p_i \geq 0, \; \eta_i \geq 0, \; \eta_i \geq 0$$

is called <u>separable</u>. A density matrix that cannot be written in this form is called <u>entangled</u>.

For example, $|\Omega\rangle\langle\Omega|$ (or simply $|\Omega\rangle$) is entangled.

What does entangled mean?
Let ρ be entangled, try to write

$$\rho = \sum_i \lambda_i X_i \otimes Y_i .$$

Then $\exists i$ s.t. either $\lambda_i \not\geq 0$, $X_i \not\geq 0$ or $Y_i \not\geq 0$.
For separable, there is a decomposition w/ all positive.
Ofc, not <u>all</u> decomp. are such.

Entanglement theory is the study of entangled states. What really sets q. mecha apart from classical proba theory is precisely the presence of entanglement. So questions in entanglement theory are

- How non-classical these states are?
- What can we do with them?
  Non-classical $\Rightarrow$ we can do something more with them, can be used as resource.
- Can we quantify entanglement?
- Are there different "types" of entanglement?
- How can we manipulate these states?
- Pure state entanglement vs mixed state entanglement?

We have seen one example for entangled states: $|\Omega\rangle = \frac{1}{\sqrt{d}}\sum_i |i\,i\rangle$. This is pure.
In fact, there are many. How to check is ρ is entangled? For pure states, it's easy:

<u>Thm</u> A pure state $|\psi\rangle \in \mathcal{H}\otimes\mathcal{K}$ is entangled iff it is not a product state.

<u>Proof</u>: if it is a product state:

$$|\psi\rangle = |\varphi\rangle \otimes |\eta\rangle \Rightarrow |\psi\rangle\langle\psi| = |\varphi\rangle\langle\varphi| \otimes |\eta\rangle\langle\eta|,$$

it is a (trivial) convex comb. of elementary tensor products w/ each comp being positive.
Conversely, if

$$|\psi\rangle\langle\psi| = \sum_i \lambda_i \, \rho_i \otimes \eta_i$$

Then, as $|\psi\rangle\langle\psi|$ is pure, i.e. extremal, this convex comb. is trivial, i.e.

$$|\psi\rangle\langle\psi| = \rho\otimes\eta \quad \text{w/ } \rho \geq 0 \text{ and } \eta \geq 0.$$

There is a basis vector $|ij\rangle$ s.t. $\langle\psi|ij\rangle \neq 0$.
For such $|ij\rangle$,

$|\psi\rangle\langle\psi|ij\rangle = \rho|i\rangle \otimes \eta|j\rangle$, and thus, as $\langle\psi|ij\rangle\neq 0$, $|\psi\rangle$ is an elementary tensor product. $\square$

Sometimes it is not evident whether a pure state is product or not.

How to check?

(1) $|\psi\rangle = |\varphi\rangle \otimes |\chi\rangle$ iff

$$\sum_{ij} \psi_{ij} |ij\rangle = |\psi\rangle = |\varphi \otimes \chi\rangle = \sum_{ij} \varphi_i \chi_j |ij\rangle,$$

i.e. if the matrix $(\psi_{ij})_{ij}$ is rank-one.

(2) $|\psi\rangle\langle\psi| = |\varphi\rangle\langle\varphi| \otimes |\chi\rangle\langle\chi|$ iff the reduced densities are rank-one.

Remember: spectrum of ρ_A is the same as spectrum of ρ_B, so checking 1 of them is enough.

What about mixed states?

Have to check that

$$\rho = \sum_i p_i \, \eta_i \otimes \nu_i \quad \text{with } p_i \geq 0, \eta_i \geq 0, \nu_i \geq 0 \text{ holds.}$$

This is a difficult task: NP-hard in the dim. of the space.

What can we do? For example, exactly what we have done before: find T positive but not CP, then hope that

$$(T \otimes \mathrm{id})(\rho) \ngeq 0.$$

<u>Thm:</u> More precisely, if $(T \otimes \mathrm{id})(\rho) \ngeq 0$ for some T positive, ρ density matrix, then ρ is <u>entangled</u>.

<u>Proof</u>: If ρ is separable,

$$\rho = \sum_i p_i \, \eta_i \otimes \nu_i \quad \text{for } p_i \geq 0, \eta_i \geq 0, \nu_i \geq 0,$$

Then

$$(T \otimes \mathrm{id})(\rho) = \sum_i p_i \, T(\eta_i) \otimes \nu_i \geq 0$$

as well, as T is positivity preserving.

Example: T = transpose: positive partial transpose (PPT) criterion for deciding whether a state is separable or entangled.

Ex. #2:

$$\rho = \lambda |\Omega\rangle\langle\Omega| + (1-\lambda)\frac{1}{d^2}\,\mathbb{1}\otimes\mathbb{1}$$

$$\rho = \lambda \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix} + (1-\lambda)\begin{pmatrix} \frac{1}{4} & & & \\ & \frac{1}{4} & & \\ & & \frac{1}{4} & \\ & & & \frac{1}{4} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1+\lambda}{4} & & & \frac{\lambda}{2} \\ & \frac{1-\lambda}{4} & & \\ & & \frac{1-\lambda}{4} & \\ \frac{\lambda}{2} & & & \frac{1+\lambda}{4} \end{pmatrix}$$

$$(T\otimes id)(\rho) = \begin{pmatrix} \frac{1+\lambda}{4} & & & \\ & \frac{1-\lambda}{4} & \frac{\lambda}{2} & \\ & \frac{\lambda}{2} & \frac{1-\lambda}{4} & \\ & & & \frac{1+\lambda}{4} \end{pmatrix}$$

When is this positive?

iff $\left(\frac{1-\lambda}{4}\right)^2 \geq \frac{\lambda^2}{4}$ and $\frac{1+\lambda}{4} \geq 0$ and $\frac{1-\lambda}{4} \geq 0$

- $1-2\lambda+\lambda^2 \geq 4\lambda^2 \iff 1-2\lambda-3\lambda^2 \geq 0 \Rightarrow \lambda \in [-1, \frac{1}{3}]$
- $1+\lambda \geq 0 \Rightarrow \lambda \geq -1$
- $1-\lambda \geq 0 \Rightarrow \lambda \leq 1$

So if $\lambda \in (\frac{1}{3}, 1]$, then ρ is entangled.

Thm (w/o proof): the PPT criterion detects all entangled states in $(d_A, d_B) = (2,2)$ and $(3,2)$:

ρ is entangled iff $(T \otimes id)(\rho) \not\geq 0$.

There are counterexamples for 3×3, 4×2 systems.

<u>Another example for positive but not CP map:</u>

$T(\rho) = tr(\rho) \cdot \mathbb{1} - \rho$

$T(\rho)$ is <u>not</u> TP.

$T(\rho) \geq 0$ as $tr(\rho) . \mathbb{1} \geq \lambda_{max} \mathbb{1}$

$\rho \leq \lambda_{max} \mathbb{1}$.

One can try to detect entanglement w/

$(T \otimes id)(\rho_{AB}) = \mathbb{1} \otimes tr_A \rho_{AB} - \rho_{AB}$

This is the "reduction criterion":

$\mathbb{1} \otimes tr_A \rho_{AB} - \rho_{AB} \not\geq 0 \Rightarrow \rho_{AB}$ entangled.

* Positive map → Witness
* Physical importance
* Nice picture

* CHSH, meaning of entanglement
* LOCC,
* Entropy
* Teleportation, dense coding
* QKD

13th lecture : 13/11/2023

Recap:

* Entanglement: $\rho \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$ density matrix

  If $\rho = \sum_i p_i \eta_i \otimes \nu_i$ w/ $p_i \geq 0$, $\eta_i \geq 0$, $\nu_i \geq 0$, then ρ is separable. Otherwise it is entangled.

* Pure state is separable iff it is a product state. Entangled otherwise.

* Detecting entanglement: through a positive, but not CP map.

  → Positive: $T(\rho) \geq 0$ if $\rho \geq 0$.

  → CP: $(T \otimes id)(\rho_{AB}) \geq 0$ if $\rho_{AB} \geq 0$

  If we find positive but not CP s.t.

  $$(T \otimes id)(\rho_{AB}) \ngeq 0 \Rightarrow \rho_{AB} \text{ is entangled.}$$

In lab it's still hard to check. We want measurement that detects entanglement.

Entanglement witnesses

W is entanglement witness iff

(1) $W = W^\dagger$

(2) $\mathrm{tr}(\rho W) \geq 0 \;\; \forall \rho$ separable.

(3) But W is not positive.

Remark: W is a physical observable, can be measured. It can detect entanglement:

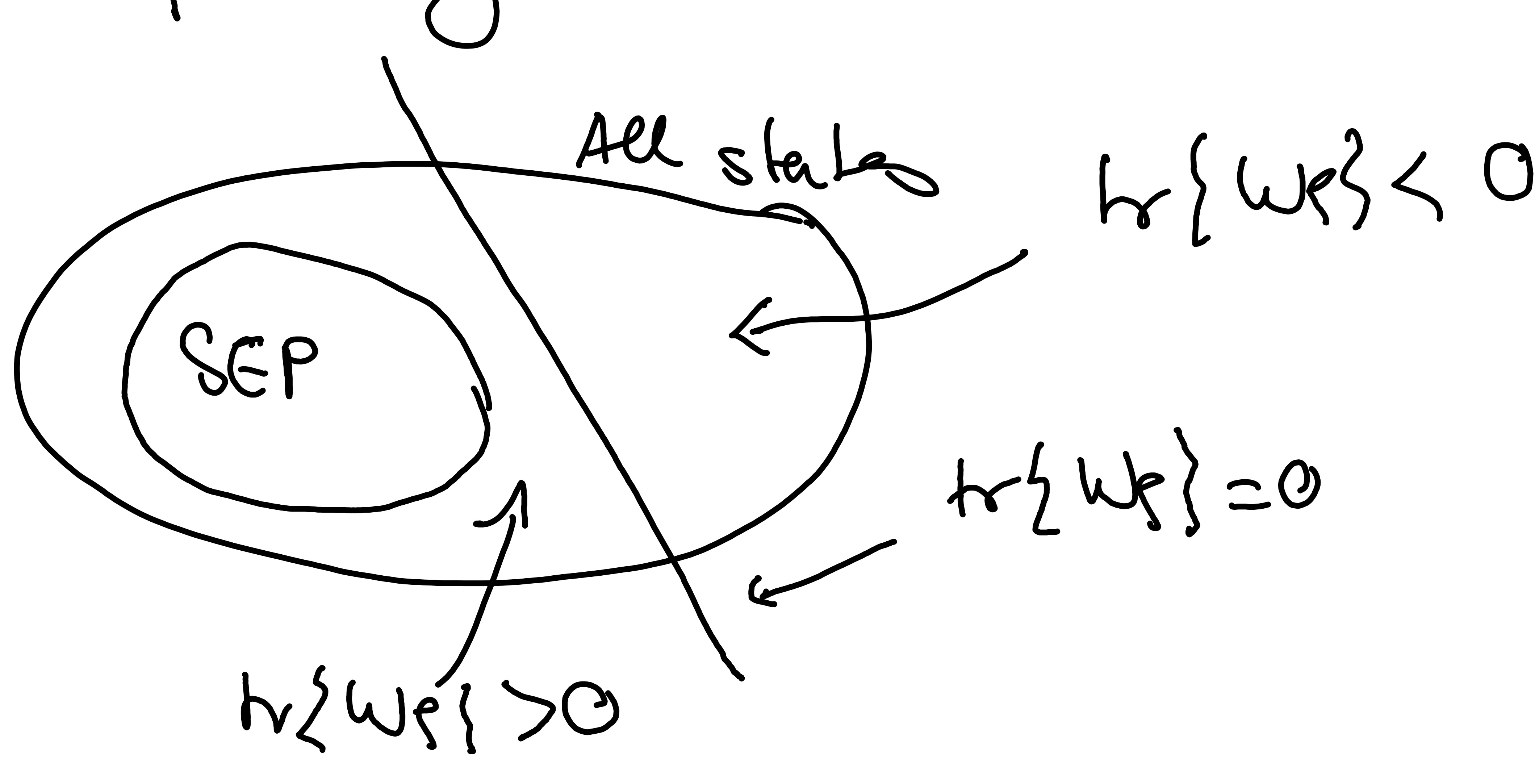
$$\mathrm{tr}\{W\rho\} = \langle W \rangle < 0 \Rightarrow \rho \text{ is entangled.}$$

Remark #2: As W is not positive, it detects some entanglement: $\exists\, |\psi\rangle$ s.t.

$$0 > \langle \psi | \rho | \psi \rangle = \mathrm{tr}\{W |\psi\rangle\langle\psi|\} \Rightarrow |\psi\rangle \text{ is entangled.}$$

Remark #3: The set $\{\rho \,|\, \mathrm{tr}\{W\rho\} = 0\}$ is a hyperplane.

Graphically:



Do entanglement witnesses exist at all?

Choi-Jamiolkowski isomorphism:

$W \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$ and $T: \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$

are in 1-to-1 correspondence through

$$W = (T \otimes id)(|\Omega\rangle\langle\Omega|)$$

<u>Thm</u>: W is ent. witness iff T is positive, but not CP.

<u>Proof</u>:

* We know: $W \geq 0$ iff T is CP, i.e.

  W is <u>not</u> positive iff T is <u>not</u> CP.

* We will show:

  $tr(\rho W) \geq 0 \; \forall \rho \Leftrightarrow T$ positive $\Rightarrow W = W^+$.

  This will finish the proof.

Let us show: T positive $\Rightarrow W = W^+$.

Note: T positive $\Rightarrow T(X^+) = T(X)^+$ $\boxed{HW}$

(any matrix can be expressed as lin. comb. of positive matrices)

Therefore if $T(X^\dagger) = T(X)^\dagger$, then

$$W^\dagger = \left(\sum_{ij} T(|i\rangle\langle j|) \otimes |i\rangle\langle j|\right)^\dagger = \sum_{ij} T(|i\rangle\langle j|)^\dagger \otimes |j\rangle\langle i| =$$

$$= \sum_{ij} T(|j\rangle\langle i|) \otimes |j\rangle\langle i| = W.$$

Finally, let us show T positive iff

$tr\{\rho W\} \geq 0 \ \forall \rho$ sep.

$\boxed{\Rightarrow}$ Let T be positive, ρ sep. Calculate

$tr\{\rho W\}$.

Remember: as $(\mathbb{1}\otimes X)|\Omega\rangle = (X^T \otimes \mathbb{1})|\Omega\rangle$,

we have

$$T(X^T) = tr_B\{(\mathbb{1}\otimes X)W\}$$

ρ is separable iff $\rho = \sum_i \eta_i \otimes \nu_i$ w/ $\eta_i \geq 0$, $\nu_i \geq 0$

$$tr\{\rho W\} = \sum_i tr\{\eta_i \otimes \nu_i W\} =$$

$$= \sum_i tr\{\eta_i \, tr_B((\mathbb{1}\otimes\nu_i)W)\}$$

$$= \sum_i tr\{\eta_i T(\nu_i^T)\} \geq 0.$$

$\boxed{\Leftarrow}$ If $\mathrm{tr}\{W\rho\} \geq 0 \ \forall \rho$ sep, then

$$\mathrm{tr}\{(|\psi\rangle\langle\psi| \otimes \nu^T)\, W\} = \langle\psi|T(\nu)|\psi\rangle \geq 0$$

$\forall \nu \geq 0, |\psi\rangle$. This means that $T(\nu)$ is positive $\forall \nu \geq 0 \Rightarrow T$ is positive.

$\square$

Thm: Every ent. state can be detected by a suitable witness.

Proof: $\boxed{\text{Homework}}$ The witness that works is constructed the following way.

Let η be the ent. state we want to detect, and let

$$\eta_0 := \underset{\rho \in SEP}{\mathrm{argmax}}\ \mathrm{tr}\{\rho\eta\}.$$

Then

$$W = \mathrm{tr}\{\eta\eta_0\}\mathbb{1} - \eta.$$

CHSH inequality

→ Seen what is entanglement

→ How to detect it

Let us understand now that it is different than classical proba theory.

<u>Game</u>: Alice, Bob, Charlie

$$\begin{tikzcd} & \text{Charlie} \arrow[dl, "x"'] \arrow[dr, "y"] & \\ A \arrow[dr, "a"'] & & B \arrow[dl, "b"] \\ & C & \end{tikzcd}$$

$$a \oplus b \stackrel{?}{=} x \wedge y$$

- x, y: indep. uniform random bits
- A, B: A sees x, replies bit a
  B sees y, replies bit b
- C: checks whether $a \oplus b = x \wedge y$. If yes, A & B wins.

During the game, A & B can't communicate. They can, however, can talk of a strategy beforehand, they can do things probabilistically.

Let E be the exp. value of the game (w/ win = +1, loose = −1):

$$E = \text{proba}(\text{win}) - \text{proba}(\text{loose}).$$

<u>Statement</u>: If A & B can share an entangled quantum state beforehand and are allowed to do local operations on it, then they can do better than any classical strategy:

max proba to win w/ classical strategy: 75%
max proba to win w/ quantum strategy: ~85%

<u>Interpretation 1</u>: entanglement can be used as a resource, quantum mecha allows for things that classical probability theory does not.

<u>Remark</u>: We need <u>multiple</u> parties!

Single-party QM is not special, the extra power arises from the tensor product structure!

Interpretation #2 : The optimal quantum outcome cannot be explained by classical theories (Local Hidden Variable models), thus, if we can create experiment s.t. A & B are guaranteed not to communicate (simply because they don't have time), then, if they win w/ > 75%, then we can conclude that our world is quantum. Such experiments were made.

Analysis of the game, general framework

$$\begin{tikzcd} & C \arrow[dl, "x"'] \arrow[dr, "y"] & \\ A \arrow[dr, "a"'] & & B \arrow[dl, "b"] \\ & a+b=xy\,? & \end{tikzcd}$$

<u>Note</u>: addition is mod 2, $a, b, x, y \in \{0,1\}$.

Whatever happens (even if A & B can communicate): we want to understand

$p(a,b|x,y)$: proba answers a,b given x,y.

This describes a strategy.

Our requirement: they can't communicate.

Classically: first guess:

$$P(a,b|x,y) = P_A(a|x)\, P_B(b|y)$$

But they could equally decide to toss a coin beforehand, and have a strategy where their reply depends on the coin toss:

$$p(a,b|x,y) = \sum_\lambda P_A(a|x,\lambda)\, P_B(b|y,\lambda)\, q(\lambda)$$

Here, λ: coin toss beforehand / Hidden Variable.

Def: Value of the game: win: +1, loose: −1, simply best exp. value achievable.

For this game:

$$E = \sum_{\substack{a,b \\ x,y}} (-1)^{a+b+xy} \, p(a,b|x,y)$$

0 if $a+b=xy$.
1 if $a+b \neq xy$.

For classical:

$$p(a,b|x,y) = \sum_{\lambda} p(a|x,\lambda)\, p(b|x,\lambda) \cdot q(\lambda)$$

For quantum:

$$p(a,b|x,y) = \left\| \left(M_{a,x} \otimes N_{b,y} \right) |\phi\rangle \right\|^2$$

Where: $M_{a,x} / N_{b,y}$ are meas. depending on x (resp. y),

$$\sum_a M_{a,x}^{+} M_{a,x} = \mathbb{1} \quad \forall x$$

$$\sum_b N_{a,y}^{+} N_{b,y} = \mathbb{1} \quad \forall y$$

and $|\phi\rangle$ is a shared quantum state.

LHV analysis:

$$E = \sum_{\substack{ab\\xy}} (-1)^{a+b+xy} \, p(a,b|x,y)$$

$$= \sum_{xy} (-1)^{xy} \sum_{a,b} (-1)^{a+b} \, p(a,b|x,y)$$

$$\underset{\text{LHV}}{=} \sum_{xy} (-1)^{xy} \sum_{\substack{a,b\\\lambda}} (-1)^{a+b} \, p(a|x,\lambda)\, p(b|y,\lambda)\, q(\lambda)$$

$$= \sum_{xy} (-1)^{xy} \sum_{\lambda} q(\lambda) \left(\sum_{a} (-1)^{a} p(a|x,\lambda) \right) \cdot$$

$$\cdot \left(\sum_{b} (-1)^{b} \, p(b|y,\lambda) \right)$$

$$= \sum_{xy} (-1)^{xy} \sum_{\lambda} q(\lambda) \cdot A(x,\lambda)\, B(y,\lambda)$$

$$= \sum_{\lambda} q(\lambda) \Big[A(0,\lambda)\, B(0,\lambda) + A(1,\lambda)\, B(0,\lambda)$$

$$+ A(0,\lambda)\, B(1,\lambda) - A(1,\lambda)\, B(1,\lambda) \Big]$$

$$= \sum_{\lambda} \Big\{ \big[A(0,\lambda) + A(1,\lambda) \big] B(0,\lambda)$$

$$+ \big[A(0,\lambda) - A(1,\lambda) \big] B(1,\lambda) \Big\} \, q(\lambda)$$

$$|E| \leq \sum_{\lambda} |A(0,\lambda) + A(1,\lambda)| \cdot |B(0,\lambda)|\, q(\lambda)$$
$$+ |A(0,\lambda) - A(1,\lambda)| \cdot |B(1,\lambda)|\, q(\lambda)$$
$$\leq \sum_{\lambda} \Big[|A(0,\lambda) + A(1,\lambda)| +$$
$$+ |A(0,\lambda) - A(1,\lambda)| \Big]\, q(\lambda)$$
$$\leq \underbrace{\sum_{\lambda}}_{q(\lambda)} 2 \max \{ |A(0,\lambda)|, |A(1,\lambda)| \} \leq 2.$$

QM analysis:

$$E = \sum_{xy} (-1)^{xy} \sum_{ab} (-1)^{a} (-1)^{b}\, P(a,b|x,y)$$
$$= \sum_{xy} (-1)^{xy} \sum_{ab} (-1)^{a} (-1)^{b}\, \mathrm{tr}\{ \rho\, M_{a,x} \otimes N_{b,y} \}$$
$$= \sum_{xy} (-1)^{xy}\, \mathrm{tr}\{ \rho\, A_x \otimes B_y \},$$

where

$$A_x = M_{0,x} - M_{1,x}.$$
$$B_y = N_{0,y} - N_{1,y}.$$

Wlog. we can assume that the measurements are projective. Therefore

$$A_x^2 = (\Pi_{0x}-\Pi_{1x})^2 = \underbrace{\Pi_{0x}+\Pi_{1x}}_{\mathbb{1}} - \underbrace{\Pi_{0x}\Pi_{1x} - \Pi_{1x}\Pi_{0x}}_{0 \text{ as } \Pi_{0,x} \text{ and } \Pi_{1,x} \text{ are orth. proj.}} = \mathbb{1}.$$

Similarly, $B_y^2 = \mathbb{1}$.

Now $E(\rho)$ is convex $\Rightarrow$ extrem value at extremal point $\Rightarrow$ ρ is pure.

$$|E| \leqslant \left| \sum_{xy} (-1)^{xy} \langle \psi | A_x \otimes B_y | \psi \rangle \right|$$

for some op. A_x, B_y $\quad A_x^2 = B_y^2 = \mathbb{1}$, $\|\psi\| = 1$.

We obtain thus

$$|E| \underset{\text{at } \rho = |\psi\rangle\langle\psi|}{=} |\langle\psi| A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 |\psi\rangle|$$

Use now Cauchy-Schwartz:

$$|\langle\psi|O|\psi\rangle|^2 \leqslant \underbrace{\langle\psi|\psi\rangle}_{1} \cdot \langle\psi|O^\dagger O|\psi\rangle$$

Let us calculate $O^\dagger O = O^2$, with

$$O = A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1).$$

We obtain

$$O^2 = \left(A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)\right)^2 =$$

$$= A_0^2 \otimes (B_0 + B_1)^2 + A_1^2 \otimes (B_0 - B_1)^2$$

$$+ A_0 A_1 \otimes (B_0 + B_1)(B_0 - B_1)$$

$$+ A_1 A_0 \otimes (B_0 - B_1)(B_0 + B_1)$$

$$= \mathbb{1} \otimes \left[\underbrace{(B_0 + B_1)^2 + (B_0 - B_1)^2}_{2(B_0^2 + B_1^2) = 4\mathbb{1}} \right]$$

$$- A_0 A_1 \otimes B_0 B_1 + A_0 A_1 \otimes B_1 B_0$$

$$+ A_1 A_0 \otimes B_0 B_1 - A_1 A_0 \otimes B_1 B_0$$

$$= 4\mathbb{1} + A_1 A_0 \otimes B_0 B_1 + A_0 A_1 \otimes B_1 B_0$$

$$- A_0 A_1 \otimes B_0 B_1 - A_1 A_0 \otimes B_1 B_0$$

We obtain thus

$$|E_{QM}|^2 \leq \langle \psi | O^2 | \psi \rangle \leq 4 + \langle \psi | A_1 A_0 \otimes B_0 B_1 | \psi \rangle + \langle \psi | A_0 A_1 \otimes B_1 B_0 | \psi \rangle - \langle \psi | A_0 A_1 \otimes B_0 B_1 | \psi \rangle - \langle \psi | A_1 A_0 \otimes B_1 B_0 | \psi \rangle \leq 8$$

Using Cauchy-Schwartz as e.g.

$$|\langle \psi | A_1 A_0 \otimes B_0 B_1 | \psi \rangle|^2 \leq \|(A_0 \otimes B_1)|\psi\rangle\|^2 \cdot \|(A_1 \otimes B_0)|\psi\rangle\|^2 = 1.$$

Therefore $|E_{QM}| \leq 2\sqrt{2}$. ☆

14th lecture: 17/11/23

Recap:

- Ent. witnesses: $W = W^\dagger$, $W \not\geq 0$ s.t.

  $\operatorname{tr}\{\rho W\} > 0 \quad \forall \rho$ separable.

- Connection with positive but not CP maps.

- CHSH (Clauser Horne Shimony Holt)
  - C sends bits x to A, y to B
  - A and B send answer a, and B w/o communicating.
  - Goal: $a + b = xy$.

- Strategy: $P(a,b|x,y)$
  - Classical (LHV model)

    $P(a,b|x,y) = \sum_\lambda q(\lambda) P_A(a|x) P_B(b|y)$
  - Quantum:

    $P(a,b|x,y) = \operatorname{tr}\{\rho M_{a,x} \otimes N_{b,y}\}$,

    where $M_{a,x} \geq 0$, $N_{b,y} \geq 0$ and $\sum_a M_{a,x} = \mathbb{1}\ \forall x$

    $\sum_b N_{b,y} = \mathbb{1}\ \forall y$.

- Exp. value: $E = p(\text{win}) - p(\text{loose})$

  $|E_{cl}| \leq 2$.

  $|E_{QM}| \leq 2\sqrt{2}$.

Let us show that $|E_{QM}| = 2\sqrt{2}$ is achievable. Then there's a clear difference between classical and quantum strategies.

$$E_{QM} = \sum_{\substack{ab\\xy}} (-1)^{a+b+xy} \operatorname{tr}\{\rho M_{a,x} \otimes N_{b,y}\}$$

$$= \sum_{xy} (-1)^{+xy} \operatorname{tr}\{\rho A_x \otimes B_y\} \qquad (A_x = M_{0,x} - M_{1,x})$$

$$= \operatorname{tr}\{\rho (A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1)\}$$

- max. attained in a pure state

$$|E_{QM}| \leq |\langle\psi| \underbrace{A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)}_{O} |\psi\rangle|$$

$$\leq \sqrt{\langle\psi| O^2 |\psi\rangle} \leq \ldots \leq 2\sqrt{2}.$$

Equality can be reached; e.g.:

- $A_0 = X$, $A_1 = Z$, $B_0 = \frac{X+Z}{\sqrt{2}}$, $B_1 = \frac{X-Z}{\sqrt{2}}$
- $|\psi\rangle = \frac{1}{\sqrt{2}} |01\rangle - |10\rangle$.

Let's check that it works:

$$|E_{QM}| = |\langle\psi| A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1) |\psi\rangle|$$

$$= |\langle\psi| X \otimes X + Z \otimes Z |\psi\rangle| \cdot \sqrt{2}$$

$$X\otimes X + Z\otimes Z = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad |\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \quad \text{OK.}$$

Note: One can choose $B_0 = X$, $B_1 = X$ as well.

Note: Notice that $|\psi\rangle$ is entangled. For sep. states,

$$P(a,b|x,y) = \sum_i p_i \, \mathrm{tr}\{ \rho_i \Pi_{a,x} \otimes \eta_i N_{b,y} \} = \sum_i p_i \, p_A(a|x,i) \, p_B(b|y,i)$$

$\Rightarrow$ Same as LHV model! Sep $\cong$ classical.

Entanglement conversion, quantification.

State is entangled if it is not of the form $\sum_i p_i \, \eta_i \otimes \nu_i$, $\eta_i \geq 0$ and $\nu_i \geq 0$.

Note that local operations leave this structure invariant:

$$\sum_i p_i \, A_j^\dagger \eta_i A_j \otimes \nu_i \quad \text{still this form}$$

(A_j's are either Kraus operators or meas. operators)

This structure is the same even if (classical) communication is allowed:

- A time evolves } single meas.
- A measures }
- communicates result to B
- B time evolves depending on history (including A's output)
- B measures

⋮

So given ρ_{AB}, local ops. and classical communication (LOCC) is the protocol

ρ_{AB}

A meas. $\xrightarrow{\text{output } i}$ B meas. depending on i

$\xleftarrow{\text{output } j}$

A meas dep. on i, j $\longrightarrow$ ...

→ Can be finite / infinite round.

We say $\rho \xrightarrow{\text{LOCC}} \eta$ if for <u>all outcomes</u> protocol finishes in η. ($\rho \xrightarrow{\text{SLOCC}} \eta$ if <u>some</u> outcome is η)

Point is: if ρ_{AB} was separable, ρ_{AB} is still separable even after this protocol.

It is natural to say that LOCC operations <u>decrease</u> entanglement.

So when quantifying entanglement, we want:

$$\rho \xrightarrow{LOCC} \eta \Rightarrow E(\rho) \geq E(\eta)$$

where E any entanglement measure (real number for each density matrix).

That is: if $\rho \xrightarrow{LOCC} \eta$, then ρ is more entangled than η (more = greater or equal)

Let us first understand LOCC a bit better, then ent. quantification.

Example: $\mathbb{C}^2 \otimes \mathbb{C}^2$, pure states.

Thm: Let $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,

and $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ any other state.

Then there is an LOCC protocol s.t.

$$|\Omega\rangle \xrightarrow{LOCC} |\psi\rangle.$$

Remark: $|\Omega\rangle$ is more entangled as any other state (same as $(U \otimes V)|\Omega\rangle$ for U,V unitaries), hence the name maximally entangled state.

Proof: Explicit construction. Write

$$|\psi\rangle = \lambda_0 |\varphi_0\rangle \otimes |\chi_0\rangle + \lambda_1 |\varphi_1\rangle \otimes |\chi_1\rangle$$

Schmidt decomposition. Normalization:

$$\lambda_0^2 + \lambda_1^2 = 1.$$

Then create meas. ops

$$M_0 = \begin{pmatrix} \lambda_0 & \\ & \lambda_1 \end{pmatrix} \quad M_1 = \begin{pmatrix} \lambda_1 & \\ & \lambda_0 \end{pmatrix}$$

$$M_0^2 + M_1^2 = \mathbb{1}.$$

Let A apply the meas.

Outcome 0's post-meas. state:

$$\frac{1}{p_0} M_0 |\Omega\rangle = \lambda_0 |00\rangle + \lambda_1 |11\rangle$$

Outcome 1's post-meas. state:

$$\frac{1}{p_1} M_1 |\Omega\rangle = \lambda_1 |00\rangle + \lambda_0 |11\rangle.$$

So if outcome 0,

A applies $|\varphi_0\rangle\langle 0| + |\varphi_1\rangle\langle 1|$

B applies $|\varphi_0\rangle\langle 0| + |\chi_1\rangle\langle 1|$

If outcome 1,

A applies $|\varphi_1\rangle\langle 0| + |\varphi_0\rangle\langle 1|$

B applies $|\chi_1\rangle\langle 0| + |\chi_0\rangle\langle 1|$.

unitaries

For <u>both</u> outcomes, we obtain

$$|\psi\rangle = \lambda_0 |\varphi_0\rangle |\chi_0\rangle + \lambda_1 |\varphi_1\rangle |\chi_1\rangle.$$

$\square$

<u>Note again</u>: we need to reach target for <u>all</u> outcomes.

<u>Note as well</u>: Here we only needed 1 round

of communication. This is not a coincidence.

We have seen: from $|\Omega\rangle$ we can reach anything. (Hence the name max. ent. state).

Can we reach $|\Omega\rangle$ from other states?

Does LOCC make sense?

We will see: can't reach $|\Omega\rangle$ deterministically, only probabilistically (unless $|\psi\rangle = (U \otimes V)|\Omega\rangle$)

<u>Eg</u>: $|\psi\rangle = \lambda_0 |\varphi_0\rangle|\chi_0\rangle + \lambda_1 |\varphi_1\rangle|\chi_1\rangle$ w/ $\lambda_0 > \lambda_1$

A measures

$$M_0 = \frac{\lambda_1}{\lambda_0}|\varphi_0\rangle\langle\varphi_0| + |\varphi_1\rangle\langle\varphi_1|$$

$$M_1 = \sqrt{1 - \frac{\lambda_1^2}{\lambda_0^2}}\, |\varphi_0\rangle\langle\varphi_0|$$

Post-meas. state if outcome is 0:

$$\frac{1}{\sqrt{p_0}} M_0|\psi\rangle = \frac{1}{\lambda_1} \quad \lambda_1 |\varphi_0\rangle|\chi_0\rangle + \lambda_1 |\varphi_1\rangle|\chi_1\rangle$$

$\rightsquigarrow$ A, B can make $|\Omega\rangle$ w/ unitaries.

For outcome 1, we fail.

So we succeed: w/ proba $\frac{1}{\lambda_1}$.

As it is not <u>all</u> possible outcomes,

$$|\psi\rangle \overset{LOCC}{\not\longrightarrow} |\Omega\rangle \text{ unless } |\psi\rangle \overset{LU}{\sim} |\Omega\rangle.$$

$$|\psi\rangle \xrightarrow{SLOCC} |\Omega\rangle \text{ unless } \lambda_1 = 0.$$

We have seen: both protocols are extremely short, they end in 1 round of communication!

<u>Thm</u>: For a pure state $|\psi\rangle$, every LOCC protocol can be replaced by another protocol w/ only 1 round of communication:

1. A measures, sends outcome to B
2. B applies a unitary depending on outcome.

☆

15th lecture 20/11/23

- Entanglement (sep.: $\rho = \sum_i p_i \eta_i \otimes \nu_i$ w/ $p_i, \eta_i, \nu_i \geq 0$)
- Entanglement is a <u>resource</u> that allows achieving tasks impossible w/ classical physics. Ex.: CHSH game
- Operations that should not grow entanglement: LOCC.
- Local operations:
  - measurement
  - time evolution (unitaries for pure states)
  - combination of these
- LOCC can contain several (even ∞) rounds of communication

<u>Thm</u>: If $|\psi\rangle \xrightarrow{LOCC} |\phi\rangle$, then there is a 1-round protocol that transforms $|\psi\rangle$ to $|\phi\rangle$.

<u>Proof</u>: Let us show that A can simulate B's measurements on her side. As local unitaries are free, we want to achieve:

$$(\mathbb{1}\otimes \Pi_i)|\psi\rangle = (N_i \otimes U_i)|\psi\rangle .$$

where $\sum_i \Pi_i^\dagger \Pi_i = \mathbb{1}$, $\sum_i N_i^\dagger N_i = \mathbb{1}$, U_i is unitary.

Necessary:

$$\mathrm{tr}_B\left\{(\mathbb{1}\otimes \Pi_i)|\psi\rangle\langle\psi|(\mathbb{1}\otimes\Pi_i^\dagger)\right\}$$

$$= \mathrm{tr}_B\left\{(N_i\otimes U_i)|\psi\rangle\langle\psi|(N_i^\dagger\otimes U_i^\dagger)\right\}$$

$$\rho_{i,A} = N_i \rho_A N_i^\dagger$$

If ρ_A is full rank, we can find such N_i:

$$N_i = \rho_{i,A}^{1/2}\rho_A^{-1/2}. \quad \text{(works as well if } \rho_A \text{ not full rank)}$$

This N_i is a measurement:

$$\sum_i N_i^\dagger N_i = \sum_i \rho_A^{-1/2}\rho_{i,A}\rho_A^{-1/2} = \mathbb{1} \text{ as}$$

$$\sum_i \rho_{i,A} = \sum_i \mathrm{tr}_B\left((\mathbb{1}\otimes\Pi_i^\dagger\Pi_i)|\psi\rangle\langle\psi|\right) = \rho_A .$$

Finally: if $(\mathbb{1}\otimes M_i)|\psi\rangle = \sum_j \lambda_{ij}|\varphi_{ij}\rangle\otimes|\chi_{ij}\rangle$,

then $\rho_{i,A} = \sum_j \lambda_{ij}^2 |\varphi_{ij}\rangle\langle\varphi_{ij}|$

And as $\rho_{i,A} = N_i \rho_A N_i^\dagger$,

$(N_i\otimes\mathbb{1})|\psi\rangle = \sum_j \lambda_{ij}|\varphi_{ij}\rangle\otimes|\hat{\chi}_{ij}\rangle$,

i.e. it has the same Schmidt values and left Schmidt vectors.

Then there is a unitary U_i that transforms $|\hat{\chi}_{ij}\rangle$ to $|\chi_{ij}\rangle$.

That is, $(N_i\otimes U_i)|\psi\rangle = (\mathbb{1}\otimes M_i)|\psi\rangle$.

So A can simulate B's measurements, and thus all meas. can be carried out on A's side! Finally, consecutive meas/time ev. can be done via a single measurement (w/many outputs), and then all time ev. on B's side can be carried out at once.

$\square$

Let us try to understand when

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle \text{ is possible.}$$

We have proven that 1 round LOCC is enough!

So question: when is

$$(M_i \otimes U_i)|\psi\rangle = \sqrt{p_i}\,|\phi\rangle$$

possible? (M_i: meas, U_i unitaries, p_i: proba)

<u>Remark</u>: as local unitaries are free,

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle \text{ iff}$$

$$(U \otimes V)|\psi\rangle \xrightarrow{LOCC} (\hat{U} \otimes \hat{V})|\phi\rangle,$$

the answer will depend <u>only</u> on the Schmidt values of $|\psi\rangle$ and $|\phi\rangle$.

Let us derive first a necessary criterion.

(And show later that it is sufficient as well).

Let: $(\Pi_i \otimes \mathcal{U}_i)|\psi\rangle = \sqrt{p_i}\,|\phi\rangle \quad \forall i$

Let us trace the A subsystem!

$$\eta^B := \mathrm{tr}_A |\phi\rangle\langle\phi|$$

$$\rho_i^B := \frac{1}{p_i}\,\mathrm{tr}\{(\Pi_i \otimes \mathbb{1})|\psi\rangle\langle\psi|(\Pi_i^\dagger \otimes \mathbb{1})\}$$

Then $\rho^B = \sum_i p_i \rho_i^B$ and

$$\mathcal{U}_i \rho_i^B \mathcal{U}_i^\dagger = \eta^B, \text{ or}$$

$$\rho_i^B = \mathcal{U}_i^\dagger \eta^B \mathcal{U}_i \quad \forall i.$$

Consider now a rank k orth. projector

$$\max_{\substack{P:\text{ orth. proj}\\ \text{rank}=k}} \mathrm{tr}\{P\rho^B\} = \max_P \mathrm{tr}\{P \sum_i p_i \rho_i^B\} \leq$$

$$\leq \sum_i p_i \max_P \mathrm{tr}\{P\rho_i^B\} = \sum_i p_i \max_P \mathrm{tr}\{P\mathcal{U}_i^\dagger \eta^B \mathcal{U}_i\}$$

$$= \sum_i p_i \max_P \mathrm{tr}\{\mathcal{U}_i P \mathcal{U}_i^\dagger \eta^B\} = \sum_i p_i \max \mathrm{tr}\{P\eta^B\}$$

$$= \max_P \mathrm{tr}\{P\eta^B\}$$

So we have learned that if $|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle$, then

$$\max_P \mathrm{tr}\{P\underbrace{\rho^B}_{\mathrm{tr}_A|\psi\rangle\langle\psi|}\} \leq \max_P \mathrm{tr}\{P\underbrace{\eta^B}_{\mathrm{tr}_A|\phi\rangle\langle\phi|}\}$$

These quantities can be expressed with the Schmidt values of $|\psi\rangle, |\phi\rangle$ (the eigenvalues of ρ^B, η^B):

<u>Thm</u> (Ky-Fan): Let A be Hermitian.

$$\max_{\substack{P:\ P\ \text{ortho proj} \\ \operatorname{tr} P = k}} \operatorname{tr}\{PA\} = \sum_{i=1}^{k} \lambda_i ,$$

where λ_i are the eig. values of A arranged in descending order.

<u>Proof</u>:

$\boxed{\geq}$: Choose $P = \sum_{i=1}^{k} |a_i\rangle\langle a_i|$, where $|a_i\rangle$ are the eig. vectors of A.

$\boxed{\leq}$: Notice that

$$\operatorname{tr}\{PA\} = \sum_i \underbrace{\langle a_i|P|a_i\rangle}_{w_i} \lambda_i = \sum_i w_i \lambda_i ,$$

where $\sum_i w_i = \operatorname{tr} P = k$ and $0 \leq w_i \leq 1 \ \forall k$.

<u>Best</u>: $w_i = 1$ for the k largest values. $\square$

Def: Majorization: let $\lambda, \mu \in \mathbb{R}^n_{\geq 0}$ and let $\lambda^{\downarrow}, \mu^{\downarrow}$ be the vectors where the entries of λ and μ are ordered descending.
We say that μ majorizes λ, $\mu \succ \lambda$ if for all $k = 1, \dots, n$,

$$\sum_{i=1}^{k} \mu_i^{\downarrow} \geq \sum_{i=1}^{k} \lambda_i^{\downarrow}.$$

We have thus seen that

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle$$

Implies that the Schmidt values of $|\phi\rangle$ majorize the Schmidt values of $|\psi\rangle$.

Thm: Let $\lambda, \mu \in \mathbb{R}^n$ be probability distributions. Then $\lambda \prec \mu$ iff there exists $m \in \mathbb{N}$, a proba distribution $q \in \mathbb{R}^m$ and permutation matrices $\{P_i\}_{i=1}^{m}$ s.t.

$$\lambda = \sum_i q_i P_i \mu.$$

Proof :

$\boxed{\Leftarrow}$ $\lambda = \sum_i q_i P_i \mu$ implies that

$\lambda^{\downarrow} = \sum_i q_i \hat{P}_i \mu^{\downarrow}$ for some $\hat{P}_i$ permutation matrices. Then

$$\sum_{j=1}^{k} \lambda^{\downarrow}_j = \sum_{j=1}^{k} \sum_i q_i (\hat{P}_i \mu^{\downarrow})_j \leq$$

$$\leq \sum_i \sum_{j=1}^{k} q_i \mu^{\downarrow}_j = \sum_{j=1}^{k} \mu^{\downarrow}_j .$$

$\boxed{\Rightarrow}$ Homework.

$\square$

Let us show now that if the Schmidt values of $|\phi\rangle$ majorize the Schmidt values of $|\psi\rangle$, then

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle .$$

Let ρ_A be the reduced density of $|\psi\rangle$, η_A the reduced density of $|\phi\rangle$.

Let

$$\rho_A = \sum_i \lambda_i |\chi_i\rangle\langle\chi_i|$$

$$\eta_A = \sum_i \mu_i |\varphi_i\rangle\langle\varphi_i| .$$

Then $\lambda \prec \mu$ implies that

$$\lambda = \sum_i q_i P_i \mu .$$

That is, if

$$\mathcal{U}_i = \sum_j |\chi_{P_i(j)}\rangle\langle\varphi_j| ,$$

Then

$$\rho_A = \sum_i q_i \, \mathcal{U}_i \eta_A \mathcal{U}_i^+ .$$

Let us define now

$$M_i = \sqrt{q_i}\,(\eta_A)^{1/2}\, \mathcal{U}_i^+ (\rho_A)^{-1/2} .$$

Then

(1) $$M_i \rho_A M_i^+ = q_i \eta_A$$

(2) $$\sum_i M_i^+ M_i = \mathbb{1}$$

Therefore M_i transforms the Schmidt vectors and values of $|\psi\rangle$ well, thus there are unitaries V_i s.t.

$$(M_i \otimes V_i)|\psi\rangle = \sqrt{q_i}\,|\phi\rangle$$

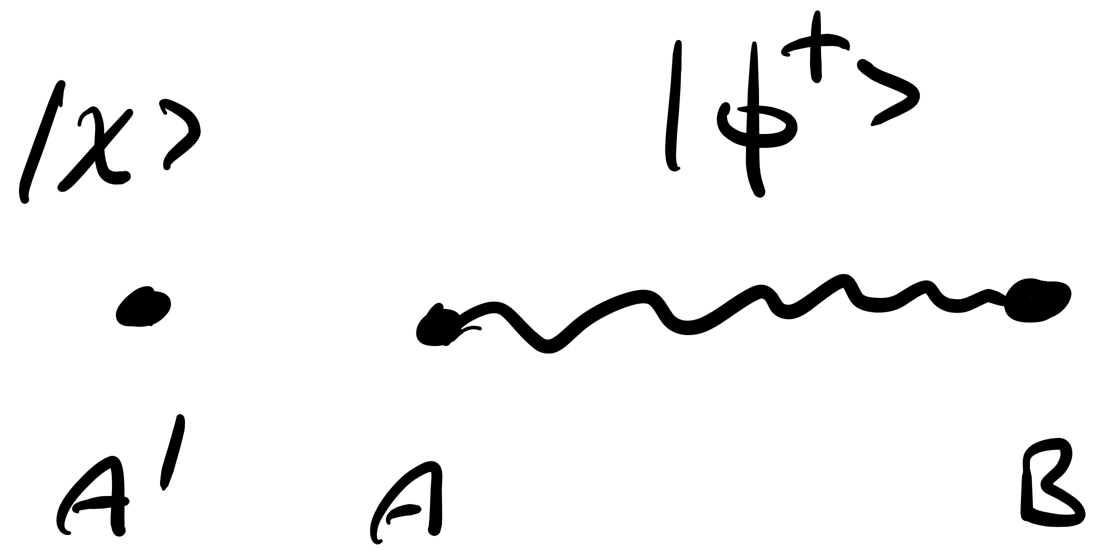
We have thus seen:

<u>Thm</u>: $|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle$ iff the Schmidt values of $|\phi\rangle$ majorize the Schmidt values of $|\psi\rangle$.

Applications of entanglement: Teleportation and dense coding

a) Teleportation

Setup:



- A & B share entangled state $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$

- A has unknown quantum state

$$|\chi\rangle_{A'} = a|0\rangle_{A'} + b|1\rangle_{A'}$$

(Could e.g. also be part of a larger system → linearity!)

- A & B cannot (reliably*) transmit quantum states, but can communicate classically "for free".

* If the line is unreliable, A & B can still use it to create entangled states $|\phi^+\rangle$, e.g. by repeat-until-success, or entanglement distillation (→ later!), or using "quantum repeaters" (→ later!)

Question: Can A get $|\chi\rangle$ (safely) to B?

Problem: Any measurement of $|X\rangle$ would only reveal partial information, yet destroy state!

Solution: **Quantum Teleportation!**

Teleportation Protocol:

(1) A performs measurement on $A'A$ in Bell basis

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = (Z\otimes I)|\phi^+\rangle = (I\otimes Z)|\phi^+\rangle$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = (X\otimes I)|\phi^+\rangle = (I\otimes X)|\phi^+\rangle$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = (ZX\otimes I)|\phi^+\rangle = (I\otimes XZ)|\phi^+\rangle$$

We also write the four Bell states as

$$|\phi_{\alpha\beta}\rangle = (Z^\alpha X^\beta \otimes I)|\phi^+\rangle = (I\otimes X^\beta Z^\alpha)|\phi^+\rangle$$

$\alpha, \beta = 0, 1$

Outcome probabilities for meas. outcome $|\phi_{\alpha\beta}\rangle$:

$$\rho_A = \mathrm{tr}_B\left[|\phi^+\rangle\langle\phi^+|_{AB}\right] = \frac{1}{2} I_A \quad \longleftarrow \text{ state of } A.$$

$$p_{\alpha\beta} = \langle\phi_{\alpha\beta}|\ |\chi\rangle\langle\chi|_{A'} \otimes \tfrac{1}{2} I_A\ |\phi_{\alpha\beta}\rangle$$

$$= \frac{1}{2}\,\mathrm{tr}\left[\left(|\chi\rangle\langle\chi|_{A'} \otimes I_A\right)\ |\phi_{\alpha\beta}\rangle\langle\phi_{\alpha\beta}|\right]$$

$$= \frac{1}{2}\,\mathrm{tr}_{A'}\left[\,|\chi\rangle\langle\chi|_{A'} \cdot \underbrace{\mathrm{tr}_A\left[|\phi_{\alpha\beta}\rangle\langle\phi_{\alpha\beta}|\right]}_{=\frac{1}{2} I_{A'}}\right]$$

$$= \frac{1}{2}\,\mathrm{tr}\left[\,|\chi\rangle\langle\chi|_{A'} \cdot \tfrac{1}{2} I_{A'}\right]$$

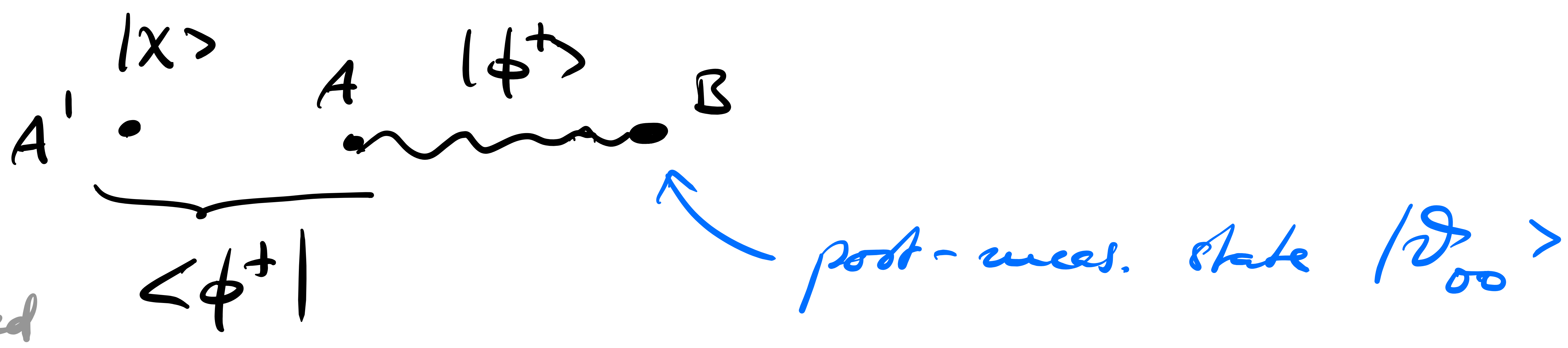
$$= \underline{\underline{\frac{1}{4}}}$$

$\Rightarrow$ <u>equal probability</u> $p_{\alpha\beta} = 1/4$ for all outcomes.

(This <u>is good</u> – if $p_{\alpha\beta}$ would depend on $|\chi\rangle$, it would reveal information on $|\chi\rangle$ and thus perturb the state!)

What is the state of B after the measurement?

i) Outcome $|\phi^+\rangle = |\phi_{00}\rangle$:



unnormalized

$$|\tilde{\vartheta}_{00}\rangle = \langle\phi^+|_{A'A} \left(|\chi\rangle_{A'} \otimes |\phi^+\rangle_{AB} \right)$$

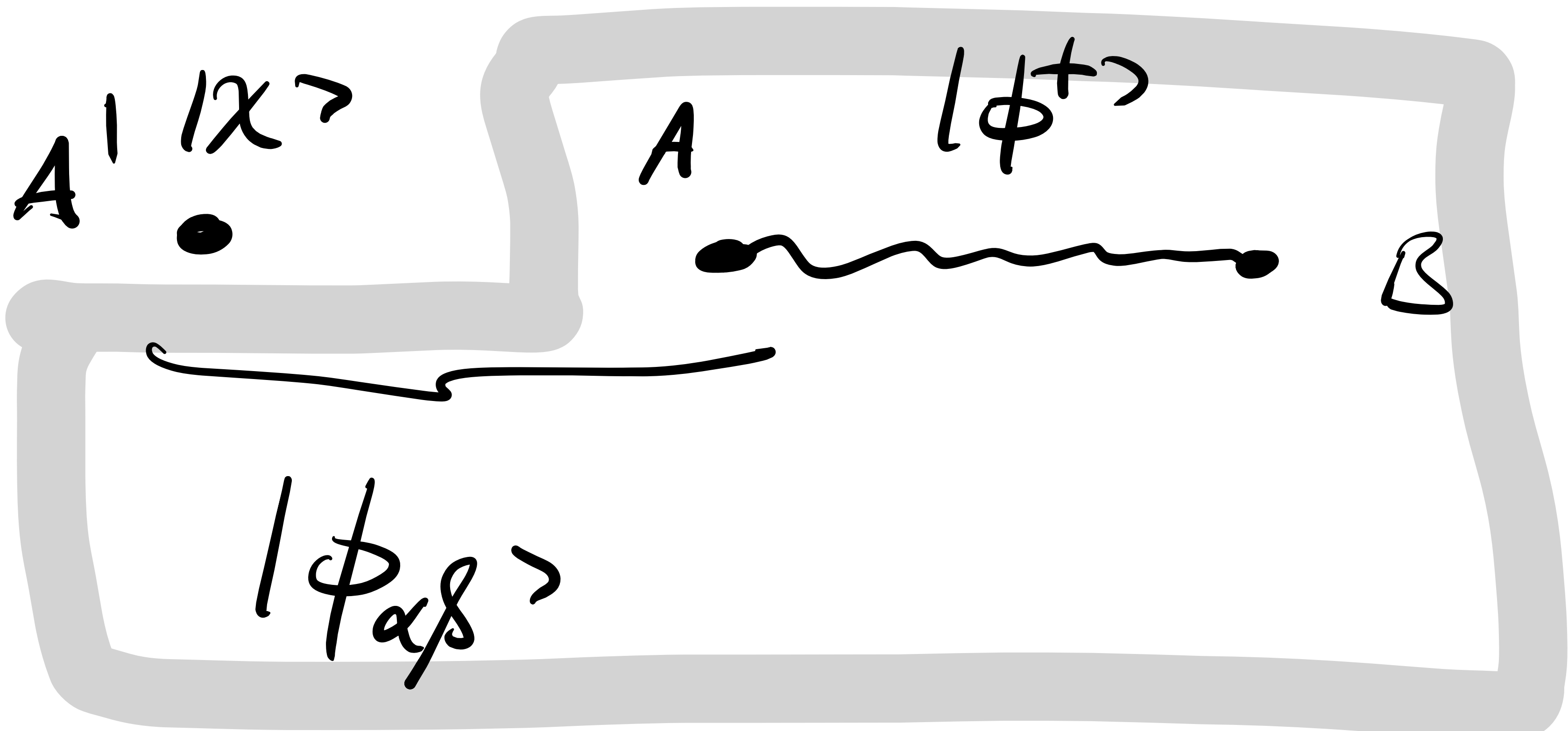
$$= \frac{1}{2} \underbrace{\left(\langle 00|_{A'A} + \langle 11|_{A'A}\right)\left(\left(a|0\rangle_{A'} + b|1\rangle_{A'}\right)\otimes}_{= a\langle 0|_A + b\langle 1|_A}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)\right)$$

$$= \frac{1}{2}\left(a|0\rangle_B + b|1\rangle_B\right) \qquad (*)$$

$\Rightarrow$ State $|\vartheta_{00}\rangle = |\chi\rangle$ appears at B!

(works with 25% probability.)

ii) What about the other outcomes?



First consider $\langle \phi_{\alpha\beta}|_{A'A} |\phi^+\rangle_{AB}$ — worked

going above:

$$\langle \phi_{\alpha\beta}|_{A'A} |\phi^+\rangle_{AB} = \langle \phi^+|_{A'A} \left(I_{A'} \otimes Z_A^{\alpha} X_A^{\beta}\right) |\phi^+\rangle_{AB}$$

$$= \langle \phi^+|_{A'A} \left(Z_A^{\alpha} X_A^{\beta} \otimes I_B\right) |\phi^+\rangle_{AB}$$

$$= \langle \phi^+|_{A'A} \left(I_A \otimes X_B^{\beta} Z_B^{\alpha}\right) |\phi^+\rangle_{AB}$$

$$= X_B^{\beta} Z_B^{\alpha} \langle \phi^+|_{A'A} |\phi^+\rangle_{AB}$$

Now combine with derivation $\circledast$ in part i)

$$|\tilde{\vartheta}_{\alpha\beta}\rangle = \langle \phi_{\alpha\beta}|_{A'A} \left(|\chi\rangle_{A'} \otimes |\phi^+\rangle_{AB}\right)$$

$$= X_B^{\beta} Z_B^{\alpha} \underbrace{\langle \phi^+|_{A'A} \left(|\chi\rangle_{A'} \otimes |\phi^+\rangle_{AB}\right)}_{\overset{\circledast}{=} \frac{1}{2}|\chi\rangle_B}$$

$$= \frac{1}{2} X^{\beta} Z^{\alpha} |\chi\rangle_B .$$

$\Longrightarrow$ After A's measurement, B obtains $|\vartheta_{\alpha\beta}\rangle = X^\beta Z^\alpha |\chi\rangle$ with probability 1/4 each.

$\Longrightarrow$ average state of B – without learning meas. result – is $\frac{1}{4}\sum X^\beta Z^\alpha |\chi\rangle\langle\chi| Z^\alpha X^\beta = \frac{1}{2} I$.

i.e.: Bob has no information about $|\chi\rangle$ (in fact: same state as without meas.)

(2) A communicates meas. outcome (α,β) to B, and

(3) B applies $(X^\beta Z^\alpha)^\dagger$ to their state

$\Longrightarrow$ Bob obtains

$$(X^\beta Z^\alpha)^\dagger |\vartheta_{\alpha\beta}\rangle = (X^\beta Z^\alpha)^\dagger (X^\beta Z^\alpha)|\chi\rangle = \underline{|\chi\rangle}$$

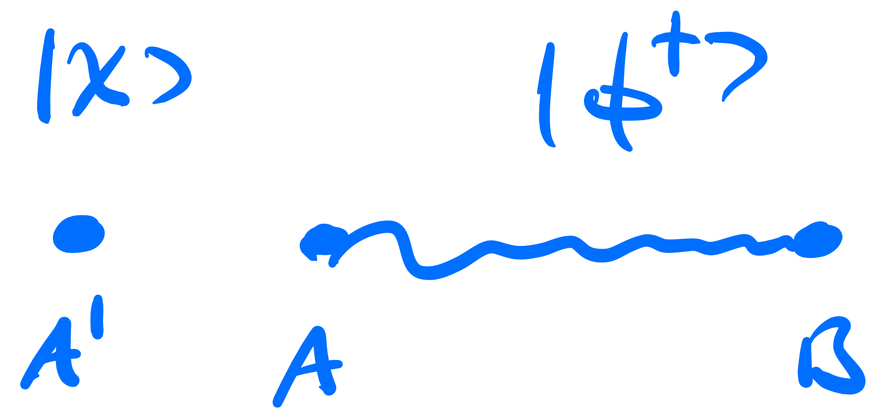
$\Longrightarrow$ Bob obtains $|\chi\rangle$ with probability 1!

$\Longrightarrow$ State $|\chi\rangle$ has been <u>teleported</u> to B.

<u>Notes:</u> • No faster-than-light communication (avg. state of B is $\frac{1}{2}I$ prior to receiving (α,β) – which has finite transm. speed.)

- Communicating 1 qubit requires 1 "e-bit" (= a max. entangled state $|\phi^+\rangle$ of 1+1 qubit) + 2 bits of classical communication ("c-bits")

<u>Teleportation protocol – summary:</u>



① Measure A, A' in $|\Phi_{\alpha\beta}\rangle$ basis.

② Communicate (α,β) from A to B.

③ Apply $(X^\beta Z^\alpha)^\dagger$ on B.

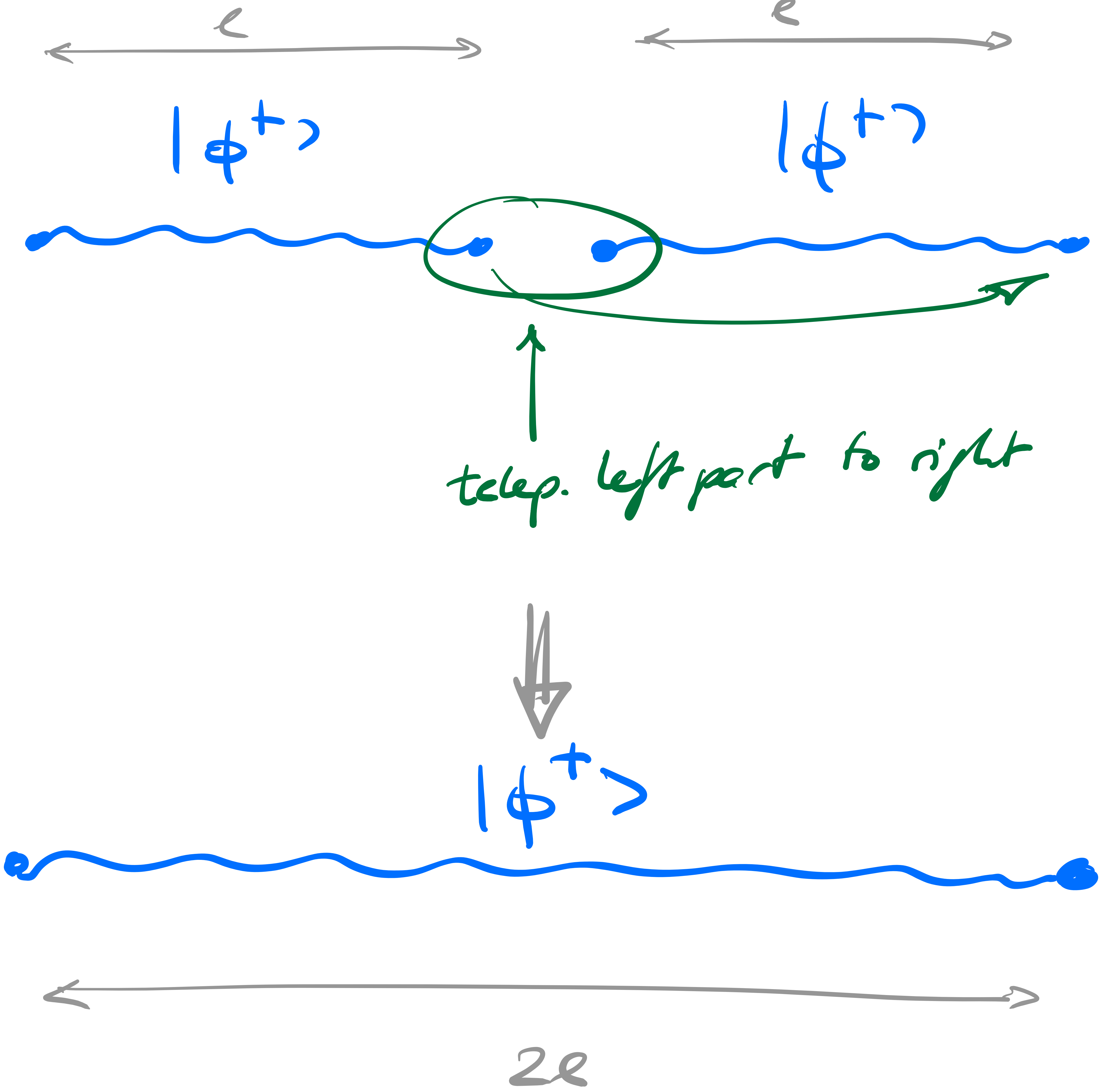
Can be straightforwardly generalized to $\mathbb{C}^d$.

One application of teleportation:

<u>Quantum Repeaters</u>

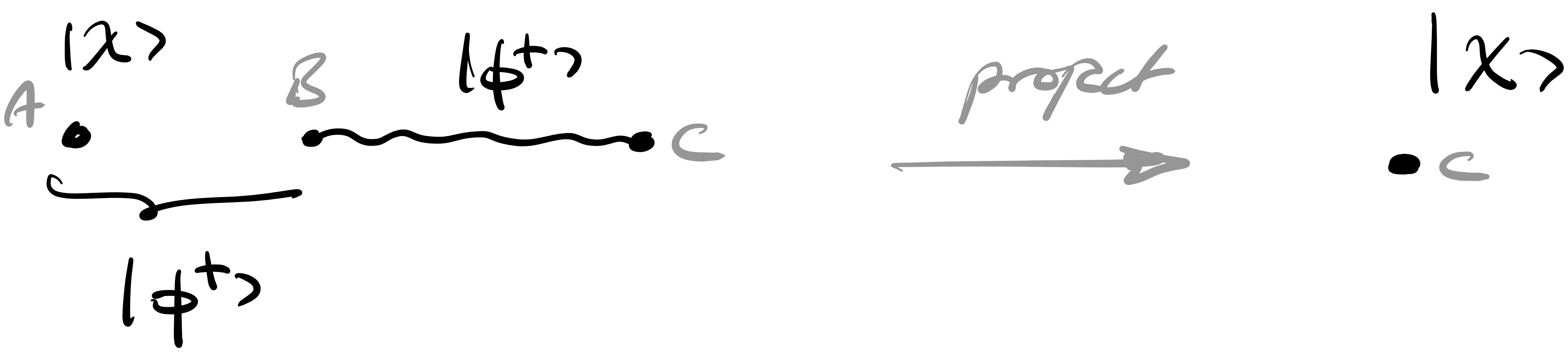
We can (reliably) create entanglement over distance ℓ $\rightarrow$ can we create entanglement over distance 2ℓ?

(E.g.: Photon loss at const. rate $\rightarrow$ prob. to send half of an ent. pair over dist. ℓ is $e^{-\ell/\xi}$.)



b) Relation between teleportation and the Choi-Jamiołkowski isomorphism

① Consider "postselected teleportation"

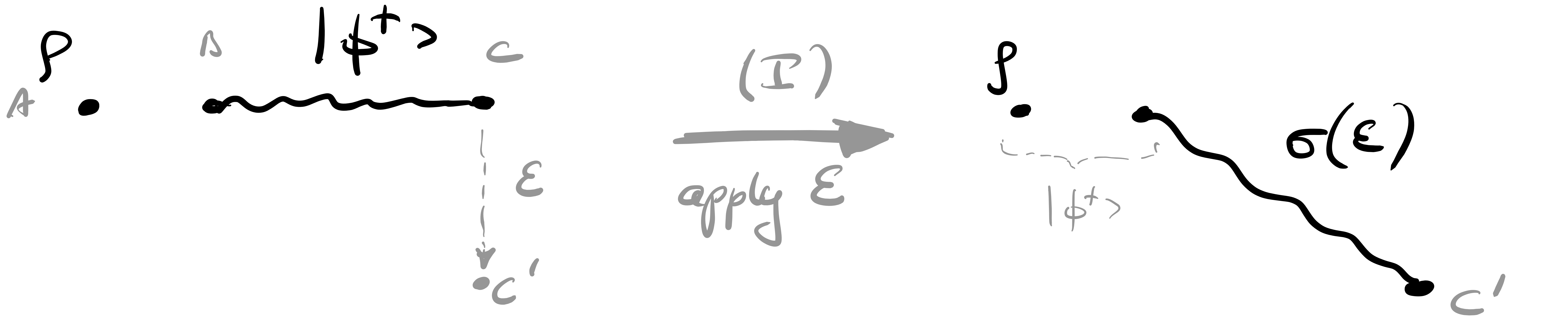


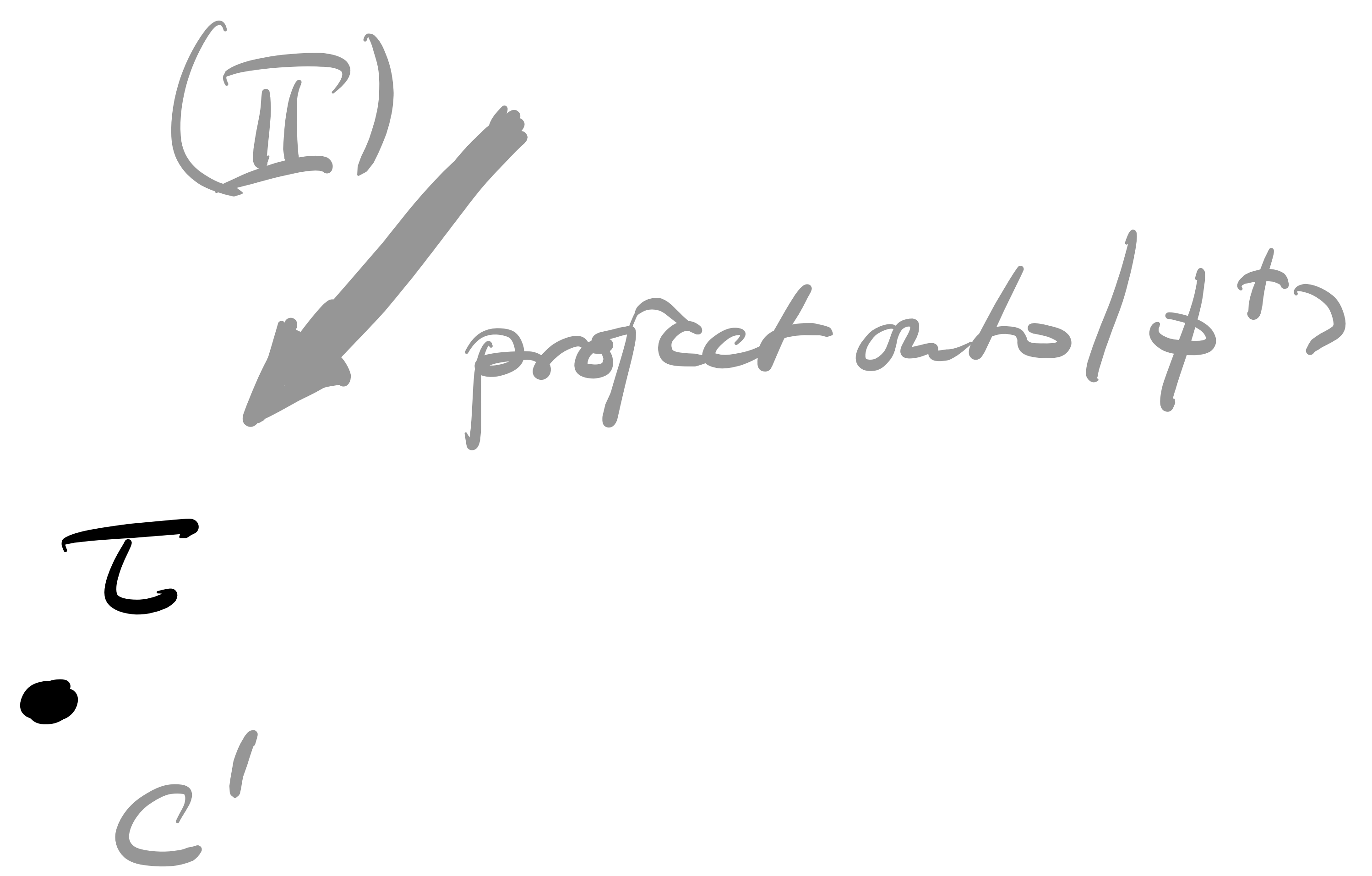
project onto $|\phi^+\rangle$: "postselected" measurement, i.e. we only consider this outcome

... so this is a complicated way of writing the identity map.

② Protocol for applying $\rho \mapsto \mathcal{E}(\rho)$:

③ Now interchange the order of applying $\mathcal{E}$ and projecting — they commute (as they act on diff. systems), so this is the same map:





Since orders commute, this is the same as ②, i.e.

$$\tau = \mathcal{E}(\rho)\,!$$

This is the <u>Choi-Jamiolkowski isomorphism</u> (!):

(I) is the $\mathcal{E} \longmapsto \sigma$ map

("apply $\mathcal{E}$ to half a max. entangled state")

(II) is the $\sigma \longmapsto \mathcal{E}$ map

("teleport σ through the Choi state")

c) Dense coding

Have seen:

- shared entanglement + class. channel $\to$ q. channel

$$1 \text{ ebit} + 2 \text{ cbit} \longrightarrow 1 \text{ qubit}$$

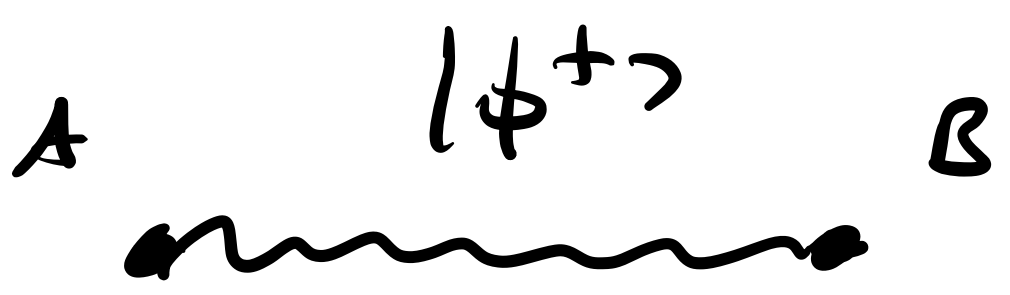
Can we do the converse? Use a quantum channel to transmit classical information?

Trivially possible by encoding $0 \to |0\rangle$, $1 \to |1\rangle$

$$1 \text{ qubit} \longrightarrow 1 \text{ cbit}$$

Can we do better if we also share entanglement?

Dense coding (sometimes also "superdense coding"):



Idea: Encode two bits in $\{|\phi_{\alpha\beta}\rangle\}_{\alpha,\beta=0,1}$ (an ONB)

1. A & B share $|\phi^+\rangle$.
2. A can encode two bits α,β locally:

$$|\phi_{\alpha\beta}\rangle_{AB} = \left(Z_A^{\alpha} X_B^{\beta} \otimes I \right) |\phi^+\rangle_{AB}$$

i.e., A applies $Z^\alpha X^\beta$ to her part of $|\phi^+\rangle$.

3. A sends her part of the state to B via the quantum communication channel.
4. B measures in Bell basis $\{|\phi_{\alpha\beta}\rangle\}$ and recovers α and β.

shared ent. + q. channel → class. channel

1 ebit + 1 qubit → 2 cbit

d) Optimality of teleportation & dense coding

We can use the teleportation & dense coding protocol mutually to argue that both are optimal in terms of communication cost.

To this end, assume shared ent. is free (i.e.: this is not part of our cost function).

i) Assume we can teleport with $r < 2$ bits of class. communication per qubit sent (i.e., there are protocols to send k_q qubits w/ k_c class. bits s.th. $\frac{k_c}{k_q} \longrightarrow r$).

Use this "hyper-teleportation" protocol to send quantum states in the (normal) dense coding prot.:

send $2n$ cbits

$\Big\downarrow$ dense coding

send n qubits

$\Big\downarrow$ "hyper-teleportation"

send rn cbits, $r<2$

$\Rightarrow$ Can compress class. information (in the presence of entanglement).

$\Rightarrow$ Can <u>iterate this</u> to <u>arbitrarily</u> compress class. info – i.e., send n bits with $k \ll n$ bits – as long as we have free entanglement.

This is impossible! (Intuitively, can also be formalized)

ii) Assume we can "hyper-dense-code" $2s>2$ class. bits per qubit sent.

send $2s$ class. bits

$\Big|$

$\big\downarrow$ "hyper-dense coding"

send 1 qubit

$\big\downarrow$ teleportation

send 2 cbits

... and again, we can send 2s bits by only transmitting 2 bits, etc. ...