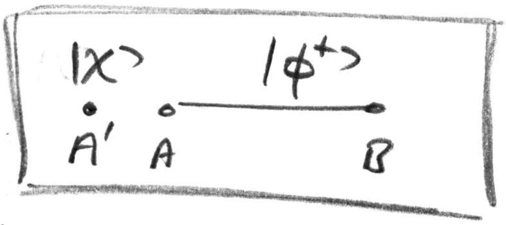
## Teleportation protocol:

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



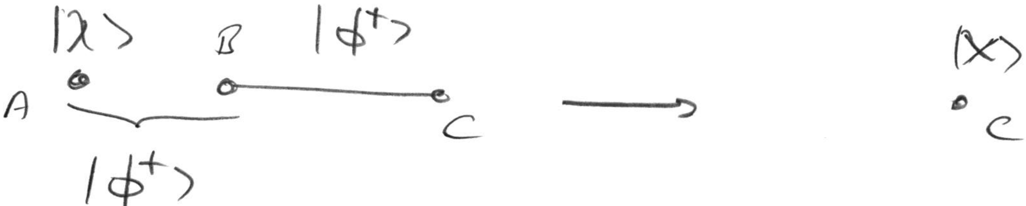

2. Communicate $(\alpha,\beta)$ from $A$ to $B$.
3. Perform $(X^\beta Z^\alpha)^\dagger$ on $B$.

Generalization to qu-d-its straightforward! ($\rightarrow$ HW)

---

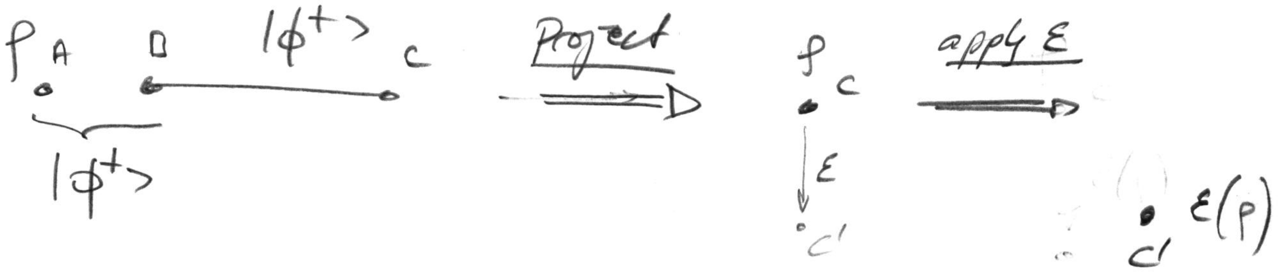
## Relation betw. teleportation & Choi-Jamiolkowski:

1. Consider "postselected teleportation"

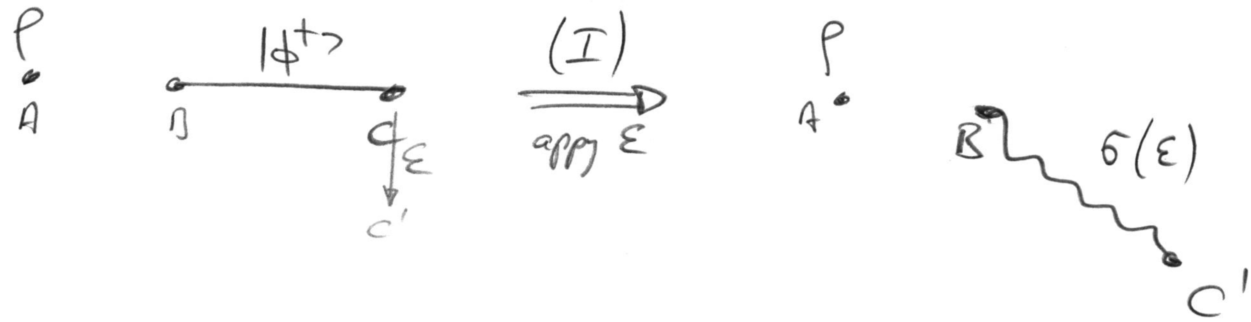


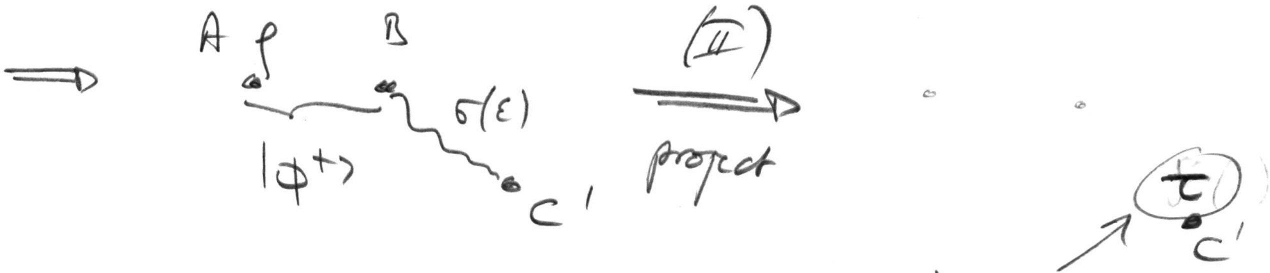

projection onto $|\phi^+\rangle$ $\equiv$ "postselected" meas.

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



③ <u>Interchg. order of ~~proj.~~ & appl. of $\mathcal{E}$:</u>




$\boxed{\tau = \mathcal{E}(\rho)\text{, since order commutes!}}$

This is Choi-Jamiołkowski:

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

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

(check formulas $\rightarrow$ HW)

---

<u>Dense coding:</u>

Have seen:

- ent. + class. channel $\Rightarrow$ q. channel

  1ebit + 2 class. bits $\longrightarrow$ 1 qubit

- converse possible? q channel $\rightarrow$ class. channel?

trivially by encoding $0 \to |0\rangle$, $1 \to |1\rangle$. 

$$\text{q. channel} \longrightarrow \text{class. channel}$$
$$1 \text{ qubit} \longrightarrow 1 \text{ class. bit}$$

<u>Can we do better w/ entanglement?</u>

$$A \quad |\phi^+\rangle \quad B$$

Encode <u>2 bits</u> in $|\phi_{\alpha\beta}\rangle$ (ONB)

① A can encode two bits $\alpha, \beta$ locally:

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

② A sends her part of the state to B.

③ B measures in Bell basis $\to$ recover $\alpha, \beta$.

$$\text{ent.} + \text{q. channel} \longrightarrow \text{class. channel}$$
$$1 \text{ ebit} + 1 \text{ qubit} \longrightarrow 2 \text{ class. bits}$$

("Dense coding" or "superdense coding")

<u>Note</u>: Together w/ teleportation, this shows optimality of the classical/quantum communication for both protocols.

# 4. Entanglement conversion & quantification

## a) Introduction & Setup

Entanglement $\equiv$ what cannot be changed by local operations & classical communication (LOCC)

Q: When can we convert ent. states into each other w/ LOCC?

Relevance:

- Different protocols might required different ("cheaper"/ "more expensive") entangled states.
- Use to quantify entanglement in terms of some reference state; How many "e-bits" $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are contained in a state?

Known: same Schmidt coefficients $\Leftrightarrow$ related by local unitary $\Leftrightarrow$ same entanglement

What if Schmidt coeffs different?

Example: $|\chi\rangle = \sqrt{\frac{2}{3}}\,|00\rangle + \sqrt{\frac{1}{3}}\,|11\rangle$ ; $|\phi^+\rangle = \sqrt{\frac{1}{2}}\,|00\rangle + \sqrt{\frac{1}{2}}\,|11\rangle$

1. Can we convert $|\phi^+\rangle \longrightarrow |\chi\rangle$ ?

A does POVM $\{\Pi_0, \Pi_1\}$; $\Pi_0 = \begin{pmatrix} \sqrt{2/3} & \\ & \sqrt{1/3} \end{pmatrix}$; $\Pi_1 = \begin{pmatrix} \sqrt{1/3} & \\ & \sqrt{2/3} \end{pmatrix}$.

$\rightarrow$ post-meas. states $|\tilde{\psi}_k\rangle = \Pi_k|\phi^+\rangle$:

$$|\tilde{\psi}_0\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle\right); \quad |\tilde{\psi}_1\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle\right)$$

$\Rightarrow$ $p_0 = \frac{1}{2}$: $|\psi_0\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle = |\chi\rangle$ : <u>OK!</u> ✓

$p_1 = \frac{1}{2}$: $|\psi_1\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$ :

A & B need to apply $X \otimes X$.

<u>Protocol</u>: A does POVM, sends result to B, if result is 1, both apply $X$.

<u>Success probability</u> $\underline{\underline{p = p_0 + p_1 = 1}}$

<u>Best possible</u>: We cannot get $> 1$ copies, as POVM cannot increase Schmidt rank!

## 2. Can we do the converse: $|\chi\rangle \longrightarrow |\phi^+\rangle$?

A does POVM $\{\Pi_0, \Pi_1\}$; $\Pi_0 = \begin{pmatrix} \sqrt{\frac{1}{2}} & \\ & 1 \end{pmatrix}$; $\Pi_1 = \begin{pmatrix} \sqrt{\frac{1}{2}} & \\ & 0 \end{pmatrix}$.

$$\rightarrow |\tilde{\psi}_0\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle; \quad |\tilde{\psi}_1\rangle = \sqrt{\frac{1}{3}}|00\rangle.$$

$p = \frac{2}{3}$: $|\psi_0\rangle = |\chi\rangle$

$p = \frac{1}{3}$: $|\psi_1\rangle = |00\rangle \longrightarrow$ no entanglement left!

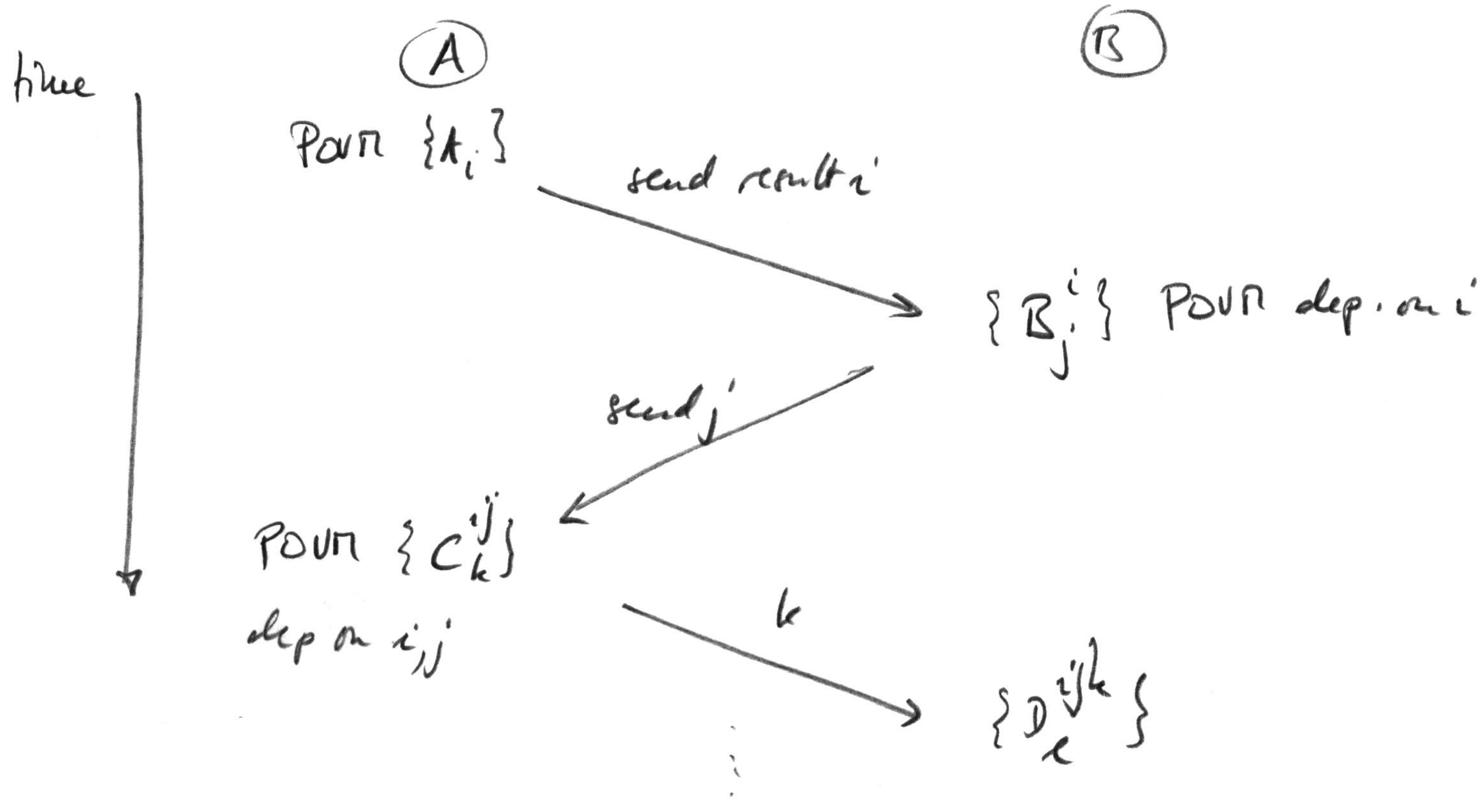
$\Rightarrow$ $|\chi\rangle \longrightarrow |\phi^+\rangle$ w/ prob. $p = 2/3$.

(will see: best possible!)

$\Rightarrow$ Conversion not reversible! (cannot be used to quantify entanglement)

## What is the best protocol?

General LOCC protocol:




etc.: any # of rounds!

$$\rho \longmapsto \sum{}' (\ldots C_k^{ij} A_i) \otimes (\ldots D_l^{ijk} B_j^i)\, \rho\, (\;)^\dagger \otimes (\;)^\dagger \;!$$

Very complicated structure!

But: For pure states, protocol can be replaced by

one-round protocol w/ one-way communication

$$\text{POVM } \{M_k\} \xrightarrow{k} U_k : \text{unitary},$$

A B

i.e. $|\psi\rangle \longrightarrow |\tilde{\psi}_k\rangle = M_k \otimes U_k |\psi\rangle$

POVM unitary

(Proof idea: A can "simulate" any meas. of B by a diff. meas. on her side, if state is known. ⟶ Homework!)

General protocol for ent. conversion:

$$|\psi\rangle \to |\tilde{\psi}_k\rangle = M_k \otimes U_k |\psi\rangle; \quad p_k = \| |\tilde{\psi}_k\rangle \|^2$$

For entanglement: $|\psi\rangle$, $|\psi_k\rangle = \frac{|\tilde{\psi}_k\rangle}{\||\tilde{\psi}_k\rangle\|}$ fully char. by Schmidt coefficients; and $U_k$ irrelevant

⟹ study instead possible conversions

$$\rho_A \longrightarrow \{p_k, \rho_{A,k}\}:$$

Under which conds. $\exists$ POVM $M_k$ s.th. $p_k \rho_{A,k} = M_k \rho M_k^\dagger$ ?

(Note: several $\rho_{A,k}$ might be equal.)

## 6) Single-copy protocols: majorization

<u>Def.</u>: For $\lambda \in \mathbb{R}^d_{\geq 0}$, let $\lambda^\downarrow = (\lambda_1^\downarrow, \ldots, \lambda_d^\downarrow)$, $\lambda_1^\downarrow \geq \lambda_2^\downarrow \geq \ldots \geq 0$

denote the <u>ordered version</u> of $\lambda$.

<u>Definition (Majorization)</u>: We say that <u>$\lambda$ is majorized by $\mu$</u> (or <u>$\mu$ majorizes $\lambda$</u>),

$$\lambda \prec \mu,$$

iff $\sum_{i=1}^{k} \lambda_i^\downarrow \leq \sum_{i=1}^{k} \mu_i^\downarrow$ $\forall k = 1, \ldots, d$, w/ equality for $k=d$.

<u>Theorem:</u> The following are equivalent:

(i) $\lambda \prec \mu$

(ii) there exist permutations $P_i$ & probabilities $q_i$ s.th.

$$\lambda = \sum q_i P_i \mu$$

(iii) there exists a doubly stochastic $Q$ (i.e. $Q_{ij} \geq 0$, $\sum_i Q_{ij} = \sum_j Q_{ij} = 1$ : rand. process w/ fpt. $(\frac{1}{d}, \ldots, \frac{1}{d})$)

s.th. $\lambda = Q\mu$.

((ii) $\Leftrightarrow$ (iii) follows from Birkhoff's thm: every $Q = \sum q_i P_i$)

Intuition: $\lambda \prec \mu \Leftrightarrow \lambda$ can be obtained by rand. permutation of $\mu$: it is "more random" (e.g. as a prob. distr.); "largest": $(1,0,\dots,0)$; "smallest": $(\frac{1}{d},\dots,\frac{1}{d})$.

Remarks:

- Majorization defines partial order on prob. distributions
- $\lambda \prec \mu$: $\lambda$ more disordered than $\mu$ (in part: more entropy)

  (Made rigorous by "Schur concavity/convexity": for a concave/convex $f(x)$, $F(\lambda)=\sum f(\lambda_i)$ fulfils $\lambda \prec \mu \Leftrightarrow F(\lambda) \gtreqless F(\mu)$)

Generalization to operators:

A hermitian matrix: $\lambda^\downarrow(A)$ = ordered eigenvalues of A.

Lemma: $\lambda^\downarrow(A+B) \prec \lambda^\downarrow(A)+\lambda^\downarrow(B)$

(Intuition: Eigenvals of A+B most ordered if in same basis.)

(Proof: Using Ky-Fan maximum principle:

$$\sum_{j=1}^k \lambda_j^\downarrow(A) = \max_P \mathrm{tr}(AP);\quad P \text{ all proj's of rank } P=k.$$

Then,

$$\sum_{j=1}^k \lambda_j^\downarrow(A+B) = \max_P \mathrm{tr}((A+B)P) \le$$

$$\le \max_P \mathrm{tr}(AP) + \max_P \mathrm{tr}(BP) = \sum_{j=1}^k \lambda_j^\downarrow(A) + \sum_{j=1}^k \lambda_j^\downarrow(B)$$

**Theorem (single-copy entanglement conversion):**

We can convert $|\psi\rangle \longrightarrow \{p_k, |\psi_k\rangle\}_{k=1}^K$ by LOCC if & only if
$\lambda^\downarrow(\rho) \prec \sum_{k=1}^K p_k \lambda^\downarrow(\rho_k)$, where $\rho = \mathrm{tr}_A |\psi\rangle\langle\psi|$, $\rho_k = \mathrm{tr}_A |\psi_k\rangle\langle\psi_k|$.

Proof: "$\Rightarrow$": Protocol: A does POVM $\{\Pi_k\}$; wlog Bob's unitary $U_k = \mathbb{1}$ (only Schmidt coeffs matter!).

Then, $\sum_{k=1}^K p_k \lambda^\downarrow(\rho_k) = \sum_{k=1}^K \lambda^\downarrow(p_k \rho_k) =$

$$= \sum_{k=1}^K \lambda^\downarrow\Big(\mathrm{tr}_A\big[(\Pi_k \otimes \mathbb{1})|\psi\rangle\langle\psi|(\Pi_k^\dagger \otimes \mathbb{1})\big]\Big)$$

$$\overset{\text{Lemma}}{\succ} \lambda^\downarrow\Big(\mathrm{tr}_A\Big[\underbrace{\sum_k \Pi_k^\dagger \Pi_k \otimes \mathbb{1}}_{=\mathbb{1}} |\psi\rangle\langle\psi|\Big]\Big) = \lambda^\downarrow(\rho) \ \checkmark$$

"$\Leftarrow$": $\lambda^\downarrow(\rho) \prec \sum p_k \lambda^\downarrow(\rho_k) \Rightarrow \exists\, P_j, q_j$ s.th. $\lambda^\downarrow(\rho) = \sum p_k q_j P_j \lambda^\downarrow(\rho_k)$

Wlog: $\rho, \rho_i$ diagonal $\rightarrow$ otherwise, add unitaries!

Def. $E_{kj}$ via $E_{kj}\sqrt{\rho} = \sqrt{p_k q_j}\sqrt{\rho_k}\, P_j^\dagger$. Then,

$$\sqrt{\rho}\Big(\sum_{kj} E_{kj}^\dagger E_{kj}\Big)\sqrt{\rho} = \sum_{kj} p_k q_j P_j \rho_k P_j^\dagger \overset{\rho,\rho_k \text{ diag.}}{=} \rho$$

$$\Rightarrow \sum_{kj} E_{kj}^\dagger E_{kj} = \mathbb{1}$$ (if $\rho$ invertible; otherwise any $E_{kj}$ on $\ker \rho$ will do)

And $E_{kj}\rho E_{kj}^{\dagger} = P_k q_j \rho_k \Rightarrow \sum_j E_{kj}\rho E_{kj}^{\dagger} = p_k \rho_k$ (65)

$\Rightarrow$ POVM for $\rho \longmapsto \{p_k, \rho_k\}$, i.e., $|\psi\rangle = \{p_k, |\psi_k\rangle\}$.

(Note: We bin several POVM ops $j$ to same outcome!)

Example: Optimal rate for $\left(\frac{1}{2}, \frac{1}{2}\right) \longleftrightarrow \left(\frac{2}{3}, \frac{1}{3}\right)$:

$$\left(\tfrac{1}{2}, \tfrac{1}{2}\right) \prec \left(\tfrac{2}{3}, \tfrac{1}{3}\right).$$

$$\left(\tfrac{2}{3}, \tfrac{1}{3}\right) \prec \tfrac{2}{3}\left(\tfrac{1}{2}, \tfrac{1}{2}\right) + \tfrac{1}{3}(1, 0) = \left(\tfrac{2}{3}, \tfrac{1}{3}\right)$$

max. value!

## c) Asymptotic protocols

single-copy protocol: not reversible, ent. is lost

(e.g. $\left(\frac{2}{3}, \frac{1}{3}\right)$: needs 1 ebit, gives "$\frac{2}{3}$ ebits").

Can we do better with more copies?

$$|\chi\rangle^{\otimes 2} \longrightarrow p_2 |\phi^+\rangle^{\otimes 2} + p_1 |\phi^+\rangle^{\otimes 2} \quad ?$$

$$|\chi\rangle^{\otimes 3} \longrightarrow p_3 |\phi^+\rangle^{\otimes 3} + p_2 |\phi^+\rangle^{\otimes 2} + \ldots$$

Average yield of max. ent. states:

$$\bar{p} = \frac{p_1 + 2p_2 + 3p_3 + \ldots}{k \leftarrow \# \text{ copies}}$$

Can we increase $\bar{p}$ by using more copies?

Yes! ($\rightarrow$ Homework)