Wrap-up previous lecture:

III.3. Applications of entanglement

What can A & B do if they share ent. pair?

a) Dense coding

Send 2 class. bits by sending 1 qubit + using 1 ent pair:

1 cbit + 1 qubit → 2 bits

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

A ~~~ B

A uses $U \in \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ to convert $|\phi^+\rangle$ to one Bell state

& sends her qubit to B.

→ B measures in Bell basis & recovers information.

b) Teleportation:

Send 1 qubit by sending 2 class. bits + using 1 ent. pair:

1 cbit + 2 bit → 1 qubit

A: $|X\rangle$ A $|\phi^+\rangle_B$ → B: $U|X\rangle$

meas. in Bell basis

$U = \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$

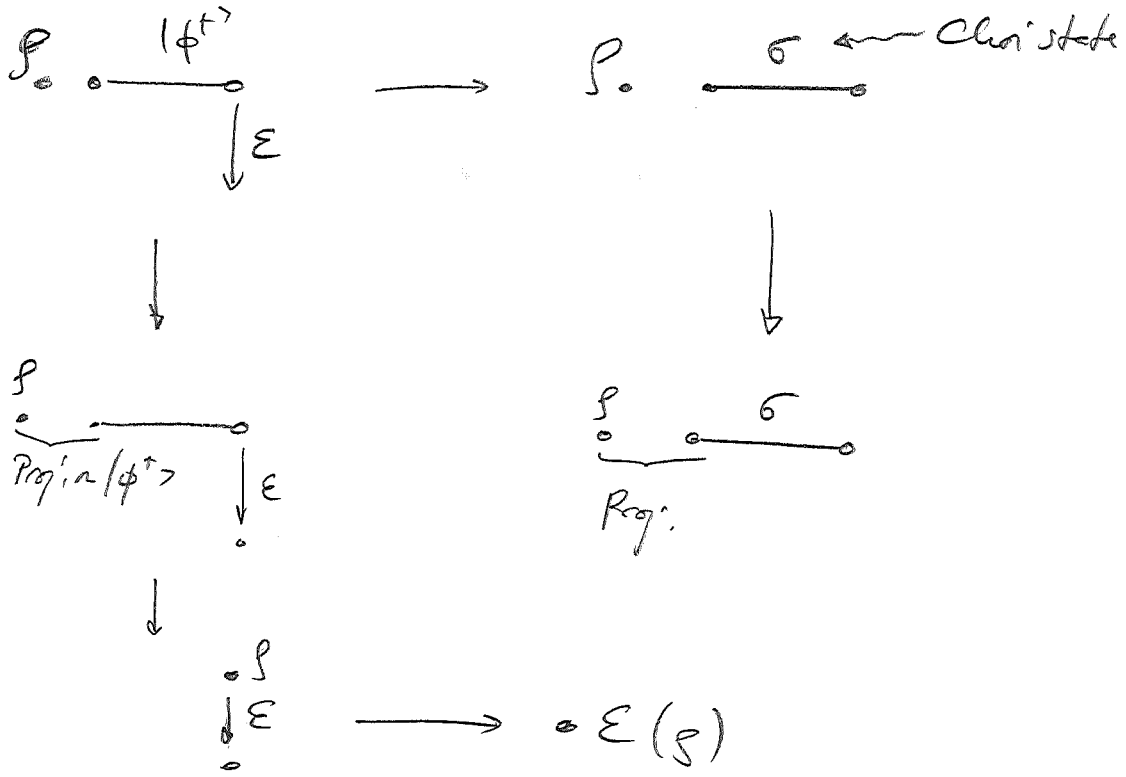
dep. on Bob's outcome

A sends meas. result → Bob can undo U!

Note: No info contained before class. comm.

→ no faster than light (FTL) communication!

Relation to Choi-Jamiołkowski isomorphism:



III.4. Entanglement conversion & quantification

a) Introduction & Setup

When can we convert ent. states into each other (with local operations)?

Relevance:

- Protocols might require dif. ent. states
- Use to quantify ent.: how many "e-bits" $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are "contained" in a state?

Know already: Same Schmidt coeffs ⇔ related by local unitary ⇔ same entanglement.

Example:

$$|\chi\rangle = \sqrt{\tfrac{2}{3}}|00\rangle + \sqrt{\tfrac{1}{3}}|11\rangle; \quad |\phi^+\rangle = \sqrt{\tfrac{1}{2}}|00\rangle + \sqrt{\tfrac{1}{2}}|11\rangle$$

Can we convert $|\phi\rangle \longrightarrow |\chi\rangle$?

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

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

$$\Rightarrow p = \tfrac{1}{2}: \; |\phi_0\rangle = \sqrt{\tfrac{2}{3}}|00\rangle + \sqrt{\tfrac{1}{3}}|11\rangle = |\chi\rangle \Rightarrow \text{OK} \checkmark$$

$p = \frac{1}{2}$: $|\phi_1\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$: same Schmidt coeffs., but A&B need to apply $\sigma_x \otimes \sigma_x$.

Protocol: A does POVM, sends result to Bob, who applies a unitary dep. on A's outcome.

Success prob. $p = \frac{1}{2}$.

But possible: We cannot get more copies since POVMs cannot increase Schmidt rank.

What about the converse: $|\chi\rangle \longrightarrow |\phi^+\rangle$?

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

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

$p_0 = \frac{2}{3}$: $|\psi_0\rangle = |x\rangle$

$p_0 = \frac{1}{3}$: $|\psi_0\rangle = |00\rangle$ → no entanglement.

$|x\rangle \longrightarrow |\phi^+\rangle$ w/ prob. $p = \frac{2}{3}$.

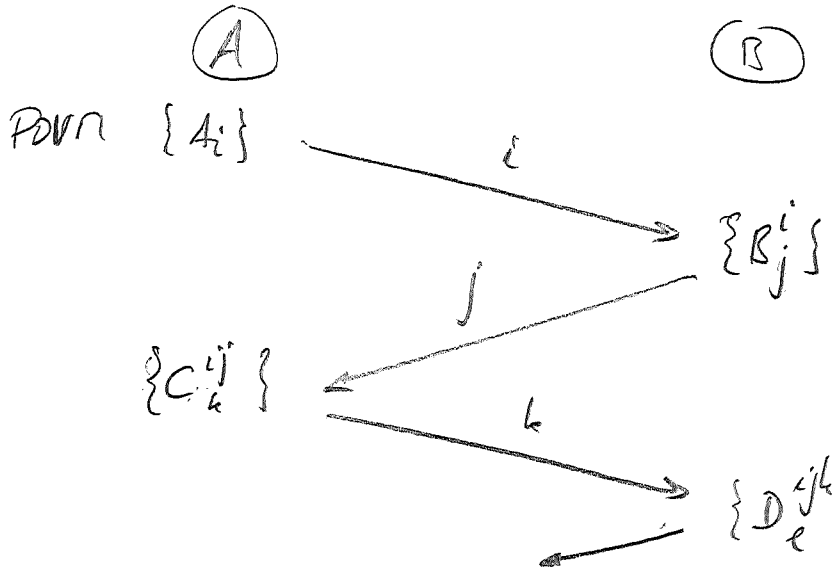
→ conversion not reversible! (→ cannot be used to assign one number to the entanglement)

Is this the best A & B can do?

<u>What is the optimal protocol?</u>

"Local operations & classical communication" (LOCC) protocols:

A does POVM, sends result to B, B does POVM, sends result to A ...



<u>arbitrary</u> many rounds!

$$\rho \longmapsto \sum \left(\sum_{\ell} D_\ell^{ijk} B_j^i\right) \otimes \left(\sum_k C_k^{ij} A_i\right) \rho \left(\ \right)^\dagger \otimes \left(\ \right)^\dagger \ !$$

But: For *pure* states, $A \nrightarrow B$ can replace this by a 1-round protocol w/ one-way comm.:

Proof: Homework. Idea: A can use ent. to simulate result of B's measurements ("quantum steering").

General protocol:

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

$$\left(\text{i.e., } |\psi_k\rangle = \frac{|\tilde{\psi}_k\rangle}{\||\tilde{\psi}_k\rangle\|} \text{ w/ prob. } p = \langle\tilde{\psi}_k|\tilde{\psi}_k\rangle\right)$$

$|\tilde{\psi}_k\rangle$ & $|\psi\rangle$ fully char. by Schmidt coeffs.

$\rightarrow$ sufficient to study possible conversions

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

of A's RDM (or, equiv., of Bob's by A's meas!), i.e.:

when $\exists$ POVM $M_{k,i}$ s.t. $p_k \rho_{A,k} = \tilde{\rho}_{A,k} = \sum_i M_{k,i} \rho M_{k,i}^\dagger$

Note: Will use $\tilde{\rho}_{A,k}$-notation w/out further def. in the following!

{ grouping of outcomes (cf. $|\phi^+\rangle \rightarrow |X\rangle$!)

6) Majorization

For $\lambda \in \mathbb{R}^d_{\geq 0}$, let $\lambda^{\downarrow} = (\lambda_1^{\downarrow}, \dots, \lambda_d^{\downarrow})$; $\lambda_1^{\downarrow} \geq \lambda_2^{\downarrow} \geq \dots \geq 0$

denote the ordered version of λ.

(Note: Most of the following holds also w/out ≥ 0.)

Definition (Majorization I):

We say that λ is majorized by μ (or μ majorizes λ),

$$\lambda \prec \mu,$$

if there exist permutations P_i & prob. q_i s.th.

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

(i.e., λ can be obtained from μ by rand. perm.: it is "more random")

("largest": $(1, 0, \dots 0)$; "smallest": $(\frac{1}{d}, \dots, \frac{1}{d})$)

Theorem: Definition I is equiv. to the following two Defs:

(→ cf. Homework!)

Definition (II): $\lambda \prec \mu :\Leftrightarrow \exists$ doubly stochastic Q

(i.e.: $Q_{ij} \geq 0$, $\sum_i Q_{ij} = \sum_j Q_{ij} = 1$: random process w. fixed pt. $(\frac{1}{d}, \dots, \frac{1}{d})$)

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

(Proof via Birkhoff's Thm: Every d.s. Q is of the form $Q = \sum q_i P_i$.)

Definition (III):

$$\lambda \prec \mu \iff \sum_{i=1}^{k} \lambda_i^{\downarrow} \leq \sum_{i=1}^{k} \mu_i^{\downarrow} \quad \forall k = 1, \dots, d, \text{ w/ equality for } k = d$$

Remarks:

- Majorization defines <u>partial order</u> on prob. distributions.
- $\lambda \succ \mu$: λ more disordered than μ (via path: entropy larger!)

We can also define Majorization for positive (or herm.) operators:

$$A \prec B \iff \lambda^{\downarrow}(A) \prec \lambda^{\downarrow}(B), \text{ with } \lambda^{\downarrow}(X) \text{ the ordered eigenvectors of } X.$$

<u>Theorem</u> (Ky-Fan maximum principle):

For A hermitian,

$$\sum_{j=1}^{k} \lambda_j^{\downarrow}(A) = \max_{P} \operatorname{tr}(AP),$$

with max. ovo all orth. projectors of rank k.

<u>Proof</u>: Let $A = \sum_{j=1}^{d} \lambda_j^{\downarrow}(A) |q_j\rangle\langle q_j|$. With the choice $P = \sum_{i=1}^{k} |q_i\rangle\langle q_i|$,

$$\operatorname{tr}(AP) = \sum_{j=1}^{k} \lambda_j^{\downarrow}(A).$$

For a general P, write $P = \sum_{i=1}^{k} |p_i\rangle\langle p_i|$, with an ONB $\{|p_i\rangle\}_{i=1}^{d}$. Then:

$$\langle p_i|A|p_i\rangle = \sum |\underbrace{\langle p_i|q_j\rangle}_{=u_{ij}}|^2 \lambda_i^{\downarrow}(A)$$

u_{ij} unitary $\Rightarrow \sum_i |u_{ij}|^2 = \sum_j |u_{ij}|^2 = 1$; u_{ij} dbl. stoch.

$$\Rightarrow \left(\langle p_j|A|p_j\rangle\right)_j \prec \lambda^{\downarrow}(A)$$

$$\Rightarrow \operatorname{tr}(AP) = \sum_{j=1}^{k} \langle p_j|A|p_j\rangle \leq \sum_{j=1}^{k} \lambda_i^{\downarrow}(A) \qquad \square$$

Corollary: $\lambda^{\downarrow}(A+B) \prec \lambda^{\downarrow}(A) + \lambda^{\downarrow}(B)$

Proof: $\sum_{i=1}^{k} \lambda_i^{\downarrow}(A+B) = \max_{P:\, \operatorname{rk} P = k} \operatorname{tr}\left(P(A+B)\right) \leq$

$$\leq \max_P \operatorname{tr}(PA) + \max_P \operatorname{tr}(PB) = \sum_{i=1}^{k} \lambda_i^{\downarrow}(A) + \sum_{i=1}^{k} \lambda_i^{\downarrow}(B)$$

$\square$

c) Single-copy entanglement cannot

Theorem: If we can convert $|\psi\rangle \to \{p_k, |\psi_k\rangle\}$ by LOCC, then $\lambda^{\downarrow}(\rho) \prec \sum p_k \lambda^{\downarrow}(\rho_k)$, with ρ, ρ_k as before (= the RDM of $|\psi\rangle, |\psi_k\rangle$).

Proof: We can choose $\rho = tr_A |\psi\rangle\langle\psi|$, $\rho_k = tr_A |\psi_k\rangle\langle\psi_k|$.

A does POVM $\{\Pi_{ki}\}$. We have then

$$\sum_{k=1}^{d} p_k \lambda^{\downarrow}(\rho_k) = \sum_k \lambda^{\downarrow}(\tilde{\rho}_k) = \sum_k \lambda^{\downarrow}\left(tr_A\left[\sum_i (\Pi_{ki} \otimes I)|\psi\rangle\langle\psi|(\Pi_{ki}^{\dagger} \otimes I)\right]\right)$$

$$\overset{\text{Corollary}}{\succcurlyeq} \lambda^{\downarrow}\left(tr_A\left(\sum_i (\Pi_{ki}^{\dagger}\Pi_{ki} \otimes I)|\psi\rangle\langle\psi|\right)\right) = \lambda^{\downarrow}(\rho). \quad \blacksquare$$

Conversely:

Theorem: Let $\lambda^{\downarrow}(\rho) \prec \sum p_i \cdot \lambda^{\downarrow}(\rho_i)$. Then, there is a POVM s.th. $\rho \longrightarrow \{p_i, \rho_i\}$ (i.e., a LOCC protocol for $|\psi\rangle \longrightarrow \{p_i, |\psi_i\rangle\}$).

Proof: $\lambda^{\downarrow}(\rho) \prec \sum p_i \cdot \lambda^{\downarrow}(\rho_i) \Rightarrow \exists P_j, q_j$ s.th. $\lambda^{\downarrow}(\rho) = \sum p_i P_j P_j^{\dagger} \lambda^{\downarrow}(\rho_i)$.

Wlog.: ρ, ρ_i all diagonal (otherwise, append unitaries).

Define E_{ij} via $E_{ij}\sqrt{\rho} = \sqrt{p_i q_j}\sqrt{\rho_i} P_j^{\dagger}$. Then,

$$\sqrt{\rho}\left(\sum_{ij} E_{ij}^{\dagger} E_{ij}\right)\sqrt{\rho} = \sum_{ij} p_i q_j P_j \rho_i P_j^{\dagger} \overset{\rho, \rho_i \text{ diag.}}{=} \rho$$

$$\Rightarrow \sum_{ij} E_{ij}^{\dagger} E_{ij} = \mathbb{1} \quad (\text{if } \rho \text{ invertible}).$$

(Note: ρ not inv. $\Rightarrow$ E_{ij} can be def. freely on ker ρ ✓)

Moreover, $E_{ij}\,\rho\,E_{ij}^{+} = p_i q_j \rho_i$

$$\Rightarrow \sum_j E_{ij}\,\rho\,E_{ij}^{+} = p_i \rho_i$$

$\Rightarrow$ LOCC-protocol for $\rho \longrightarrow \{p_i, \rho_i\}$. ∎

<u>Note:</u> The protocols we had initially for

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

were indeed optimal:

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

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

↑ max. possible value!

Avg. "extractable ent." in $|X\rangle = \sqrt{\tfrac{2}{3}}|00\rangle + \sqrt{\tfrac{1}{3}}|11\rangle$:

"$\frac{2}{3}$ e-bit".