III. Entanglement

1. Introduction

Consider bipartite pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

If $|\psi_P\rangle = |\phi^A\rangle \otimes |\phi^B\rangle$:
($|\phi^A\rangle \in \mathcal{H}_A$, $|\phi^B\rangle \in \mathcal{H}_A$)

A & B can describe all their measurements etc.
on $|\psi\rangle$ independently $\rightarrow$ no correlations.

We call such a state a product state.

Product states have Schmidt coefficients $(1, 0, \dots)$,

and $\rho_A = \mathrm{tr}_B |\psi_P\rangle\langle\psi_P| = |\phi^A\rangle\langle\phi^A|$,

$\rho_B = \mathrm{tr}_A |\psi_P\rangle\langle\psi_P| = |\phi^B\rangle\langle\phi^B|$

are pure states (i.e., rank-1 projectors).

$\Longleftrightarrow \quad \mathrm{tr}\,\rho_A^2 = \mathrm{tr}\,\rho_B^2 = 1$.

(Note: For general $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$ ← ensembles, $\sum p_i = 1$, we have

$\mathrm{tr}\,\rho^2 = \sum p_i^2 \leq 1$) "purity"

We call (pure) states which are not product states entangled.

Consider e.g. $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

- Measurement outcomes of A & B are anti-correlated
  → no independent description possible.
- $\rho_A = \rho_B = \frac{1}{2}\mathbb{1}$: all meas. outcomes equally likely.
  → $\mathrm{tr}\,\rho_A^2 = \mathrm{tr}\,\rho_B^2 < 1$ for all entangled states!
  → ent. states have more than one Schmidt-coeff. $\neq 0$.

Encoding of information:

$\dim(\mathbb{C}^2 \otimes \mathbb{C}^2) = 2^2$ → 2 bits!

Product states:

$|\psi_{ij}\rangle = |i\rangle|j\rangle$: orthonormal set.

→ encoding in product states.

→ A & B can read out information individually

Entangled states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

ONB

"Bell states",

"Bell basis"

→ encodes 2 bits of info

→ How much info can we retrieve w/ indiv. meas.?

A's meas. fully random → no info

→ total info at most 1 bit!

A & B meas both in Z basis:

→ recov if equal (ϕ's) or different (ψ's)

Similar w/ X-basis: + or −, etc.

→ 2 bit of info, but only 1 bit can be recovered locally ⟹ info hidden in (non-classical) correlations

→ data hiding schemes!

Goals of study of entanglement:

- How non-classical are entangled states?
- What can we do with entangled states? ("resources")
- How can we quantify the amount of entanglement?
- How can we manipulate entanglement?
- What about entanglement in mixed states?

2. Bell inequalities

How non-local are entangled states?

Consider the following game of A+B with coins:

- A+B get each a set of 3 coins $(0,1,2)$ prepared in some way by C.
- A and B can only each look at one coin; they get heads $= +1$ or tails $= -1$. Let us denote the result by $a_i = \pm 1$ and $b_j = \pm 1$ $(i,j = 0,1,2)$.
- If A & B look at the same coin, they always get the same result, $a_i = b_i$.
- Can A infer the value of two coins?

  Idea: A looks at i; Bob at $j = i' \neq i$.

  Since $a_{i'} = b_{i'}$, they now know a_i and $a_{i'}$.

- What can we say about the probability

$$p(a_i = a_{i'}) \; ?$$

$$p(a_0 = a_1) + p(a_1 = a_2) + p(a_2 = a_0) \geq 1,$$

since in each instance, at least two coins must be equal.

$$\Rightarrow p(a_0 = b_1) + p(a_1 = b_2) + p(a_2 = b_0) \geq 1 \; !$$

What happens in a quantum version of this experiment?

A & B share an entangled state, and perform proj. measurement along three different axes with outcomes $\pm 1 \longrightarrow$ meas operators a_i and b_j.

A & B share $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

We have $(\vec{\sigma}^A + \vec{\sigma}^B)|\psi^-\rangle = 0$

$$\left[\text{i.e. } (\sigma_i^A + \sigma_i^B)|\psi^-\rangle = 0 \ \forall i, \ \vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)\right]$$

Then, $\langle\psi^-|(\vec{\sigma}^A \cdot \vec{u})(\underbrace{\vec{\sigma}^B \cdot \vec{w}}_{= -\vec{\sigma}^A})|\psi^-\rangle$

$$= -\langle\psi^-|(\vec{\sigma}^A \cdot \vec{u})(\vec{\sigma}^A \cdot \vec{w})|\psi^-\rangle$$

$$= -\sum_{ij} u_i w_j \, \mathrm{Tr}\left(\underbrace{\rho_A}_{=\frac{1}{2}\mathbb{1}} \sigma_i^A \sigma_j^A\right) = -\sum_i u_i w_i = -\vec{u}\cdot\vec{w}$$

$$= -\cos\theta$$

θ: angle between $\vec{u}$ & $\vec{w}$.

Measurement of A/B along $\vec{u}$ / $\vec{w}$:

$\longrightarrow$ projections $E_\pm(\vec{u}) = \frac{1}{2}\left(\mathbb{1} \pm \vec{u}\cdot\vec{\sigma}\right)$

$$P(\pm1,\pm1) = \langle\psi^-| E_\pm(\vec{u})\, E_\pm(\vec{w}) |\psi^-\rangle$$

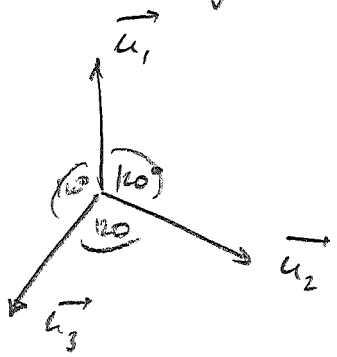
$$= \frac{1}{4}\langle\psi^-| \underbrace{\mathbb{1}}_{\to 1} \pm \underbrace{\vec{u}\cdot\vec{\sigma}_A}_{\to 0} \pm \underbrace{\vec{w}\cdot\vec{\sigma}_B}_{\to 0} + \underbrace{(\vec{u}\cdot\vec{\sigma}_A)(\vec{w}\cdot\vec{\sigma}_B)}_{\to -\cos\Theta} |\psi^-\rangle$$

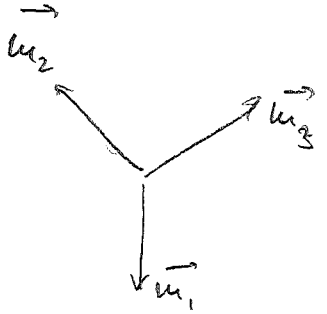
$$= \frac{1}{4}(1-\cos\Theta)$$

$$P(\pm1,\mp1) = \frac{1}{4}(1+\cos\Theta).$$

$$\Rightarrow P_{\text{equal}} = \frac{1}{2}(1-\cos\Theta);\quad P_{\text{different}} = \frac{1}{2}(1+\cos\Theta)$$

Now let A measure along





in the X-Z-plane, and Bob along $\vec{w}_i = -\vec{u}_i$

- A+B measure in same bases:

$$P_{\text{equal}} = \frac{1}{2}(1-\cos 180°) = 1 \qquad \checkmark$$

- A+B measure in different bases:

$$P_{equal} = \frac{1}{2}\left(1 - \underset{\parallel}{\cos\theta}\right) = \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$$

$$\theta = \pm 60°$$

$$\Rightarrow \cos\theta = +1/2$$

$$\Rightarrow P(a_1 = b_2) + P(a_2 = b_3) + P(b_3 = a_1) = \frac{3}{4} < 1 \; !$$

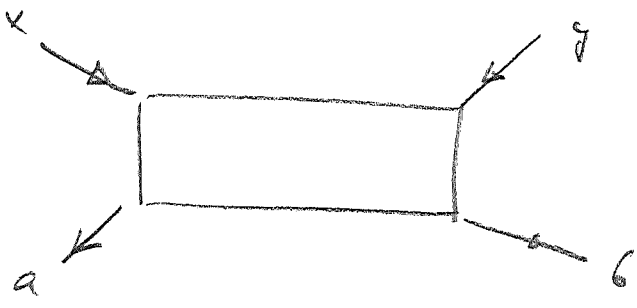
↯

→ Quantum mechanical predictions incompatible with a local realistic description!

→ We cannot assign values to observables we have not measured ("realism").

Non Bell inequalities:

Formal setup:



x, y: measurement directions (input)

a, b: values of observables (output)

Which output distributions $P(a,b|x,y)$ are consistent with a given physical theory?

Local hidden variable (LHV) models – local realism:

All outcomes are given through some "hidden" variable which is set beforehand (no faster-than-light):

$$P(a,b|x,y) = \sum_\lambda p_\lambda P^A_\lambda(a|x) P^B_\lambda(b|y)$$

- λ: hidden variable
- p_λ: prob. over λ
- $P^A_\lambda(a|x)$, $P^B_\lambda(b|y)$: can be deterministic (encode in λ)

Consider now $x=0,1$ and $y=0,1$, with outcomes (measurements) $a_0, a_1, b_0, b_1 = \pm 1$.

Since $a_i = \pm 1$, $b_i = \pm 1$:

$$C = (a_0+a_1)b_0 + (a_0-a_1)b_1 = \pm 2$$

$$\Rightarrow |\langle C \rangle| \leq \langle |C| \rangle = 2$$

($\langle \cdot \rangle$: avg. over p)

CHSH equality (Clauser, Horne, Shimony, Holt):

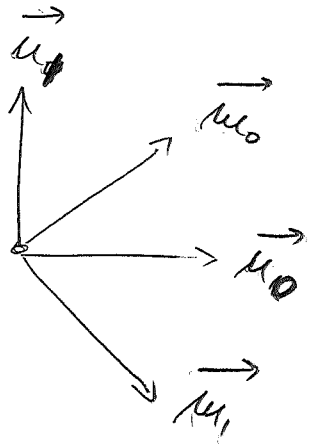
$$\left| \langle a_0 b_0 \rangle + \langle a_1 b_0 \rangle + \langle a_0 b_1 \rangle - \langle a_1 b_1 \rangle \right| \leq 2$$

Quantum mechanics:

Use $|\psi^-\rangle$;

$a_i = \vec{\sigma}^A \cdot \vec{u}_i$

$b_i = \vec{\sigma}^B \cdot \vec{u}_i$



$$\langle a_i b_j \rangle = -\cos\theta$$

$$\langle a_0 b_0 \rangle = \langle a_1 b_0 \rangle = \langle a_0 b_1 \rangle = \cos 45° = \frac{1}{\sqrt{2}}$$

$$\langle a_1 b_1 \rangle = \cos 135° = -\frac{1}{\sqrt{2}}$$

$$\Rightarrow \left| \langle a_0 b_0 \rangle + \langle a_1 b_0 \rangle + \langle b_0 a_1 \rangle - \langle a_1 b_1 \rangle \right| = 2\sqrt{2} > 2.$$

→ Incompatible w/ LHV models.

→ Not: Unlike original Bell inequality, does not require knowledge of eg. correlations in some basis.

Lecture 7

(I) Protocols

Noiseless qubit channel
Noiseless classical bit channel
Noiseless entanglement
} nonlocal unit resource

Nonlocal : two spatially separated parties share it or if one party uses it to communicate to another

Unit resource : if it comes in some "gold standard" form, such as qubits, classical bits or entangled bits (ebits)

- Noiseless qubit channel : any mechanism that implements the following map

$$|i\rangle_A^* \to |i\rangle_B \quad (\text{i.e. } |\varphi_i\rangle_A \to |\psi_i\rangle_B),$$

where $i \in \{0, 1\}$, $\{|0\rangle_A, |1\rangle_A\}$ is some orthonormal basis on Alice's system

do not have to be the same → $\{|0\rangle_B, |1\rangle_B\}$ is some orthonormal basis on Bob's system

The above map is linear and preserves superposition states

$$\alpha|0\rangle_A + \beta|1\rangle_A \to \alpha|0\rangle_B + \beta|1\rangle_B.$$

Noiseless qubit channel can be written as:

$$\sum_{i=0}^{1} |i\rangle^B \langle i|^A .$$

We label the communication resource of a noiseless qubit channel as follows:

$[q \to q]$ — one forward use of a noiseless qubit channel.

- A noiseless classical bit channel: any mechanism that implements the following map:

$$|i\rangle_A \to |i\rangle_B$$

$$|i\rangle_A \to 0 \text{ for } i \neq j,$$

where $i, j \in \{0, 1\}$ and orthonormal bases are again arbitrary. We can write it as:

$$\rho \to \sum_{i=0}^{1} |i\rangle^B \langle i|^A \rho |i\rangle^A \langle i|^B$$

This resource is weaker than noiseless qubit channel, since it does not preserve superposition states.

We denote the communication resource of a noiselers classical bit channel as:

$[c \to c]$ — one forward use of a noiseless classical bit channel.

It is possible for a noiseless qubit channel to simulate a noiseless classical bit channel and we denote this fact with the following resource inequality:

$$[q \to q] \geq [c \to c].$$

- Shared entanglement resource.

The "ebit" is our "gold standard" resource for pure bipartite (two-party) entanglement.

An ebit is the following Bell state:

$$|\Phi^+\rangle_{AB} = \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}},$$

where Alice posses the first qubit and Bob posses the second. The resource is denoted as $[qq]$.

(I.1) Entanglement Distribution

We show how a noiseless qubit channel can generate a noiseless ebit. The protocol consists of two steps:

1. Alice prepares a Bell state locally in her lab: she first prepares two qubits $|0\rangle^A |0\rangle^{A'}$ and then performs a Hadamard gate on qubit A:

$$\left(\frac{|0\rangle^A + |1\rangle^A}{\sqrt{2}}\right) |0\rangle^{A'}.$$

She then performs a CNOT gate with qubit A as the source and qubit A' as the target. The state becomes

$$\frac{|00\rangle^{AA'} + |11\rangle^{AA'}}{\sqrt{2}} = |\Phi^+\rangle^{AA'}$$

2. Alice sends qubit A' to Bob with one use of noiseless qubit channel. Alice & Bob share the ebit $|\Phi^+\rangle_{AB}$.

The resource inequality of this protocol is

$$[q \to q] \geq [qq]$$

Notes: notice the difference between

Bell state – local state is Alice's lab

and

ebit – a nonlocal resource shared between Alice and Bob.

I. 2 Quantum Super-Dense Coding

We know that with one use of noiseless quantum channel we can transmit one classical bit.

Super-dense coding doubles classical bits by using noiseless entanglement.

1. Suppose Alice and Bob share an ebit $|\Phi^+\rangle_{AB}$.
   Alice applies one of four unitary operations $\{I, X, Z, XZ\}$ to her side of the above state. The state becomes one of the four Bell states, depending on the message that Alice chooses:

   $$|\Phi^+\rangle_{AB},\ |\Phi^-\rangle_{AB},\ |\Psi^+\rangle_{AB},\ |\Psi^-\rangle_{AB}$$

2. Alice transmits her qubit to Bob with one use of noiseless qubit channel

3. Bob performs a Bell measurement (a meas. in the basis $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$ to distinguish the four states.

Thus Alice can transmit 2 class. bits (corresponding to 4 mess.) if she uses a noiseless q.ch. and shares an ebit with Bob.

The super-dense coding protocol implements the following resource inequality:

$$[q\,q] + [q \to q] \geq 2\,[c \to c].$$

I.3 Quantum Teleportation

The protocol destroys the quantum state of a qubit in one location and recreates it on a qubit at a distant location, with the help of shared entanglement.

Algebraic calculations in preparation for the protocol:

Consider a qubit $|\psi\rangle^{A'}$ that Alice possesses, where

$$|\psi\rangle_{A'} = \alpha|0\rangle_{A'} + \beta|1\rangle_{A'}.$$

Suppose Alice also shares a maximally entangled state $|\Phi^+\rangle_{AB}$ with Bob. The joint state of the systems A, A', B is as follows: $|\psi\rangle_{A'}\,|\Phi^+\rangle_{AB}$

$$|\psi\rangle_{A'}\,|\Phi^+\rangle_{AB} = \left(\alpha|0\rangle_{A'} + \beta|1\rangle_{A'}\right)\left(\frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|000\rangle_{A'AB} + \beta|100\rangle_{A'AB} + \alpha|011\rangle_{A'AB} + \beta|111\rangle_{A'AB}\right]$$

use Bell states on system $A'A$:

$$|00\rangle_{A'A} = \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{A'A} + |\Phi^-\rangle_{A'A}\right)$$

$$|10\rangle_{A'A} = \frac{1}{\sqrt{2}}\left(|\Psi^+\rangle_{A'A} - |\Psi^-\rangle_{A'A}\right)$$

$$|01\rangle = \cdots$$

$$|11\rangle = \cdots$$

$$= \frac{1}{2}\left[\alpha\left(|\Phi^+\rangle + |\Phi^-\rangle\right)_{A'A}|0\rangle_B + \beta\left(|\Psi^+\rangle - |\Psi^-\rangle\right)_{A'A}|0\rangle_B\right.$$

$$\left. + \alpha\left(|\Psi^+\rangle + |\Psi^-\rangle\right)_{A'A}|1\rangle_B + \beta\left(|\Phi^+\rangle - |\Phi^-\rangle\right)_{A'A}|1\rangle_B\right]$$

$$= \frac{1}{2}\Big[|\Phi^+\rangle_{A'A} (\alpha|0\rangle + \beta|1\rangle)_B + |\Phi^-\rangle_{A'A} (\alpha|0\rangle - \beta|1\rangle)_B$$
$$+ |\Psi^+\rangle_{A'A} (\alpha|1\rangle + \beta|0\rangle)_B + |\Psi^-\rangle_{A'A} (\alpha|1\rangle - \beta|0\rangle)_B \Big]$$

using Pauli matrices X, Z and their action on $|\psi\rangle$:

$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$
$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$
$$XZ|\psi\rangle = \alpha|1\rangle - \beta|0\rangle$$

$$= \frac{1}{2}\Big[|\Phi^+\rangle_{A'A} |\psi\rangle_B + |\Phi^-\rangle_{A'A} Z|\psi\rangle_B + |\Psi^+\rangle_{A'A} X|\psi\rangle_B + |\Psi^-\rangle_{A'A} XZ|\psi\rangle_B \Big].$$

Quantum teleportation protocol:

1. Alice possesses a qubit $|\psi\rangle_A$, and shares an ebit with Bob. She performs a Bell measurement on system $A'A$. The state collapses to one of the following four states with uniform probability:

$$|\Phi^+\rangle_{A'A} |\psi\rangle_B$$
$$|\Phi^-\rangle_{A'A} Z|\psi\rangle_B$$
$$|\Psi^+\rangle_{A'A} X|\psi\rangle_B$$
$$|\Psi^-\rangle_{A'A} XZ|\psi\rangle_B$$

2. Notice that the state is a product state with respect to the cut $A'A - B$. At this point Alice already knows what state Bob has, because she knows the result of the measurement. On the other hand, Bob doesn't know anything about his state.

2. Alice transmits two classical bits to Bob that indicate which of the four measurement results she obtains. Now Bob knows which operation he needs to perform in order to restore his state to Alice's original $|\psi\rangle$.

3. Bob performs the restoration operation: I, X, Z, XZ

The resource inequality for q. teleportation is as follows:

$$[qq] + 2[c \to c] \geq [q \to q].$$

(II) Implementation of Choi-Jamiołkowski iso via teleportation

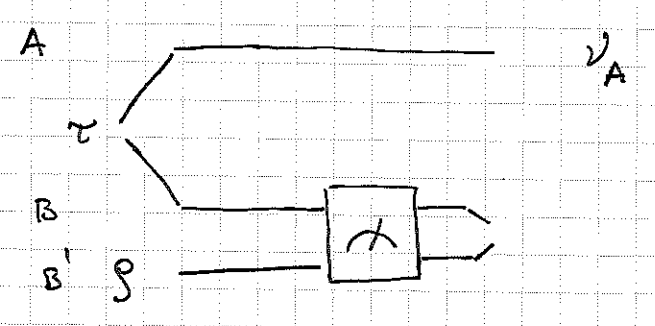
If T is a quantum channel then its Jam. state τ can operationally be obtained by letting T act on a max. entangled state.

Converse? Given τ, how to implement T as an action on any state ρ?

1. Alice & Bob share state $\tau = (T_A \otimes 1_B)|\Omega\rangle\langle\Omega|$, where $|\Omega\rangle = \sum_i \frac{1}{\sqrt{d}} |ii\rangle_{AB}$.

2. Bob also has a state ρ (on system B'). He performs a measurement on his system BB' using a POVM which contains state $\omega = |\Omega\rangle\langle\Omega|$.

3. Alice's state after the measurement is $T(\rho)$ if Bob has obtained a meas. outcome corresp. to ω.



Denote Alice's state by ν_A after a succesful Bob's measurement, which occurs with prob. p.

$$\nu_A = \frac{1}{p} \mathrm{Tr}_{BB'} \left((\mathbb{1}_A \otimes \omega_{BB'}) (\tau_{AB} \otimes \rho_{B'}) (\mathbb{1}_A \otimes \omega_{BB'}) \right)$$

To show that $\nu_A = T(\rho)$ compute the exp. value for any A:

$$p \,\mathrm{Tr}(A \nu_A) = \mathrm{Tr}\left((A_A \otimes \mathbb{1}_{BB'}) (\mathbb{1}_A \otimes \omega_{BB'}) (\tau_{AB} \otimes \rho_{B'}) (\mathbb{1}_A \otimes \omega_{BB'}) \right)$$

$$= \mathrm{Tr}\left((\tau_{AB} \otimes \rho_{B'}) (A_A \otimes \omega_{BB'}) \right) \circledast$$

Remind that $\omega = \frac{1}{d} \sum_{ij} |ix_j| \otimes |ix_j|_{B'}$.

Denote the coeff. $\rho = \sum_{kl} \lambda_{kl} |k\rangle\langle l|$ in the above basis.

$$\circledast \; \mathrm{Tr}\left((\tau_{AB} \otimes \sum_{kl} \lambda_{kl} |k\rangle\langle l|_{B'}) (A \otimes \frac{1}{d} \sum_{ij} |ix_j|_B \otimes |ix_j|_{B'}) \right)$$

$$= \frac{1}{d} \sum_{\substack{kl \\ ij}} \mathrm{Tr}\left(\tau (A_A \otimes |ix_j|_B) \otimes \lambda_{kl} |k\rangle\langle l| ix_j|_{B'} \right)$$

$$= \begin{cases} l = i \\ k = j \end{cases} \text{– taking a trace over } B'$$

$$= \frac{1}{d} \mathrm{Tr}\left(\tau \left(A \otimes \underbrace{\sum_{ij} |ix_j| \lambda_{ji}}_{\rho^T} \right) \right) = \mathrm{Tr}(\tau A \otimes \rho^T) \frac{1}{d}$$

$$= \frac{1}{d^2} \mathrm{Tr}(A T(\rho))$$

Therefore $\nu_A = T(\rho)$ and $p = \frac{1}{d^2}$.

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

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

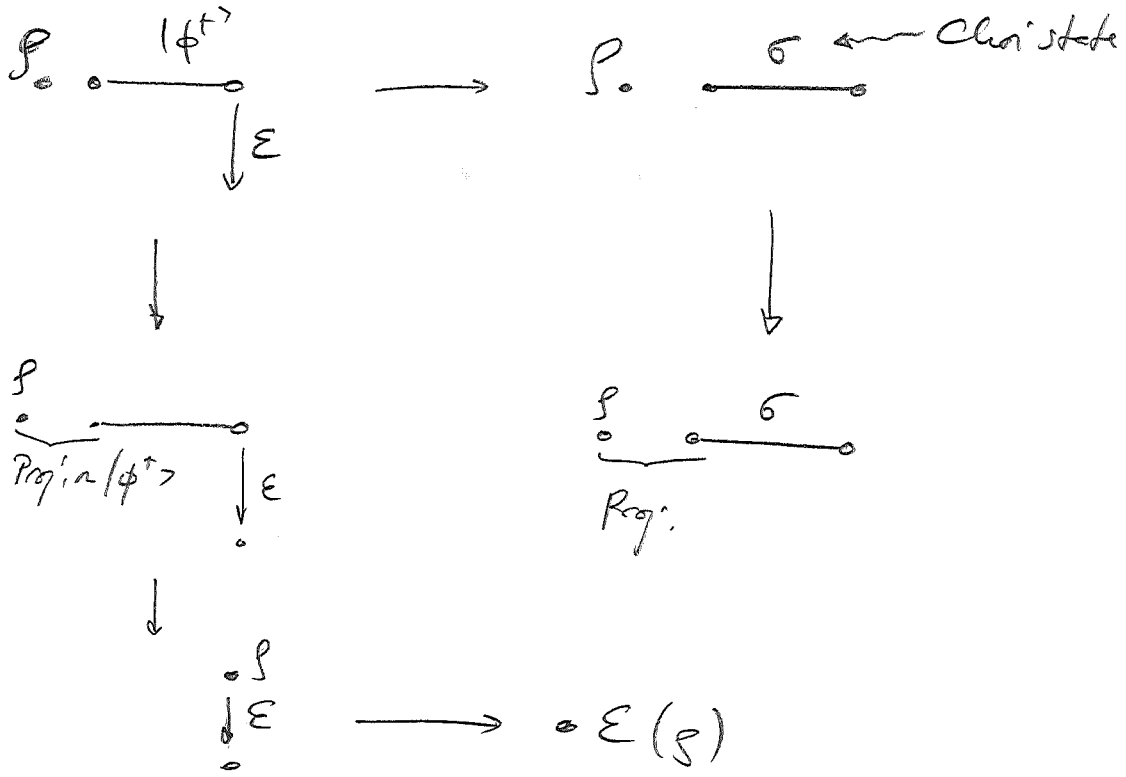
dep. on Bob's outcome

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. $p = \frac{2}{3}$.

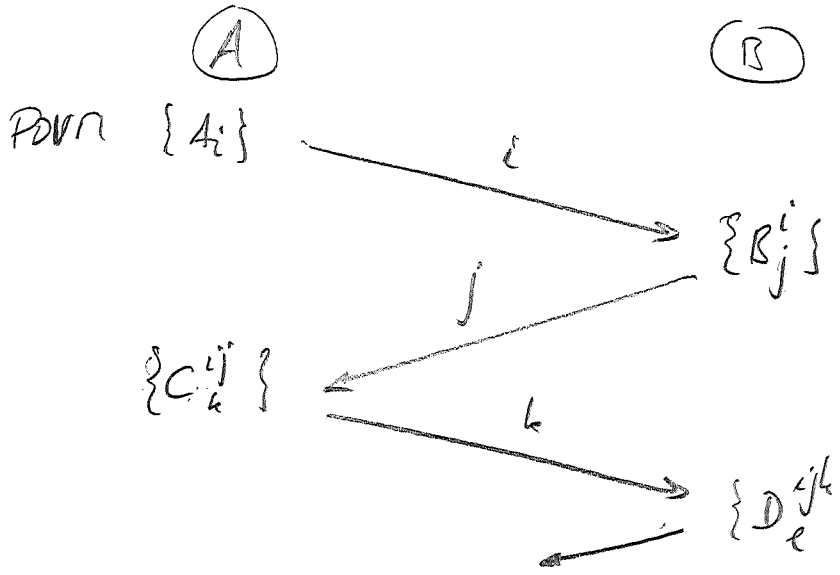
→ conversion not reversible! (→ cannot be used to assign one number to the entanglement)

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".

d) Asymptotic protocols

Single-copy conversion: not reversible.

→ at least two numbers to quantify ent.:

ebits needed to *initial* state

extractable ebits.

Can we do better w/ more copies?

$$|\chi\rangle^{\otimes 2} = \left(\sqrt{\tfrac{2}{3}}|00\rangle + \sqrt{\tfrac{1}{3}}|11\rangle\right)^{\otimes 2} \longleftrightarrow |\phi^+\rangle^{\otimes ?}$$

$|\phi^+\rangle^{\otimes 2} \to |\chi\rangle^{\otimes 2}$:

$$\left(\tfrac{4}{9}, \tfrac{2}{9}, \tfrac{2}{9}, \tfrac{1}{9}\right) \prec \left(\tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}\right)$$

$p=1$ & best possible as Schmidt rank cannot be increased by POVM.

$|\chi\rangle^{\otimes 2} \to |\phi^+\rangle^{\otimes ?}$.

$$\left(\tfrac{4}{9}, \tfrac{2}{9}, \tfrac{2}{9}, \tfrac{1}{9}\right) \prec p\left(\tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}\right) + q\left(\tfrac{1}{2}, \tfrac{1}{2}, 0, 0\right) + (1-p-q)(1,0,0,0)$$

Optimum: $p = \frac{2}{3}$, $q = \frac{1}{9}$:

$$\left(\tfrac{4}{9}, \tfrac{2}{9}, \tfrac{1}{6}, \tfrac{1}{6}\right).$$

$p = \frac{2}{3}$: 2 copies
$q = \frac{1}{9}$: 1 copy

} asymp. yield per copy of $|x\rangle$:

$$\frac{2 \times \frac{2}{3} + 1 \times \frac{1}{9}}{2} = \frac{2}{3} + \frac{1}{18} > \frac{2}{3} \; !$$

$\Rightarrow$ Improved yield as compared to 1-copy protocol!

How good can we get by using $N \to \infty$ copies?

Requirements for asymptotic protocols:

$\to$ convert $|\phi^+\rangle^{\otimes m} \longleftrightarrow |x\rangle^{\otimes n}$ with

rate $\frac{n}{m} \to R > 0$ for $n, m \to \infty$

$\to$ success prob. $p \to 1$ for $n \to \infty$

$\to$ Conversion need not be perfect: sufficient if distance from correct state $\delta \to 0$ as $n \to \infty$.

How to measure error δ?

Use $\delta = 1 - F$ w "fidelity" $F = |\langle \psi | \phi \rangle|^2$

δ bounds error on any observable O:

$$|\langle \psi | O | \psi \rangle - \langle \phi | O | \phi \rangle| \leq 2\sqrt{\delta}\, \|O\|_\infty \quad (\to \text{Homework})$$

i.e.: $\delta \to 0 \Rightarrow$ states indistinguishable by any measurement!

Now consider $|\chi\rangle = \sum \sqrt{p(x)}\, |x\rangle_A |x\rangle_B$, $x = 1, \dots, d$

$$|\chi\rangle^{\otimes n} = \sum_{x_1 \dots x_n} \sqrt{p(x_1) \cdot \dots \cdot p(x_n)}\; |x_1, \dots, x_n\rangle |x_1, \dots, x_n\rangle$$

sequence $x_1, \dots, x_n$ are indep. & identically distributed (i.i.d.) random variables w/ prob. $p(x_i)$

Law of large numbers (L.L.N.)

$$\forall \varepsilon > 0 \;\; \forall \delta > 0 \;\; \exists N \;\; \forall n \geq N \quad p\left(\left| \frac{1}{n} \sum_{i=1}^{n} x_i - E(x) \right| \geq \varepsilon \right) \leq \delta$$

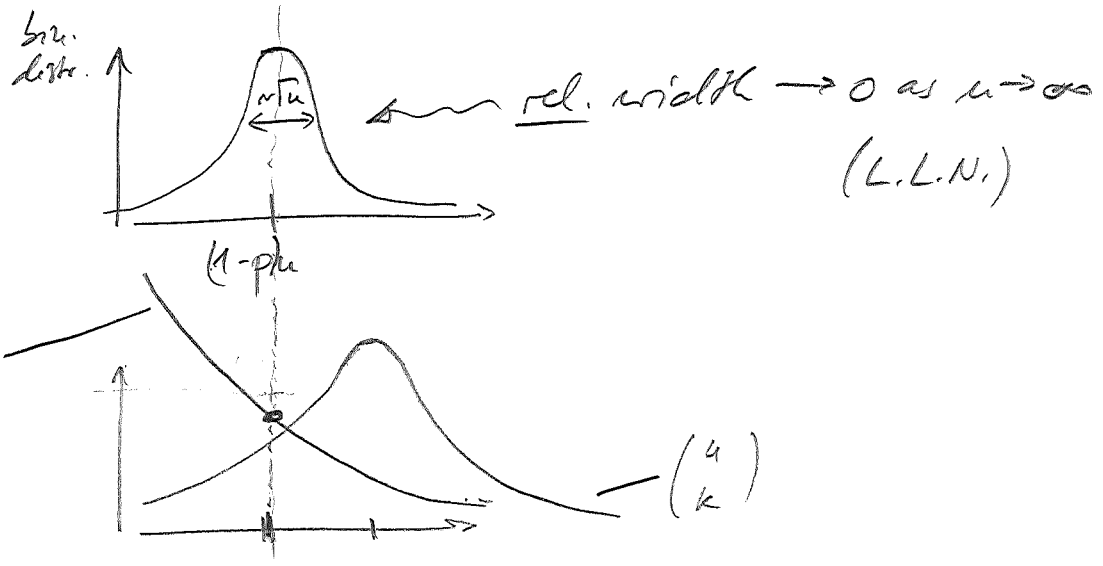
with $E(x) = \sum_x p(x)\, x$.

(i.e., $p(|\dots| \geq \varepsilon) \to 0 \;\; \forall \varepsilon$)

What is the typical output of an i.i.d. source?

E.g.: $x = 0, 1$; $p_0 \equiv p$; $p_1 = 1-p$:

$\to$ Binomial distr. $p^k (1-p)^{n-k} \binom{n}{k}$:



Typ. output: expect output x $n \cdot p(x)$ times.

$$\Rightarrow p(x_1, \dots, x_n) = p(x_1) \cdot \dots \cdot p(x_n) \approx p(1)^{np(1)} \cdot \dots \cdot p(d)^{np(d)}$$

base 2

$$\Rightarrow -\log p(x_1, \dots, x_n) \approx n \cdot \underbrace{\left(-\sum_x p(x) (\log p(x)) \right)}_{=: H(p)}$$

Shannon entropy of p.

$\Rightarrow$ expect typically $p(x_1, \dots, x_n) \approx 2^{-nH(p)}$,

and there are about $2^{nH(p)}$ such typical sequences.

More precisely:

Def.: We say that $x_1, \dots, x_n$ is a ε-typical sequence if

$$2^{-n(H(p)+\varepsilon)} \leq p(x_1, \dots, x_n) \leq 2^{-n(H(p)+\varepsilon)}$$

Denote the set of ε-typ. seq. by $T(n, \varepsilon)$.

Theorem:

(1) $\forall \varepsilon > 0 \ \forall \delta > 0 \ \exists N \ \forall n \geq N$: a random sequence of len. n is ε-typical w/ prob. $\geq 1 - \delta$.

(2) $\forall \varepsilon > 0 \ \forall \delta > 0 \ \exists N \ \forall n \geq N$.

$$(1-\delta) 2^{n(H(p)-\varepsilon)} \leq |T(n, \varepsilon)| \leq 2^{n(H(x)+\varepsilon)}$$

Proof:

① $-\log p(x_i)$ is i.i.d. random.

$$\overset{\text{L.L.N.}}{\Longrightarrow} \forall \varepsilon, \delta \; \exists N \; \forall n \geq N \; P\Big(\Big| \underbrace{\frac{1}{n} \sum_{i=1}^{n} -\log p(x_i)}_{= -\log p(x_1, \dots, x_n)} - \underbrace{E\big(-\log p(x)\big)}_{= H(p)} \Big| \geq \varepsilon \Big) \leq \delta$$

$$\Longrightarrow \quad P\Big(\Big| -\tfrac{1}{n} \log p(x_1, \dots, x_n) - H(p) \Big| \geq \varepsilon \Big) \leq \delta$$

$$\Longrightarrow \text{w. prob.} \geq 1-\delta, \quad -n\big(H(p)+\varepsilon\big) \leq \log p(x_1, \dots, x_n) \leq -n\big(H(p)-\varepsilon\big)$$

□

② $$1 \geq \sum_{x_1 \dots x_n \in T(n,\varepsilon)} p(x_1, \dots, x_n) \geq \sum_{T(n,\varepsilon)} 2^{-n(H(p)+\varepsilon)} = \big|T(n,\varepsilon)\big| \cdot 2^{-n(H(p)+\varepsilon)}$$

$$1-\delta \leq \sum_{T(n,\varepsilon)} p(x_1, \dots, x_n) \leq \big|T(n,\varepsilon)\big| \; 2^{-n(H(p)-\varepsilon)}$$

□

In brief: ε-Typ. sequence $\iff$ $\dfrac{\log p(x_1, \dots, x_n)}{n}$ ε-close to $H(p)$.

Asympt., a sequence is ε-typical w/ $p \to 1$,

and there are $\sim 2^{nH(p)}$ ε-typ. seq.

Application to our question:

$$|\chi\rangle = \sum_x \sqrt{p(x)}\, |x\rangle_A |x_B\rangle$$

$$\Rightarrow |\chi\rangle^{\otimes n} = \sum \sqrt{p(x_1)\cdots p(x_n)}\, |x_1,\dots,x_n\rangle |x_1,\dots,x_n\rangle$$

Fix $\varepsilon > 0$.

Define $|\vartheta_n\rangle := \sum_{x_1,\dots,x_n \in T(n,\varepsilon)} \sqrt{p(x_1)\cdots p(x_n)}\, |x_1,\dots,x_n\rangle |x_1,\dots,x_n\rangle$

and $$|\hat{\vartheta}_n\rangle := \frac{|\vartheta_n\rangle}{\sqrt{\langle \vartheta_n | \vartheta_n \rangle}}$$

We have

$$\langle \hat{\vartheta}_n | \chi^{\otimes n} \rangle = \frac{\overbrace{\sum_{\varepsilon\text{-typ.}} p(x_1,\dots,x_n)}^{\geq 1-\delta \text{ for sufficiently large } n}}{\sqrt{\sum_{\varepsilon\text{-typ.}} p(x_1,\dots,x_n)}} \xrightarrow{n\to\infty} 1$$

and $|T(n,\varepsilon)| \leq 2^{n(H(p)+\varepsilon)}$ for n large enough.

Protocol: A prepares $|\hat{\vartheta}_n\rangle$ locally & teleports Bob's part to Bob. $\Rightarrow$ uses $m = \log |T(n,\varepsilon)| = n(H(p)+\varepsilon)$ ebits.

$\Rightarrow \frac{m}{n} \to H(p)+\varepsilon$ "entanglement distillation rate".

Can be realized for any $\varepsilon > 0 \Rightarrow$ asymptotic rate $H(p)$.

Converse: Distill ebits from $|X\rangle^{\otimes n}$:

- Use $|\hat{\psi}_n\rangle$ instead since fidelity $\to 1$.
- $|\psi_n\rangle$: max. Schmidt coef. $2^{-n(H(p)-\varepsilon)}$

$\Rightarrow$ $|\hat{\psi}_n\rangle$: max. Schmidt coeff. $\frac{1}{1-\delta} 2^{-n(H(p)-\varepsilon)}$

Choose m s.th. $\frac{2^{-n(H(p)-\varepsilon)}}{1-\delta} \leq 2^{-m}$

$\Rightarrow$ $(2^{-m}, 2^{-m}, \dots) \succ$ (Schmidt coeffs. of $|\hat{\psi}_n\rangle$)

$\Rightarrow$ can convert $|\hat{\psi}_n\rangle$ to m ebits by LOCC.

Protocol: (1) A projects onto ε-typ. subspace $\to |\hat{\psi}_n\rangle$

(i.e: POVM $\{M_0 = \Pi_{\varepsilon\text{-typ}};\ M_1 = 1 - M_0\}$)

↓ success prob. $1-\delta \to 1$

(2) A & B convert $|\hat{\psi}_n\rangle$ to m ebits.

$\to$ works for any $m \leq n(H(p)-\varepsilon) - \log(1-\delta)$

$\to$ Rate $\frac{m}{n} \to H(p) - \varepsilon$ $\forall \varepsilon$

$\Rightarrow$ asymptotic "entanglement distillation rate" $H(p)$.

Asymptotically:

Distillation rate = Dilution rate = $H(\rho)$.

Optimal? — Yes. Otherwise we could use protocol to increase # of Bell pairs by going in circles.

Remark: Instead of $H(\rho)$, we typ. use the von Neumann entropy $S(\rho) = -\mathrm{tr}(\rho \log \rho)$, i.e.,

$$H(\rho) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|) = S(\mathrm{tr}_A |\psi\rangle\langle\psi|).$$

Protocol allows us to convert between any two states $|\psi\rangle^{\otimes n}$ and $|\phi\rangle^{\otimes n}$, provided $nS(\mathrm{tr}_B|\psi\rangle\langle\psi|) = nS(\mathrm{tr}_B|\phi\rangle\langle\phi|)$. (by going via max. ent. states).

Result: The entropy of entanglement

$$E(|\psi\rangle) = S(\mathrm{tr}_A |\psi\rangle\langle\psi|) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|)$$

uniquely quantifies the amount of entanglement in a pure bipartite state.

III.5 Mixed state entanglement

a) Introduction

When is a mixed state entangled?

i) If ρ_{AB} cannot be created by LOCC!

ii) If we can extract ebits from it.

iii) If it helps us do other tasks (w/ LOCC).

Use i)

States which can be prepared by LOCC:

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B \quad \text{"separable state"} \qquad (*)$$

$$(\rho_i^A, \rho_i^B \geq 0, p_i \geq 0)$$

ρ entangled $:\Leftrightarrow$ ρ not separable (= cannot be written as $(*)$)

Given ρ, how can we test if it is entangled?

Problem: Given ρ, unclear how to find sep. decomposition

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B$$

($\rightarrow$ ambiguity of ensemble interpret.: need to optimize over infinitely many!)

6) Entanglement witnesses

Structure of sep. states:

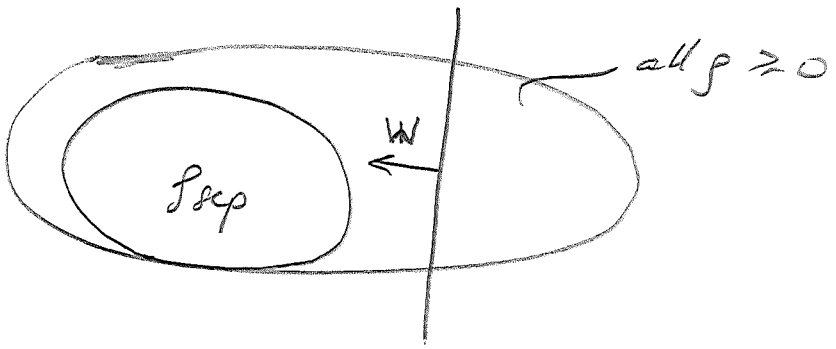
Let $\rho = \sum p_i \rho_i^A \otimes \rho_i^B$; $\sigma = \sum q_j \sigma_j^A \otimes \sigma_j^B$

$$\Rightarrow \lambda\rho + (1-\lambda)\sigma = \sum r_k \chi_k^A \otimes \chi_k^B \quad \lambda \in [0;1]$$

with $r_k = (\lambda p_1, \lambda p_2, \ldots, (1-\lambda) q_1, \ldots)$;

$$\chi_k^{A/B} = (\rho_1^{A/B}, \rho_2^{A/B}, \ldots, \sigma_1^{A/B}, \ldots)$$

$\Rightarrow \lambda\rho + (1-\lambda)\sigma$ separable: sep. states form <u>convex set</u>



Can find hyperplanes s.th. all ρ on one side are entangled.

Characterize plane + direction by (normal) vector $W = W^+$:

$$\rho \text{ sep} \Rightarrow \mathrm{tr}(W\rho) \geq 0$$

<u>i.e.:</u> $\mathrm{tr}(W\rho) < 0 \Rightarrow$ <u>ρ entangled!</u>

<u>W: "entanglement witness"</u>

Notes:

- Need to make sure $\mathrm{tr}(W\rho_{\text{sep}}) \geq 0$!
- Witness only detects <u>certain</u> ent. states!
- Convex set ≡ all tangent planes:

  ⇒ ∃ witness for <u>any</u> ent. state.
- Witness <u>linear operator</u> ⇒ experimentally measurable (in part. if W is simple)

<u>Example:</u>

$$W = \mathbb{F} \;(\text{"flip"}); \quad \mathbb{F} = \sum_{i,j=1}^{d} |i\rangle\langle j| \otimes |j\rangle\langle i|$$

$$\rho_{\text{sep}} = \sum_i p_i \rho_i^A \otimes \rho_i^B.$$

$$\mathrm{tr}\left(W\rho_{\text{sep}}\right) = \sum_i p_i \,\mathrm{tr}\left(\mathbb{F}\cdot \rho_i^A \otimes \rho_i^B\right) \overset{(1)}{=}$$

$$= \sum_i p_i \underbrace{\mathrm{tr}\left(\rho_i^A \rho_i^B\right)}_{\overset{(2)}{\geq} 0} \geq 0$$

Use:
(1) $\mathrm{tr}[\mathbb{F}\cdot(A\otimes B)] = \mathrm{tr}AB$
(2) $P, Q \geq 0 \Rightarrow \mathrm{tr}(PQ) \geq 0$

Which states does it detect? → Those w/ prevalent anti-sym. component!

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \Rightarrow \mathbb{F}|\psi^-\rangle = -|\psi^-\rangle \Rightarrow \langle\psi^-|\mathbb{F}|\psi^-\rangle = -1.$$

Mixed states:

$$\rho = \lambda |\psi^-\rangle\langle\psi^-| + (1-\lambda)\frac{\mathbb{1}}{4} \quad ; \lambda \in \left[-\tfrac{1}{3}, 1\right] : \quad (\text{"Werner state"})$$

$$\mathrm{tr}[F\rho] = \lambda \underbrace{\langle\psi^-|F|\psi^-\rangle}_{-1} + (1-\lambda)\underbrace{\mathrm{tr}\left[\frac{\mathbb{1}}{4}F\right]}_{\frac{1}{2}}$$

$$= \frac{1}{2} - \frac{3}{2}\lambda$$

$\Rightarrow$ State ent. if $\lambda \geq \frac{1}{3}$.

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

$F|\phi^+\rangle = |\phi^+\rangle \Rightarrow \langle\phi^+|F|\phi^+\rangle = 1 \Leftrightarrow$ not detected!

Optimal? Yes. E.g. $\rho = |0\rangle\langle 0| \otimes |1\rangle\langle 1| : \mathrm{tr}(F\rho) = 0$.

Other witnesses: E.g. $W = \mathbb{1} - d\cdot|\Omega\rangle\langle\Omega|$; $|\Omega\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i,i\rangle$

$\Rightarrow$ Homework

c) Positive maps and the PPT criterion

Reminder: $\Lambda : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ positive $: \Leftrightarrow (\rho \geq 0 \Rightarrow \Lambda(\rho) \geq 0)$

Usually: require Λ completely positive (CP)

Here: Will be interested in Λ positive but not CP.

Consider $\rho_{sep} = \sum_i p_i \rho_i^A \otimes \rho_i^B$:

$$(\Lambda \otimes I)(\rho_{sep}) = \sum_i p_i \underbrace{\Lambda(\rho_i^A)}_{= \tilde{\rho}_i^A \geq 0} \otimes \rho_i^B = \tilde{\rho}_{sep} \geq 0$$

i.e.: $(\Lambda \otimes I)(\rho) \not\geq 0 \Rightarrow \rho$ entangled!

↑ has neg. eigenvalues

Most important example:

$$\Lambda(\rho) = \rho^T$$

$(\Lambda \otimes I) =: \rho^{T_A}$: "partial transpose"

(i.e.: $\rho = \sum \rho_{ij}^{i'j'} |i,j\rangle\langle i',j'| \Rightarrow \rho^{T_A} = \sum \rho_{ij}^{i'j'} |i',j\rangle\langle i,j'|$)

i.e.:

$\rho^{T_A} \not\geq 0 \Rightarrow \rho$ entangled

positive partial transpose (PPT) criterion

E.g.: $|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i,i\rangle$

$$\Rightarrow (|\Omega\rangle\langle\Omega|)^{T_A} = \frac{1}{d} \sum (|i,j\rangle\langle j,i|)^{T_A} = \frac{1}{d} \sum |j,i\rangle\langle i,j|.$$

Not positive: e.g. $|v\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$:

$$\langle v| \left[(|\Omega\rangle\langle\Omega|)^{T_A} |v\rangle \right] = \frac{1}{2}(\langle 01| - \langle 10|)(|10\rangle - |01\rangle) = -1$$

Again: Also works for $\rho = \lambda |\Omega\rangle\langle\Omega| + (1-\lambda)\frac{\mathbb{1}}{d^2}$ ("isotropic state")

E.g. $d=2$:

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

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

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

$\rightarrow$ positive iff $\frac{\lambda}{2} \leq \frac{1-\lambda}{4} \iff \underline{\lambda \leq \frac{1}{3}}$

Notes: Indep. of unitary on $B \Rightarrow$ detects all PE states!

(i.e.: Stronger than witness!)

In fact: PPT criterion detects all entangled states

in dimension $d_A \times d_B = 2\times 2$ and 3×2 (but not 3×3 or 4×2)

$\Rightarrow$ "PPT bound ent. states"

Other example:

$$\Lambda(\rho) = \mathrm{tr}(\rho) I - \rho :$$

$$(\Lambda \otimes I)(\rho) = \underbrace{\mathrm{tr}\,\rho}_{=1} \cdot (I \otimes \mathrm{tr}_A \rho) - \rho = I \otimes \rho_B - \rho \neq 0 \Rightarrow \text{entangled}$$

"reduction criterion" $I \otimes \mathrm{tr}_A \rho \neq \rho$ ⇒ Homework.

d) Relation of witnesses & positive maps:

For each witness W, there is a pos. map Λ which detects at least as good as W (in fact, better):

Witness = bipartite "state" (rather: operator) W

map $\tilde{=}$ Jamiołkowski map of W_1^T

$$\Lambda(X) = \mathrm{tr}_A\left(W^T (X_A^T \otimes I_B)\right) = \mathrm{tr}_A\left(W (X_A \otimes I_B)\right)^T$$

Then: $\mathrm{tr}(W(A \otimes B)) = \mathrm{tr}_B\left(\underbrace{\mathrm{tr}_A(W(A \otimes I))}_{= \Lambda(A)^T} \cdot B\right) = \mathrm{tr}(\Lambda(A)^T B)$

$$= \sum_{ij} \left[\Lambda(A)^T\right]_{ij} B_{ji} = d \langle \Omega | \Lambda(A) \otimes B | \Omega \rangle$$

$$= (\Lambda \otimes I)(A \otimes B)$$

linearity $\Rightarrow \mathrm{tr}(W\rho) = d \langle \Omega | (\Lambda \otimes I)(\rho) | \Omega \rangle$.

i.e.: $\mathrm{tr}(W\rho) < 0 \Rightarrow (\Lambda \otimes I)(\rho) \neq 0$.

$\Rightarrow \Lambda$ stronger than W!

e.g. $W = \mathbb{F}$:

$$\Lambda(X) = tr_B\left(\mathbb{F}(I_A \otimes X_B)\right)^T = tr\left(I_A \cdot X_B\right)^T = X_B^T.$$

$\Rightarrow$ PPT criterion!

Note: PPT strictly stronger: $\mathbb{F}$ could not detect e.g. $|\Psi\rangle$!

Corollary: A state is entangled if & only if

$(\Lambda \otimes I)(\rho) \geq 0$ $\forall$ positive Λ (as sep. states $\Leftrightarrow$ all witness)

e) Quantification of mixed state entanglement

How to quantify entanglement?

i) Entanglement needed to create state

"Entanglement of formation" E_F (single copy)

"Entanglement cost" E_C (many copies)

ii) Extractable entanglement:

"Distillable entanglement" E_D:

LOCC protocol $\mathcal{E}_n$: $\| \mathcal{E}_n(\rho^{\otimes n}) - |\Omega\rangle\langle\Omega|^{\otimes n} \| \to 0.$

Note: Generally $E_C \neq E_D$: no unique measure!

Problem: E_F very hard, E_c / E_D (almost) impossible to compute $\Rightarrow$ need other measures.

(But: Cases w/ $E_D = 0$ known, e.g. PPT states. Currently big open problem.)

Have seen: ρ^{T_A} has neg. eigenvalues $\Rightarrow \rho$ entangled.

Use as ent. measure:

$$\underline{\text{Negativity}} \quad N(\rho) = \frac{1}{2}\Big(\underbrace{\sum_i |\lambda_i(\rho^{T_A})|}_{=: \|\rho^{T_A}\|_1} - 1\Big)$$

$$= \frac{1}{2}\left(\|\rho^{T_A}\| - 1\right) = \sum_{\substack{\text{neg.} \\ \text{eigenvals}}} \left(-\lambda_i(\rho^{T_A})\right).$$

or $\underline{\text{log-negativity}} \quad E_N(\rho) = \log_2 \|\rho^{T_A}\|_1$

What are desired properties for ent. measure E?

- $E_D \le E \le E_c$.
- 0 on sep. states, $\neq 0$ on ent. states.
- additive: $E(\rho_{AB} \otimes \sigma_{A'B'}) = E(\rho_{AB}) + E(\sigma_{A'B'})$
- LOCC-monotone: cannot be increased by LOCC.
- Coincides with $E(|\psi\rangle) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|)$ for pure states.

Negativity / Log-negativity:

$\mathcal{N}$: • LOCC-monotone

- 0 on sep. states, but can be $\neq 0$ on ent. states.
- $= E(|\psi\rangle)$ for pure
- not additive

E_N : • additive

- 0 on sep., but can be $\neq 0$ on ent. states
- $= E(|\psi\rangle)$ for pure
- not an LOCC monotone.