III. Entanglement

1. Introduction

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

If \( |\psi\rangle = |\phi^A\rangle \otimes |\phi^B\rangle \)

\[ \mathcal{H}_A \otimes \mathcal{H}_B \]

A \& B can describe all their measurements etc.

or \( |\psi\rangle \) independently \( \rightarrow \) no correlations.

We call such a state a **product state**.

**Product States** have Schmidt coefficients \((1, 0, \ldots)\),

and \( p_A = \text{tr}_B (|\psi\rangle \langle \psi|_A) = |\phi^A\rangle \langle \phi^A| \)

\( p_B = \text{tr}_A (|\psi\rangle \langle \psi|_B) = |\phi^B\rangle \langle \phi^B| \)

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

\[ \iff \text{tr} p_A^2 = \text{tr} p_B^2 = 1 \]

(Note: For general \( f = \sum p_i |\psi_i\rangle \langle \psi_i| \), \( \sum p_i = 1 \), we have

\[ \text{tr} f^2 = \sum p_i^2 \leq 1 \]  "purity"

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

Consider e.g. \( |4^{-}\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \).

- Measurement outcomes of A & B are anti-correlated → no independent description possible.
  - \( f_A = f_B = \frac{1}{2} \) for all cases, outcomes equally likely.
  - \( \text{Tr} f_A^2 + \text{Tr} f_B^2 < 1 \) for all entangled states.

→ ent. states have more than one Schrödinger coeff. ≠ 0.

**Encoding of information:**

\[
\text{dim} \left( C^2 \otimes C^2 \right) = 2^2 = 4 \text{ bits}.
\]

**Product states:**

\[
|4_{ij}\rangle = |i\rangle \langle j| : \text{orthonormal set}.
\]

→ encoding in product states.

→ A & B can read out information individually.
Entangled states:
\[
\begin{align*}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}} (|10\rangle + |10\rangle) \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}} (|10\rangle - |10\rangle)
\end{align*}
\]

ONB

"Bell states", "Bell basis"

→ encodes 2 bits of info

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

As meas. fully random → no info

→ total info at most 1 bit!

AB meas. both in Z basis:

→ cases: equal (\$\Phi^+$) or different (\$\Psi^+$)

Similar w/ X-basis: + or -, etc.

→ 2 bits of info, but only 1 bit can be recovered

locally → info hidden in (un-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: 0 1 0 1
2 0
C distributes coins

0 0 1 1
0 0 1 1
B
```
A and B each are 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 \(a_i = +1\) and \(b_j = +1\) \((i, j = 0, 1, 2)\).

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 can 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.

\[
\Rightarrow P(a_0 = b_1) + P(b_1 = b_2) + P(a_2 = b_0) \geq 1.
\]
What happens in a quantum version of this experiment?

AB share an entangled state, and perform proj.
measurement along three different axes with outcomes
$\pm 1 \rightarrow$ meas operators $\sigma_i$ and $\sigma_j$.

AB share $|\psi^-\rangle = \frac{1}{\sqrt{2}} (|10\rangle - |11\rangle)$.

We have $(\sigma^A_i + \sigma^B_i) |\psi^-\rangle = 0 \quad \forall i, \quad \sigma = (\sigma_x, \sigma_y, \sigma_z)$

Then,

$$<\psi^- | (\sigma^A_i \cdot \vec{n}) (\sigma^B_i \cdot \vec{n}) | \psi^- > = -\frac{\vec{n} \cdot \vec{n}}{2}$$

$$= -\sum_j w_i w_j \angle (\sigma^A \sigma^A_i \sigma^B \sigma^B_j) = -\sum_j w_i w_j = -\vec{n} \cdot \vec{n} = -\cos \theta$$

angle tilted.

$\vec{n} \bot \vec{n}$.
Measurement of $A/B$ along $\vec{u}/\vec{u}$:

$\rightarrow$ projections $E_{\pm}(\vec{u}) = \frac{1}{2} (\mathbb{I} \pm \vec{u} \cdot \vec{σ})$

$p(\pm, \pm) = \langle \Psi^- | E_{\pm}(\vec{u}) E_{\pm}(\vec{u}) | \Psi^- \rangle$

\[
\frac{1}{4} \langle \Psi^- | \left( \mathbb{I} \pm \vec{u} \cdot \vec{σ}_A \pm \vec{u} \cdot \vec{σ}_B + (\vec{u} \cdot \vec{σ}_A)(\vec{u} \cdot \vec{σ}_B) \right) | \Psi^- \rangle
\]

$\rightarrow 1 \rightarrow 0 \rightarrow 0 \rightarrow -\cos \Theta$

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

$p(\pm, \mp) = \frac{1}{4} (1 + \cos \Theta)$

$\Rightarrow \text{Pequal} = \frac{1}{2} (1 - \cos \Theta); \quad \text{Pdifferent} = \frac{1}{2} (1 + \cos \Theta)$

Now let $A$ measure along

$\vec{u}_1$, $\vec{u}_2$, $\vec{u}_3$

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

$A + B$ measure in same basis:

$\text{Pequal} = \frac{1}{2} (1 - \cos 180^\circ) = 1$
A+B scenario is defined as:

\[ P_{equal} = \frac{1}{2} \left( 1 - \cos \theta \right) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \]

\[ \theta = \pm 60^\circ \]

\[ \Rightarrow \cos \theta = \pm \frac{1}{2} \]

\[ \Rightarrow P(a_1 = b_2) + P(a_2 = b_3) + P(b_3 = a_1) = \frac{3}{4} < 1 \]

\[ \Rightarrow \text{Quantum mechanical predictions incompatible with a local realistic description!} \]

\[ \Rightarrow \text{We cannot assign values to observables we have not measured ("relin").} \]

Fon Bell inequalities:

Formal setup:

[Diagram with arrows and variables indicating measurement directions and observables]

\( x,y \): measurement direction (input)

\( a,b \): values of observables (output)
Which output distributions \( P(\theta, b \mid x, y) \) 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 before hand (no faster-than-light):

\[
P(\theta, b \mid x, y) = \sum_{\lambda} p_\lambda P_\lambda^A(a(x)) P_\lambda^B(b(y))
\]

\[
\text{hidden variable} \quad \text{can be deterministic}
\]

pro. \quad \text{over } \lambda

Consider now \( x = 0, 1 \) and \( y = 0, 1 \),

with outcomes (measurements) \( a_0, a_1, b_0, b_1, = \pm 1 \).

Since \( a_i = \pm 1 \), \( b_i = \pm 1 \):

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

\[
\Rightarrow \quad |\langle C \rangle| \leq \langle |C| \rangle = 2
\]
**CHSH equality (Clauser, Horne, Shimony, Holt):**

\[ |\langle a_0 b_0 \rangle + \langle a_1 b_0 \rangle + \langle a_0 b_1 \rangle - \langle a_1 b_1 \rangle| \leq 2 \]

---

**Quantum mechanics:**

\[ a_i = \sigma^c_i \cdot u_i \]

\[ b_i = \sigma^r_i \cdot u_i \]

\[ \langle a_i b_j \rangle = -\cos \Theta \]

\[ \langle a_0 b_0 \rangle = \langle a_1 b_0 \rangle = \langle a_0 b_1 \rangle = \cos 45^\circ = \frac{1}{\sqrt{2}} \]

\[ \langle a_1 b_1 \rangle = \cos 135^\circ = -\frac{1}{\sqrt{2}} \]

\[ \implies |\langle a_0 b_0 \rangle + \langle a_1 b_0 \rangle + \langle b_0 a_1 \rangle - \langle a_1 b_1 \rangle| = 2\sqrt{2} > 2. \]

---

- Incompatible w/ LHV models.

- Note: Unlike original Bell inequality, does not require knowledge of eq. correlations in space-time.
I. Protocols

Noiseless qubit channel
Noiseless classical bit channel
Noiseless entanglement

\[ \text{Nonlocal} \rightarrow \text{unit resource} \]

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 (e.g., ebits)

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

\[ |i\rangle_A \rightarrow |i\rangle_B \quad (\text{i.e. } |\psi_i\rangle_A \rightarrow |\psi_i\rangle_B) \]

where \( |0\rangle, |1\rangle \) is some orthonormal basis

do not have to be the same

\[ |0\rangle_A, |1\rangle_A \] is some orthonormal basis

on Alice's system

\[ |0\rangle_B, |1\rangle_B \] is some orthonormal basis

on Bob's system

The above map is linear and preserves superposition states

\[ \alpha |0\rangle_A + \beta |1\rangle_A \rightarrow \alpha |0\rangle_B + \beta |1\rangle_B \]
Noiseless qubit channel can be written as:

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

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

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

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

$$i \times i \rightarrow i \times i,$$

$$i \times i \rightarrow 0 \text{ for } i \neq j,$$

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

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

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

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

$$[c \rightarrow c]$$ — 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:

$$[q \rightarrow q] \geq [c \rightarrow c].$$
- 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 possesses the first qubit and Bob possesses the second. The resource is denoted as $[qq]$. 

\section{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 the use of a noiseless qubit channel. Alice & Bob share the ebit $|\Phi^+\rangle_{AB}$.

   The resource inequality of this protocol is
   \[
   [q \rightarrow q] \geq [qq]
   \]
Notes: notice the difference between
Bell state — local state is Alice’s lab
and ebit — a nonlocal resource shared
between Alice and Bob.

II.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 classical bits (corresponding to 4 mess.)
   if she uses a noiseless qch. and shares an ebit with Bob.
   The super-dense coding protocol implements the following
   resource inequality:

\[ I_{99} + I_{9\rightarrow 9} \geq 2 I_{c\rightarrow c} \]
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:

$|\psi\rangle_{A'} |\Phi^+\rangle_{AB} = (\alpha |0\rangle_{A'} + \beta |1\rangle_{A'}) \left( \frac{100\rangle_{AB} + 111\rangle_{AB}}{\sqrt{2}} \right)$

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

Use Bell states on system $A'A$:

$100\rangle_{A' A'} = \frac{1}{\sqrt{2}} \left( |\Phi^+\rangle_{A' A'} + |\Phi^-\rangle_{A' A'} \right)$

$110\rangle_{A' A'} = \frac{1}{\sqrt{2}} \left( |\psi^+\rangle_{A' A'} - |\psi^-\rangle_{A' A'} \right)$

$101\rangle = ...$

$111\rangle = ...$

$= \frac{1}{2} \left[ \alpha (|\Phi^+\rangle_{A' A'} + |\Phi^-\rangle_{A' A'}) 10\rangle_{A'B} + \beta (|\psi^+\rangle_{A' A'} - |\psi^-\rangle_{A' A'}) 10\rangle_{A'B} \\
+ \alpha (|\psi^+\rangle_{A' A'} + |\psi^-\rangle_{A' A'}) 11\rangle_{A'B} + \beta (|\Phi^+\rangle_{A' A'} + |\Phi^-\rangle_{A' A'}) 11\rangle_{A'B} \right]$
\[
\frac{1}{2} \left[ \phi^+_{A'A} (\alpha \psi_0 + \beta \psi_1)_B + \phi^-_{A'A} (\alpha \psi_0 - \beta \psi_1)_B \\
+ \psi^+_{A'A} (\alpha \psi_0 + \beta \psi_1)_B + \psi^-_{A'A} (\alpha \psi_0 - \beta \psi_1)_B \right]
\]

using Pauli matrices \(X, Z\) and their action on \(\psi_\pm\):

\[
X \psi_\pm = \alpha \psi_\pm + \beta \psi_\mp
\]

\[
Z \psi_\pm = \alpha \psi_\pm - \beta \psi_\mp
\]

\[
= \frac{1}{2} \left[ \phi^+_{A'A} \psi_B + \phi^-_{A'A} Z \psi_B + \psi^+_{A'A} X \psi_B + \psi^-_{A'A} XZ \psi_B \right].
\]

Quantum teleportation protocol:

1. Alice possesses a qubit \(\psi_{A'}\), 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:

\[
\phi^+_{A'A} \psi_B
\]

\[
\phi^-_{A'A} Z \psi_B
\]

\[
\psi^+_{A'A} X \psi_B
\]

\[
\psi^-_{A'A} XZ \psi_B
\]

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 basis.

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

The resource inequality for q. teleportation is as follows:
\[ I_{q} + 2I_{C \rightarrow C} \geq I_{q \rightarrow q} \]

II Implementation of Choi-Jamiołkowski isomorphism via teleportation

If \( T \) is a quantum channel then its Jam. state \( \tau \) can operationally be obtained by letting \( T \) act on a maximally entangled state.

Converse? Given \( \tau \), how to implement \( T \) as an action on any state \( \rho \)?

1. Alice & Bob share state \( \tau = (T_A \otimes I_B) \rho_{12} \otimes \rho_{21} \), where \( \rho_{12} = \sum_{i}^{\frac{1}{\sqrt{d}}} |i\rangle_i |i\rangle_{A} \).

2. Bob also has a state \( \rho \) (on system \( B' \)). He performs a measurement on his system \( BB' \) using a POVM which contains state \( \omega = \rho_{12} \otimes \rho_{21} \).

3. Alice's state after the measurement is \( T(\rho) \) if Bob has obtained a meas. outcome corres. to \( \omega \).
Denote Alice's state by $\nu_A$ after a successful Bob's measurement, which occurs with prob. $p$.

$$\nu_A = \frac{1}{p} \text{Tr}_{BB'} \left( (A \otimes \rho_{BB'} ) (\tau_{AB} \otimes \rho_{B} ) (I \otimes \omega_{BB'}) \right)$$

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

$$p \text{ Tr} (A \nu_A) = \text{Tr} \left( (A \otimes I_{B'}) \left( (I \otimes \omega_{BB'} ) (\tau_{AB} \otimes \rho_{B}) (I \otimes \omega_{BB'}) \right) \right)$$

$$= \text{Tr} \left( (\tau_{AB} \otimes \rho_{B}) (A \otimes \omega_{BB'}) \otimes \text{I} \right)$$

Rewind that $\omega = \frac{1}{d} \sum_{ij} \lambda_{ij} |i\rangle_B \otimes |j\rangle_B$. Denote the coeff. $\rho = \sum_{kl} \lambda_{kl} |k\rangle_B \otimes |l\rangle_B$ in the above basis.

$$\otimes \text{Tr} \left( (\tau_{AB} \otimes \sum_{kl} \lambda_{kl} |k\rangle_B \otimes |l\rangle_B) \right)$$

$$= \frac{1}{d} \sum_{kl} \text{Tr} \left( \tau (A \otimes \sum_{ij} |i\rangle_B \otimes |j\rangle_B) \otimes \lambda_{kl} |k\rangle_B \otimes |l\rangle_B \right)$$

$$= \frac{1}{d} \sum_{ij} \text{Tr} \left( \sum_{kl} \tau_{kl} |i\rangle_B \otimes |j\rangle_B \otimes \lambda_{kl} |k\rangle_B \otimes |l\rangle_B \right)$$

$$= \frac{1}{d} \text{Tr} \left( \tau \left( A \otimes \sum_{ij} |i\rangle_B \otimes |j\rangle_B \right) \right) = \text{Tr} (\tau A \otimes \rho^T) \frac{1}{d}$$

$$= \frac{1}{d^2} \text{Tr} (AT(\rho))$$

Therefore $\nu_A = T(\rho)$ and $p = \frac{1}{d^2}$.
Wrap-up previous lecture:

III. Applications of entanglement

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

a) Dense coding

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

\[ 1 \text{qubit} + 1 \text{ent. pair} \rightarrow 2 \text{bits} \]

\[ |\Phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]

A uses \( U \in \{I, 5_x, 5_y, 5_z\} \) to convert \( |\Phi^+\rangle \) to the Bell state

& sends her qubit to B.

\( \rightarrow \) B measures in Bell basis & receives information.

b) Teleportation:

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

\[ 1 \text{qubit} + 2 \text{bits} \rightarrow 1 \text{qubit} \]

\[ |\Phi^+\rangle \xrightarrow{\text{meas. in Bell basis}} U |x\rangle \]

\( U = \{I, 5_x, 5_y, 5_z\} \)

dep. on Bob's outcome

A sends meas. result \( \rightarrow \) Bob can undo \( U \! \)

Note: No info contained before class. hence,

\( \rightarrow \) no faster than light (FTL) communication!
Ill. 4. Entanglement conversion & quantification

a) Introduction & Setup

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

Tolerance:
- Protocols might require dif. ent. states
- Use to quantify ent. : how many $\epsilon / 2$ \( \leq \frac{1}{2} \) are "entangled" in a state?

Know already: Same Schmidt coeffs $\leftrightarrow$ related by local unitary $\leftrightarrow$ same entanglement.
Example:

\[ |x> = \frac{2}{3} |00> + \frac{1}{2} |11> \quad |\psi^+> = \frac{1}{2} |00> + \frac{1}{2} |11> \]

Can we covert \[ |\psi> \rightarrow |x> \]? 

A does POVM \[ \Pi_0, \Pi_1 \] \[ \Pi_0 = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & 1/3 \end{pmatrix} \quad \Pi_1 = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/3 \end{pmatrix} \].

\[ |\tilde{\psi}_0> = \frac{1}{12} \left( \frac{2}{3} |00> + \frac{1}{2} |11> \right) \quad |\tilde{\psi}_1> = \frac{1}{12} \left( \frac{1}{3} |00> + \frac{1}{3} |11> \right). \]

\[ p = \frac{1}{2} \quad |\tilde{\psi}_0> = \frac{2}{3} |00> + \frac{1}{2} |11> = |x> \Rightarrow \text{OK} \]

\[ p = \frac{1}{2} \quad |\tilde{\psi}_1> = \frac{1}{3} |00> + \frac{2}{3} |11> : \text{same Schmidt coeff.} \]

but \[ \Pi_1 \] is need to apply \[ \sigma_x \otimes \sigma_x \].

Protocol: \[ A \] does POVM, sends result to \[ B \] who applies a unitary depending on its outcome.

Success prob. \[ p = \frac{1}{4}. \]

Best possible: We cannot yet make copies since POVMs cannot increase Schmidt rank.

What about the converse: \[ |x> \rightarrow |\psi^+> \] ?

A does POVM \[ \Pi_0, \Pi_1 \] \[ \Pi_0 = \begin{pmatrix} \sqrt{2}/3 & 1 \\ 1 & \sqrt{2}/3 \end{pmatrix} \quad \Pi_1 = \begin{pmatrix} \sqrt{2}/3 & 0 \\ 0 & \sqrt{2}/3 \end{pmatrix} \].

\[ |\tilde{\psi}_0> = \frac{1}{3} |00> + \frac{1}{3} |11> \quad |\tilde{\psi}_1> = \frac{1}{3} |00> \]
\[ P_0 = \frac{2}{3} : |4\rangle \rightarrow |x\rangle \]

\[ P_0 = \frac{1}{3} : |4\rangle = |00\rangle \rightarrow \text{no entanglement.} \]

\[ |x\rangle \rightarrow |\phi^+\rangle \text{ w/ prob. } p = \frac{2}{3} \]

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

Is this the best A & B can do?

What is the optimal protocol?

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

Alice PVM, sends result to B, B does PVM, sends result to A...
But: For pure states, Alice can replace her's by a 1-round protocol via one-way commuting:

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

General protocol:

\[ |\psi_k\rangle \rightarrow (\hat{\psi}_k = \Pi_k = |\psi_k\rangle \langle \psi_k|) \]

\[ (i.e., |\psi_k\rangle = \frac{\hat{\psi}_k}{\|\hat{\psi}_k\|} \text{ w/ prob. } p = \langle \psi_k | \hat{\psi}_k \rangle) \]

\[ |\psi_k\rangle \& |\psi\rangle \text{ fully char. by Schmidt coeff.} \]

\[ \rightarrow \text{sufficient to study possible corrs} \]

\[ \text{Stat} \rightarrow \{ P_k, \hat{P}_k, \Sigma \} \]

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

When E PVM \( \Pi_k \), s.t. \( \hat{P}_k = P_k = \sum_k \Pi_k = \sum_k P_k \).

Note: will use \( \hat{P}_k \)-notation w/ \| \hat{P}_k \| \]

Further def. in the following! (cf. \( \phi^+ \rightarrow |X\rangle \))
6) Proposition

For \( \lambda \in \mathbb{R}^d \geq 0 \), let \( \lambda^\downarrow = (\lambda^\downarrow_1, \ldots, \lambda^\downarrow_d) \); \( \lambda^\downarrow_1 \geq \lambda^\downarrow_2 \geq \ldots \geq 0 \) denote the ordered version of \( \lambda \).

(Note: Not all the following holds also \( \downarrow \) only.)

Definition (Proposition 15):

We say that \( \lambda \) is majorized by \( \mu \) (or \( \mu \) majorizes \( \lambda \)),

\[ \lambda \prec \mu, \]

if there exist permutations \( P_i \) & prob. \( q_i \) s.t.,

\[ \lambda = \sum q_i P_i \mu \]

(i.e., \( \lambda \) can be obtained from \( \mu \) by random perm. it is "more random")

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

Theorem: Definition 1 is equivalent to the following two Defs:

(\( \rightarrow \) cf. Homework!)

Definition (II): \( \lambda \prec \mu \iff \exists \text{ doubly stochastic } \Omega \)

(i.e.: \( \Omega_{ij} \geq 0 \), \( \sum \Omega_{ij} = \sum \Omega_{ji} = 1 \); random process w. fixed pi.

\( \frac{1}{\pi_1}, \ldots, \frac{1}{\pi_d} \))

s.t., \( \lambda = \Omega \mu \).

(Proof via Birkhoff's Thm: Every d.s. \( \Omega \) is of the form \( \Omega = \Sigma \pi_i P_i \) )
Definition (141):

\[ \lambda < \mu : \iff \sum_{i=1}^{k} \lambda_i^k \leq \sum_{i=1}^{k} \mu_i^k \text{ for } k = 1, \ldots, d, \text{ with equality for } k = d. \]

Remarks:

- \( \lambda \prec \mu \) defines partial order on prob dists.
- \( \lambda \not\prec \mu \) : \( \lambda \) more disordered than \( \mu \) (i.e., path; entropy larger!)

We can also define \( \lambda \prec \mu \) for positive (or hermitian) operators:

\[ A < B : \iff \lambda^v_k(A) < \lambda^v_k(B), \text{ with } \lambda^v_k(\cdot) \text{ the ordered eigenvalues of } A. \]

Theorem (Key-Fact: maximum principle):

For a hermitian \( A \),

\[ \sum_{j=1}^{k} \lambda_j^v(A) = \max_P \text{tr}(AP), \]

with max over all rank \( k \) projectors of rank \( k \).

Proof: let \( A = \sum_{j=1}^{d} \lambda_j^v(a_j X_{a_j}) \), with the choice \( P = \sum_{i=1}^{l} \langle a_i X_{a_i} \rangle \),

\[ \text{tr}(AP) = \sum_{j=1}^{k} \lambda_j^v(A). \]
For a general \( P \), we have \( P = \sum_{j=1}^{k} |p_j| |\phi_j\rangle \), with an orthonormal basis \( \{ |\phi_j\rangle \}_{j=1}^{k} \). Then:

\[
\langle \pi | A | \pi \rangle = \sum_{j=1}^{k} \frac{|\langle \pi | \phi_j \rangle|^2}{|\phi_j\rangle} = u_j
\]

\( u_j \) unitary \( \Rightarrow \sum_{j=1}^{k} |u_j|^2 = \sum_{j=1}^{k} |u_{ij}|^2 = 1 \Rightarrow u_j \) orthonormal.

\[=(\langle \rho | A | \rho \rangle)_{ij} < \lambda_i^k(A)\]

\[= \text{tr}(AP) = \sum_{j=1}^{k} \langle \rho | A | \rho_j \rangle = \sum_{j=1}^{k} \lambda_i^k(A)\]

Corollary: \( \lambda_i^k(A+B) < \lambda_i^k(A) + \lambda_i^k(B) \)

Proof: \[\sum_{i=1}^{k} \lambda_i^k(A+B) = \max_{P: \|P\|=1} \lambda_i^k(P(A+B)) \leq \max_{P} \lambda_i^k(PA) + \max_{P} \lambda_i^k(PB) = \sum_{i=1}^{k} \lambda_i^k(A) + \sum_{i=1}^{k} \lambda_i^k(B)\]

1) Simple-copy entanglement conversion

Theorem: If we can convert \( |\Psi\rangle \rightarrow \{ |\phi_k, y_k\rangle \} \) by LOCC,

then \( \lambda_k^k(s) < \sum |p_{ik}| \lambda_i^k(s_k) \), with \( p_k, s_k \) as before (the EPR of \( |\Psi\rangle, (y_k) \)).
Proof: We can choose \( g = H_A \mathbf{1}_X \mathbf{1}_Y \), \( g_k = H_A \mathbf{1}_X \mathbf{1}_Y \).

A class \( \mathcal{PM} \) of POVMs. We have then

\[
\sum_{k=1}^{d} p_k \lambda^k(p_k) = \sum_k \lambda^k(\tilde{p}_k) = \sum_k \lambda^k(\{ H_A \left[ \sum_i (\tilde{p}_k \otimes I) 1_X 1_Y (\tilde{p}_k \otimes I) \right] \})
\]

Corollary

\[
\lambda^i(\{ H_A \left[ \sum_i (\tilde{p}_k \otimes I) 1_X 1_Y (\tilde{p}_k \otimes I) \right] \}) = \lambda^i(p).
\]

Conversely:

**Theorem:** Let \( \lambda^i(p) < \sum p_i \lambda^i(p_i) \). Then, there is a POVM \( \{ \tilde{p}_j \} \) s.t. \( \hat{f} \rightarrow \{ p_i, \tilde{p}_j \} \) (i.e., a LOCC protocol for \( |1\rangle \rightarrow \{ p_i, |1\rangle \} \)).

**Proof:**

\( \lambda^i(p) < \sum p_i \lambda^i(p_i) \) \( \Rightarrow \) \( \exists \tilde{p}_j \text{s.t.} \lambda^i(p) - \sum p_i \tilde{p}_j \lambda^i(p_i) \).

Wlog.: \( p, \tilde{p}_j \) all diagonal (otherwise, append zero columns).

Define \( E_{ij} \) via \( \tilde{p}_j \hat{f} = \sqrt{p_i} \tilde{p}_j \hat{p}_i \). Then,

\[
\sqrt{p} \left( \sum_{ij} E_{ij}^+ E_{ij} \right) \hat{f} = \sum_{ij} p_i \sqrt{p_j} \hat{p}_i \hat{p}_j \hat{p}_i \hat{p}_j = \hat{f}
\]

\( \Rightarrow \sum_{ij} E_{ij}^+ E_{ij} = 1 \) (if \( \hat{f} \) is invertible).

(Note: \( p \) not mv. \( \Rightarrow E_{ij} \) can be def. freely on her \( p \).)
Moreover, \( E_{ij} \cdot p \cdot E_{ij}^+ = p_i q_j p_i \)

\[ \Rightarrow \sum_j E_{ij} \cdot p \cdot E_{ij}^+ = p_i p_i \]

\( \therefore \text{LOCC protocol for } p \rightarrow (p_i, q_j p_i) \).

Note: The protocols we had previously for

\( \left( \frac{1}{2}, \frac{1}{2} \right) \leftrightarrow \left( \frac{2}{3}, \frac{1}{3} \right) \)

are indeed optimal:

\( \left( \frac{1}{2}, \frac{1}{2} \right) \not< \left( \frac{2}{3}, \frac{1}{3} \right) \) \( \checkmark \)

\( \left( \frac{2}{3}, \frac{1}{3} \right) < \frac{2}{3} \left( \frac{1}{2}, \frac{1}{2} \right) + \frac{1}{3} (1, 0) = \left( \frac{2}{3}, \frac{1}{3} \right) \)

\( \uparrow \text{max. possible value!} \)

Typ. "extractable ent.": \( \left| x \right> = \sqrt{\frac{2}{3}} \left| 0 \right> + \sqrt{\frac{1}{3}} \left| 1 \right> + \left| 2 \right> \)
Asymptotic protocols

Simple-copy conversion: not possible,
- at least two receivers to quantify ent.
  #e displaced to build state
  #extractable ebits.

Can we do this w/ more copies?

\[ |\chi^{\otimes 2} = \left( |\frac{2}{3}\rangle_1 \otimes |\frac{1}{3}\rangle_2 \right)^{\otimes 2} \leftrightarrow |\psi^+\rangle_{\otimes 2} \]

\[ |\phi^+\rangle \rightarrow |\chi^{\otimes 2} \]

\[ \left( \frac{4}{9}, \frac{2}{9}, \frac{2}{9}, \frac{1}{9} \right) \rightarrow \left( \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4} \right) \]

\[ p = 1 \] best possible as Schmidt rank cannot be increased by Povin.

\[ |\chi^{\otimes 2} \rightarrow (\phi^+\rangle_{\otimes 2} \]

\[ \left( \frac{4}{9}, \frac{2}{9}, \frac{2}{9}, \frac{1}{9} \right) \leq p \left( \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4} \right) + q \left( \frac{1}{2}, \frac{1}{2}, 0, 0 \right) + (1-p-q) (1,0,0) \]

Optimum: \( q = \frac{2}{3}, q = \frac{1}{3} \):

\[ \left( \frac{4}{9}, \frac{2}{9}, \frac{1}{9}, \frac{1}{9} \right) \]
\[ p = \frac{2}{3}; \quad 2 \text{ ebits} \]
\[ q = \frac{1}{9}; \quad 1 \text{ qbit} \]

\[ \frac{2 \cdot \frac{2}{3} + 1 \cdot \frac{1}{9}}{2} = \frac{2}{3} + \frac{1}{18} > \frac{2}{3} \]

\[ \Rightarrow \text{ Improved yield as compared to 1-copy protocol!} \]

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

**Requirements for asymptotic protocols:**

\[ \text{correct } |\phi^+\rangle \xrightarrow{\text{w}} |\chi\rangle \xrightarrow{\text{w}} \]

rate \( \frac{\mu}{w} \to R > 0 \text{ for } N, w \to \infty \)

\[ \Rightarrow \text{ success prob. } p \to 1 \text{ for } N \to \infty \]

\[ \Rightarrow \text{ Conversion need not be perfect: sufficient if distance from correct state } \delta \to 0 \text{ as } N \to \infty. \]

**How to measure error } \delta \text{?**}

Use \( \delta = 1 - F = \text{ "fidelity" } F = |\langle \psi | \phi \rangle|^2 \)

\( \delta \) bounds error on any observable \( \mathcal{O} : \)

\[ |\langle \phi | \mathcal{O} | \psi \rangle - \langle \phi | \mathcal{O} | \phi \rangle| \leq 2 \sqrt{\delta} \| \mathcal{O} \|_{\infty} \text{ (\( \to \) Homework)} \]

i.e. \( \delta \to 0 \Rightarrow \text{ states indistinguishable by any measurement!} \)
Now consider $|x\rangle = \sum \sqrt{p(x)} |x\rangle_A |x\rangle_B$, $x = 1, \ldots, d$

$|x\rangle^{\otimes n} = \sum_{x_1 \ldots x_n} \sqrt{p(x_1) \ldots p(x_n)} |x_1, \ldots, x_n\rangle \langle x_1, \ldots, x_n|$

The sequence $x_1, \ldots, x_n$ are independently and identically distributed (i.i.d.) random variables w/ prob. $p(x_i)$

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

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

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

(i.e., $\Pr(\left| \sum x_i \right| \geq \varepsilon) \to 0$ as $n \to \infty$)

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

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

$\rightarrow$ Binomial dist. $p^k (1-p)^{n-k} \binom{n}{k}$

$\rightarrow$ 

bin. dist. $p^k (1-p)^{n-k} \binom{n}{k}$

as $n \to \infty$ (L.L.N.)
Typ. output: expect output $x$ with $p(x)$ times.

\[ \Rightarrow p(x_1 \rightarrow x_n) = p(x_1) \cdots p(x_n) \approx p(x_1)^{u(p(x_1))} \cdots p(x_n)^{u(p(x_n))} \]

\[ \Rightarrow \log p(x_1, \ldots, x_n) \approx n \log p(x) \]

\[ \Rightarrow \text{Shannon entropy of } p. \]

\[ \Rightarrow \text{expect typically } p(x_1, \ldots, x_n) \approx 2^{-nH(p)} \]

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

More precisely:

**Def.** We say that $x_1, \ldots, x_n$ is a $\varepsilon$-typical sequence if

\[ 2^{-n(H(p) + \varepsilon)} \leq p(x_1, \ldots, x_n) \leq 2^{-n(H(p) - \varepsilon)} \]

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

**Theorem:**

1. $\forall \varepsilon > 0 \forall \delta > 0 \exists N$ s.t. $u \geq N$: a random sequence of len. $u$ is $\varepsilon$-typical w/ prob. $\geq 1 - \delta$.
2. $\forall \varepsilon > 0 \forall \delta > 0 \exists N$ s.t. $u \geq N$:

\[ (1-\delta) 2^{-u(H(p) + \varepsilon/2)} \leq |T(u, \varepsilon)| \leq 2^{-u(H(p)) + \varepsilon} \]
Proof:

1. \(-\log p(x_i)\) is i.i.d. w.r.t. \(\mathcal{D}\) and hence \(\mathcal{D}\) is

\[
\Pr \left( \left| \frac{1}{n} \sum_{i=1}^{n} -\log p(x_i) - \mathbb{E}(-\log p(x)) \right| \geq \varepsilon \right) \leq \delta
\]

\[
= -\log p(x_1, \ldots, x_n) = H(p)
\]

\[
\Rightarrow \Pr \left( \left| -\frac{1}{n} \log p(x_1, \ldots, x_n) - H(p) \right| \geq \varepsilon \right) \leq \delta
\]

\[
\Rightarrow \text{w. prob. } \geq 1 - \delta, \quad -u(H(p) + \varepsilon) \leq \log p(x_1, \ldots, x_n) \leq -u(H(p) - \varepsilon)
\]

2. \(1 \geq \sum_{x_i - x_k \in T(u, \varepsilon)} p(x_1, \ldots, x_n) \geq \sum_{T(u, \varepsilon)} 2^{-u(H(p) + \varepsilon)} = |T(u, \varepsilon)| \cdot 2^{-u(H(p) + \varepsilon)}
\]

\[
1 - \delta \leq \sum_{T(u, \varepsilon)} p(x_1, \ldots, x_n) \leq |T(u, \varepsilon)| \cdot 2^{-u(H(p) - \varepsilon)}
\]

In brief: \(\varepsilon\)-tYPE sequence \(\Rightarrow \frac{\log p(x_1, \ldots, x_n)}{n} \text{ close to } H(p)\).

Asympt. a sequence is \(\varepsilon\)-tYPICAL \(\Rightarrow \mathbb{P} \to 1\),

and hence \(\sim 2^{-u(H(p))} \text{ } \varepsilon\)-tYPICAL w.g. \(\ldots\)
Application to entanglement:

\[ |X\rangle = \sum_x \sqrt{p(x)} |x\rangle |\phi_x\rangle \]

\[ \rightarrow |X\rangle^m = \sum \sqrt{p(x_1) \cdots p(x_m)} |x_1\rangle \cdots |x_m\rangle \]

Fix \( \epsilon > 0 \),

Define \( |\tilde{\Phi}_n\rangle := \sum_{x_1, \ldots, x_n \in T^{\frac{\epsilon}{m}}} \sqrt{p(x_1) \cdots p(x_n)} |x_1\rangle \cdots |x_n\rangle \)

and \( |\tilde{\Phi}_n\rangle := \frac{|\tilde{\Phi}_n\rangle}{\sqrt{\langle \tilde{\Phi}_n | \tilde{\Phi}_n \rangle}} \)

We have

\[ \langle \tilde{\Phi}_n | X^{\otimes n} \rangle = \sum_{x_1, \ldots, x_n} \frac{p(x_1, \ldots, x_n)}{\sqrt{\sum_{x_1, \ldots, x_n} p(x_1, \ldots, x_n)}} \xrightarrow{n \to \infty} 1 \]

and \( |T(n, \epsilon)| \leq 2^n (H(p) + \epsilon) \)

for \( n \) large enough.

Protocol: A prepares \( |\tilde{\Phi}_n\rangle \) locally & teleports Bob's part to Bob. \( \Rightarrow \) \( \ln u = \log |T(n, \epsilon)| = n(H(p) + \epsilon) \epsilon \ln b \).

\[ \Rightarrow \frac{\ln u}{n} \to H(p) + \epsilon \] "entanglement dilution rate",

"can be realised for any \( \epsilon > 0 \) \( \Rightarrow \) asymptotic rate \( H(p) \)."
Conversely: Distill ebits from $|x\rangle_{\hat{\omega}}$.

- Use $|\hat{v}_n\rangle$ instead since fidelity $\to 1$.

- $|\hat{v}_n\rangle$: max Schmidt coeff. $2^{-n(H(\rho)-\varepsilon)}$

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

Choose $n$ s.t. $\frac{2^{-n(H(\rho)-\varepsilon)}}{1-\delta} \leq 2^{-n}$

$\Rightarrow (2^{-n}, 2^{-n}, \ldots) \geq (\text{Schmidt coeffs. } \varepsilon |\hat{v}_n\rangle)$

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

Protocol:

1. A project onto $\varepsilon$-typ. subspace $\to |\hat{v}_n\rangle$

   (i.e.: $POVM \equiv \{ \Pi_0 = \Pi_{\varepsilon\text{-typ.}}, \Pi_\varepsilon = 1-\Pi_0 \}$)

   - Success prob. $1-\delta \to 1$

2. A C B convert $|\hat{v}_n\rangle$ to in ebits.

   $\Rightarrow$ works for any $n \leq n(H(\rho)-\varepsilon) - \log (1-\delta)$

   $\Rightarrow$ Rate $\frac{\ln n}{\ln \frac{2}{\varepsilon}} \to H(\rho) - \varepsilon$ t/c

   $\Rightarrow$ asymptotic "entanglement/distillable rate" $H(\rho)$. 
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 typically use the von Neumann entropy \( S(\rho) = - \text{tr}(\rho \log_2 \rho) \), i.e.,

\[
H(\rho) = S(\text{tr}_B |\psi\rangle \langle \psi|_1) = S(\text{tr}_A |\psi\rangle \langle \psi|_1).
\]

Protocol allows us to convert between any two states \( |\psi\rangle \) and \( |\phi\rangle \) provided \( \text{tr}_B(|\psi\rangle \langle \psi|_1) = \text{tr}_B(|\phi\rangle \langle \phi|_1) \) (by going via max. ent. state).

Result: The entropy of entanglement

\[
E(\ket{\psi}) = S(\text{tr}_A |\psi\rangle \langle \psi|_1) = S(\text{tr}_B |\psi\rangle \langle \psi|_1)
\]

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

a) Introduction

When is a mixed state entangled?

i) If $\rho_{AB}$ cannot be created by LOCC!

ii) If we can extract $\rho_{AB}$ from it.

iii) If it helps us do other tasks (not LOCC).

Use ii)

States which can be prepared by LOCC:

\[ \rho = \sum p_i \rho_i^A \otimes \rho_i^B \]

"separable state"

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

$\rho$ entangled $\iff$ $\rho$ is not separable (cannot be written as)

Given $\rho$, how can we test if it is entangled?

Problem: Given $\rho$, unclear how to find sep. decomposition

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

($\rightarrow$ ambiguity of ensemble integrals: need to optimize over 160 units!?)
6) Entanglement witnesses

Structure of sep. states:

Let $\rho = \sum_i p_i \rho_i \otimes \sigma_i \quad \sigma = \sum_j q_j \sigma_j \otimes \sigma_j$

$\Rightarrow \lambda \rho + (1-\lambda) \sigma = \sum_k \lambda_k \chi_k^A \otimes \chi_k^B \quad \lambda \in [0,1]$

with $\chi_k = (\lambda p_1, \lambda p_2, \ldots, (1-\lambda) \rho_1, \ldots)$;

$\chi_k^A = (\rho_1^{1/2}, \rho_2^{1/2}, \ldots, \rho_k^{1/2}, \ldots)$

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

Can find hyperplane s.t. all $\rho$ on one side are entangled.

Characterise plane + direction by vector $W = W^+:

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

i.e.: $\text{tr}(W \rho) < 0 \Rightarrow \rho$ entangled.

$W$: entanglement witness.
Notes:

- Need to make sure $\text{tr}(W_{\text{step}}) \geq 0$.
- Witness only detect certain rank states.
- Convex set $\equiv$ all tangent planes:
  \[ \Rightarrow \exists \text{ witness for any rank} \text{ states}. \]
- Witness linear operator $\Rightarrow$ experimentally measurable (in part, if $W$ is simple).

Example:

\[ W = \mathbb{F} \left( \frac{\text{d} \mathbb{F}}{\text{d} \mathbb{F}} \right); \quad \mathbb{F} = \sum_{i,j=1}^{d} X_{ij} \frac{\text{d} X_{ij}}{\text{d} X_{ij}} \]

\[ \text{Step } = \sum_i p^0_\small{i} \rho^0_\small{i} + \rho^\small{i} \]

\[ \text{tr} (W_{\text{step}}) = \sum_i p_\small{i} \text{tr} \left( \mathbb{F} \left( \rho^0_\small{i} \rho^\small{i} \right) \right) \geq 0 \]

\[ = \sum_i p_\small{i} \text{tr} \left( \rho^0_\small{i} \rho^\small{i} \right) \geq 0 \]

\[ \equiv \text{tr} \left( \mathbb{F} \text{tr} (\rho_0 \rho^a) \right) \geq 0 \]

\[ \text{Ultr.}:
\begin{align*}
(1) \quad & \text{tr} \left[ \mathbb{F} (A \otimes B) \right] \geq \text{tr} A B \\
(2) \quad & P_{i,j} \geq 0 \Rightarrow \text{tr} (P_{i,j}) \geq 0
\end{align*} \]

Which states does it detect? $\Rightarrow$ Those with prevalent anti-sym. component.

\[ |\psi> = \frac{1}{\sqrt{2}} (|01> - |10>) \Rightarrow F(|\psi>) = -|\psi> \Rightarrow <\psi|F|\psi> = -1. \]
$\rho = \lambda \left\{ \begin{array}{c} + \overline{2} \mapsto \frac{1}{4} \left( \begin{array}{c} 1 \ 0 \\ 0 \ 1 \end{array} \right) \quad \text{with} \quad \lambda \in \left[ -\frac{1}{2}, \frac{1}{2} \right], \end{array} \right.$

$\rho[\overline{\Phi} \Phi] = \lambda \left\{ \begin{array}{c} + \overline{2} \mapsto \frac{1}{4} \left( \begin{array}{c} 1 \ 0 \\ 0 \ 1 \end{array} \right) + (1-\lambda) \frac{1}{2} \left( \begin{array}{c} 1 \ 0 \\ 0 \ 1 \end{array} \right) \end{array} \right.$

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

$\Rightarrow \text{state cat. if } \lambda \leq \frac{1}{3}.$

What about $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$?

$|\overline{\Phi} |\phi^+\rangle = |\phi^+\rangle \Rightarrow \langle \phi^+ |\overline{\Phi} |\phi^+\rangle = 1 \Rightarrow \text{not deleted!}$

Optimal? Yes. E.g. $\rho = \lambda X \otimes \lambda X \otimes I$ : $\tau(\overline{\Phi} \Phi) = 0$.

Other examples: E.g. $W = I - d_{12} |12\rangle \langle 12|$, $|\Omega\rangle = \frac{1}{\sqrt{2}} \sum_{i=1}^{d} |i\rangle |d\rangle$

$\Rightarrow \text{Homework}$

$\ll / \text{Positive maps and the PPT criterion}$

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

Usually: require $\Lambda$ completely positive (CP)

Here: Will be interested in $\Lambda$ positive but not CP.
Consider $S_{\text{sep}} = \sum_i p_i S_i^A \otimes S_i^B$:

$$(\Lambda \circ I)(S_{\text{sep}}) = \sum_i p_i A(S_i^A) = \tilde{S}_{\text{sep}} = \tilde{S}_{\text{sep}} \geq 0$$

i.e.: $$(\Lambda \circ I)(\rho) \neq 0 \implies \rho \text{ entangled}$$

Most important example:

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

$$(\Lambda \circ I) = \rho^{T_A} \quad \text{"partial transpose"}$$

i.e.: $$\rho = \sum f_{ij}^i |i_j\rangle \langle j_i| \implies \rho^{T_A} = \sum f_{ij}^i |i_j\rangle \langle j_i|$$

l.c.: $$\rho^{T_A} \neq 0 \implies \rho \text{ entangled}$$

positive partial transpose (PPT) criterion

E.g.: $$|\rho\rangle = \frac{1}{d} \sum_{i=1}^d |i_i\rangle$$

$$\Rightarrow (|\rho\rangle \langle \rho|)^{T_A} = \frac{1}{d} \sum_{i=1}^d (|i_i\rangle \langle j_j|)^{T_A} = \frac{1}{d} \sum |j_j\rangle \langle i_i|.$$
Not positive: e.g. \( \langle \psi | \sigma_0 = \frac{1}{2} (|10\rangle - |01\rangle) \):

\[
\langle \psi | \left( |1\rangle \langle 1| \right) \sigma_k \left| \psi \rangle \rangle = \frac{1}{2} \langle 01| - \langle 10| \right) |10\rangle - |01\rangle = -1
\]

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

E.g. \( d = 2 \):

\[
\rho = \begin{pmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/4 \\ 1/4 & 0 & 0 & 1/4 \end{pmatrix} + \frac{1-\lambda}{4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\]

\[
\Rightarrow \sigma_k\rho \sigma_k = \begin{pmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 1/4 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{pmatrix}
\]

\[
\Rightarrow \text{positive iff } \frac{1}{2} \leq \frac{1-\lambda}{4} \iff \lambda \leq \frac{1}{3}
\]

Notes: Independency of unitary \( A \) & \( B \) \( \Rightarrow \) detects all PPT states!

(i.e.: Stronger than coherency)

In fact: PPT criterion detects all entangled states

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

\( \Rightarrow \) "PPT cannot detect all states"
Example:

\[ \Lambda(x) = \text{tr}(x) I - x \]

\[ (\Lambda \otimes I)(\rho) = \text{tr} \rho \cdot (I \otimes \Lambda \rho) - \rho = I \otimes \rho - \rho \neq 0 \Rightarrow \text{entangled} \]

"reduction criterion" \( I \otimes \rho \neq \rho \) Homework.

dl) Relation of witnesses & positive maps:

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

Witness: bipartite "state" (reduces: operator) \( W \)

\( \Lambda \) map: Jamiołkowski map of \( W \)

\[ \Lambda(x) = \text{tr} \left( W^T (x_A \otimes I_B) \right) = \text{tr} \left( W (x_A \otimes I_B) \right)^T \]

Then:

\[ \text{tr}(W (A \otimes B)) = \text{tr}(\Lambda(B) (A \otimes I)) \cdot B = \text{tr}(\Lambda(A)^TB) \]

\[ = \Lambda(A)^T \]

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

\[ = (\Lambda \otimes I)(A \otimes B) \]

Linearity \( \Rightarrow \) \( \text{tr}(U \rho) = d \langle \Omega | U (\Lambda \otimes I)(\rho) | \Omega \rangle \).

i.e.: \( \text{tr}(U \rho) < 0 \Rightarrow (\Lambda \otimes I)(\rho) \neq 0 \).

\( \Rightarrow \Lambda \) strange than \( W \)!
e.g. $\mathcal{W} = \mathbb{I}$:

$$\Lambda(X) = \text{tr} \left( \mathcal{W}(I_A \otimes X_B) \right)^T = \text{tr} \left( I_A \cdot X_B \right)^T = X_B^T.$$

$\Rightarrow$ PPT criterion!

Note: PPT strictly stronger: $\mathcal{W}$ could not detect e.g. $|\Psi\rangle$.

**Corollary:** A state is entangled if and only if

$$(\Lambda \otimes I)(\rho) \geq 0 \text{ positive } \Lambda \text{ (as sep. states $\Leftrightarrow$ all entries)}$$

---

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:

"Extractable entanglement" $E_D$:

LOCC protocol $E_m$: $\|E_m(s_{\Psi^n}) - 1 \otimes \mathcal{E}_m^{X^n} \| \to 0$.

Note: generally $E_c \neq E_D$: no unique measure!
Problem: $E$ very hard, $E_c/E_D$ (almost) impossible to compute $\Rightarrow$ need other measures.

(But: Cases w/ $E_D \equiv 0$ known, e.g. PPT states. Convexity open problem.)

Have seen: $g^{TA}$ has neg. eigenvalues $\Rightarrow$ $g$ entangled.

Use as ent. measure:

\[
\text{Negativity } N(g) = \frac{1}{2} \left( \sum \lambda_i(g^{TA}) \right) - 1
\]

\[
= \|g^{TA}\|_1
\]

\[
= \frac{1}{2} \left( \|g^{TA}\|_1 - 1 \right) = \sum \left( -\lambda_i(g^{TA}) \right) \text{neg. eigenvals}
\]

or log-negativity $\ln N(g) = \log_2 \|g^{TA}\|_1$

What are desired properties for ent. measures $E$?

\bullet $E_D \leq E \leq E_c$.

\bullet $0$ on sep. states, $\neq 0$ in ent. states.

\bullet additive: $E(g_{A\otimes B}) = E(g_A) + E(g_B)$

\bullet LOCC - monotone: cannot be increased by LOCC.

\bullet Coincides w/ $E(14) = S_k(\rho_A^{14}\otimes \chi^{14})$ for pure states.
Negativity / Log-monotony:

\( \mathcal{W} \): LOCC - monotone

- 0 on sep. states, but can be 0 on ent. states.
- \( \neq E(1|4) \) for pure
- not additive

\( E_1 \): additive

- 0 on sep., but can be 0 on ent. states
- \( \neq E(1|4) \) for pure
- not an LOCC monotone.