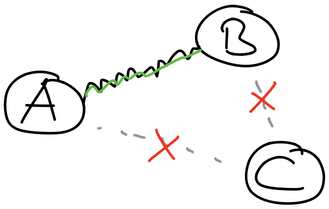
Monogamy of Entanglement



$$\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$$

$$\Downarrow$$

$$\rho_{ABC} = \rho_{AB} \otimes \rho_C$$

Can we make this more quantitative?

$\Longrightarrow \rho_{AC} = \rho_A \otimes \rho_C$ (etc.)

What is an entangled state?

Pure states: $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle \longrightarrow \boxed{\text{PSet}}$

$\Longleftrightarrow \rho_A$ not pure

if state is pure

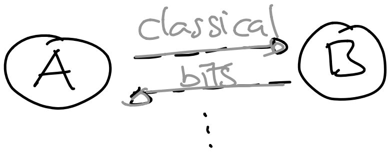
In general: ρ_{AB} is entangled if

$$\rho_{AB} \neq \boxed{\sum_i p_i \, \rho_A^i \otimes \rho_B^i}$$

separable (unentangled) state

MIXTURE; not a superposition!

Why?



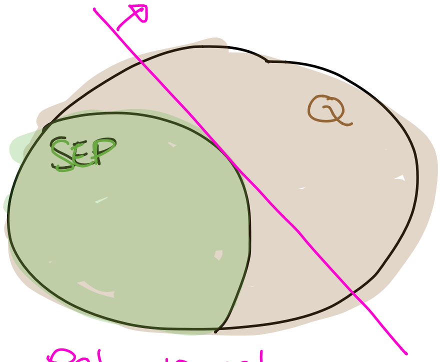
- All states that can be produced by LOCC (local ops & classical commun.)
- E.g., classical probability distributions:

$$\rho_{AB} = \sum_{a,b} p(a,b) \, |a\rangle\langle a| \otimes |b\rangle\langle b|$$

- Convex geometry perspective:

$$\{\rho_{AB} \geq 0,\ \operatorname{tr} \rho_{AB} = 1\} = Q$$
$$\rotatebox{90}{$\subseteq$}$$
$$\{\rho_{AB} \text{ separable}\} =: SEP$$

Convex sets!



→ entanglement witness

Pset

- NP-hard to test if given $\rho_{AB} \in SEP$!

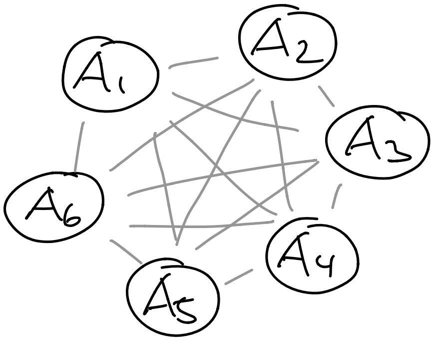
...but we will discuss the best known test...

Monogamy and Symmetry:

(i) In a permutation-symmetric state

$$|\psi_{A_1 \ldots A_n}\rangle \in \mathrm{Sym}^n(\mathbb{C}^d)$$

would expect that $\rho_{A_i A_j}$ "not very" entangled:



Ex: Mean-field $H = \sum_{i<j} \boxed{h_{ij}}$

↑ same interaction

$\hookrightarrow |E_0\rangle \in \mathrm{Sym}^n$

if nondegenerate

Pset

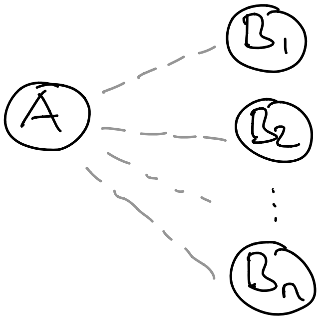
De Finetti: $\rho_{A_1 \ldots A_k} \approx \boxed{\int d\psi\, p(\psi)\, |\psi\rangle\langle\psi|^{\otimes k}}$

E.g.:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$ entangled!

$$\Longrightarrow \rho_{A_1A_2} = \frac{1}{2}\left[|0\rangle\langle 0|^{\otimes 2} + |1\rangle\langle 1|^{\otimes 2}\right]$$ ← NOT ENTANGLED !!!

② If a state ρ_{AB_1} can be extended to $\rho_{AB_1\cdots B_n}$ s.th. $\rho_{AB_1} = \dots = \rho_{AB_n}$ then ρ_{AB_1} "not very" entangled



$$\rho_{AB_1} \approx \boxed{\sum_i p_i \, \rho_A^{(i)} \otimes \rho_{B_1}^{(i)}}$$

distance ?

Trace distance:

$$T(\rho,\sigma) = \max_{0 \le Q \le I} \mathrm{tr}\left[Q(\rho-\sigma)\right] = \frac{1}{2}\|\rho-\sigma\|_1$$

- If $\rho = |\psi\rangle\langle\psi|$, $\sigma = |\phi\rangle\langle\phi|$ pure:

$$T(\rho,\sigma) = \sqrt{1-|\langle\psi|\phi\rangle|^2}$$

Pset 1

overlap!

trace norm:

$$\|\Delta\|_1 = \sum_i |\lambda_i|$$

for $\Delta = \sum_i \lambda_i |e_i\rangle\langle e_i|$

① Proof of the de Finetti theorem

$$|\Phi\rangle \in \mathrm{Sym}^{k+n}(\mathbb{C}^d)$$ MORE CONVENIENT

Idea: Measure $\{Q_\psi\}$ on last n systems

→ first k should be $|\psi\rangle^{\otimes k}$

$$\Phi_k = \mathrm{tr}_n\left[|\Phi\rangle\langle\Phi|\right] \overset{\downarrow}{=} \mathrm{tr}_n\left[(I_k \otimes \Pi_n)\,|\Phi\rangle\langle\Phi|\right]$$

$$= \binom{n+d-1}{n} \int d\psi \; \mathrm{tr}_n\left[(I_k \otimes |\psi\rangle^{\otimes n}\langle\psi|^{\otimes n})\,|\Phi\rangle\langle\Phi|\right]$$

$$\overset{\text{cyclic.}}{=} \binom{n+d-1}{n} \int d\psi \, (I_k \otimes \langle\psi|^{\otimes n})\,|\Phi\rangle\langle\Phi|\,(I_k \otimes |\psi\rangle^{\otimes n})$$

$$= \int d\psi \; p(\psi) \; |V_\psi\rangle\langle V_\psi|$$

where we introduced

$$\underbrace{\sqrt{p(\psi)}}_{\text{prob. density}} \cdot \underbrace{|V_\psi\rangle}_{\text{unit vector}} = \binom{n+d-1}{n}^{1/2} (I_k \otimes \langle\psi|^{\otimes n})\,|\Phi\rangle$$

<u>Claim</u>: $\rho_k = \int d\psi \, p(\psi)\,|V_\psi\rangle\langle V_\psi| \approx \int d\psi \; p(\psi) \; |\psi\rangle^{\otimes k}\langle\psi|^{\otimes k}$

Average overlap: Will justify later!

$$\int d\psi\, p(\psi)\, |\langle v_\psi | \psi^{\otimes k}\rangle|^2$$

$$= \int d\psi\, p(\psi)\, \langle v_\psi | \psi^{\otimes k}\rangle \langle \psi^{\otimes k} | v_\psi\rangle$$

$$= \binom{n+d-1}{n} \int d\psi\, |\langle \Phi | \psi^{\otimes (n+k)}\rangle|^2$$

$$= \binom{n+d-1}{n} \binom{n+k+d-1}{n+k}^{-1} \underbrace{\langle \Phi | \Pi_{n+k} | \Phi \rangle}_{=1}$$

$$\overset{\text{LAST}}{\underset{\text{THU}}{\boxed{\geq}}}\; 1 - \frac{kd}{n}.$$

Almost done: Could be on the $\boxed{\text{PSET}}$

$$T\left(\rho_k, \int d\psi\, p(\psi)\, |\psi\rangle^{\otimes k}\langle \psi|^{\otimes k}\right)$$

$$= \frac{1}{2} \left\| \int d\psi\, p(\psi)\, [\, |v_\psi\rangle\langle v_\psi| - |\psi\rangle^{\otimes k}\langle \psi|^{\otimes k} \right\|_1$$

$$\leq \int d\psi\, p(\psi)\, \frac{1}{2} \left\| \, |v_\psi\rangle\langle v_\psi| - |\psi\rangle^{\otimes k}\langle \psi|^{\otimes k} \right\|_1$$

$$= \int d\psi\, p(\psi) \sqrt{1 - |\langle v_\psi | \psi^{\otimes k}\rangle|^2}$$

$$\overset{\text{JENSEN}}{\boxed{\leq}} \left[\int d\psi\, p(\psi) \left(1 - |\langle v_\psi | \psi^{\otimes k}\rangle|^2\right)\right]^{1/2}$$

$$= \Big[1 - \underbrace{\int d\psi\, p(\psi)\, |\langle v_\psi | \psi^{\otimes k} \rangle|^2}_{\text{above !!!}} \Big]^{1/2}$$

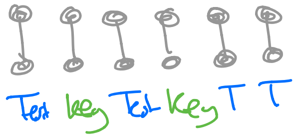
$$\leq \Big[1 - \Big(1 - \frac{kd}{n}\Big) \Big]^{1/2} = \sqrt{\frac{kd}{n}}$$

$$\Longrightarrow \quad \rho_k \approx \int d\psi\, p(\psi)\, |\psi\rangle\langle\psi|^{\otimes k} \quad \text{if } k \ll n$$

$\square$

Aside: De Finetti is useful in Q. crypto!

- general attacks ⟶ "collective" attacks
- DI-QKD:



Bell tests at random sites

Same if ρ is mixed state on $\mathrm{Sym}^N(\mathbb{C}^d)$. $(N = n + k)$

What if only $[R_\pi, \rho] = 0$? ⟵ "Permutation-invariant"

PSET?

Fact: Exists purification $|\Phi\rangle \in \mathrm{Sym}^N(\mathcal{H}_A \otimes \mathcal{H}_A)$!

$\hookrightarrow \; \Phi_k \approx \int d\psi_{AA'}\, p(\psi)\, |\psi_{AA'}\rangle^{\otimes k} \langle \psi_{AA'}|^{\otimes k}$

$\hookrightarrow \; \rho_k \approx \int d\rho_A\, p(\rho)\, \rho^{\otimes k}$ up to $\frac{kd^2}{n}$

② Extendibility

If ρ_{AB_1} separable:

$$\rho_{AB_1} = \sum_i p_i \rho_A^i \otimes \rho_B^i$$

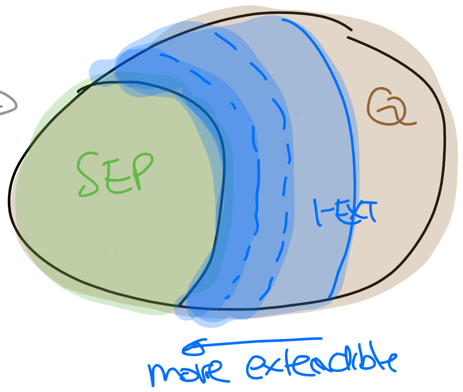
$$\rightsquigarrow \rho_{AB_1 \cdots B_n} = \sum_i p_i \rho_A^i \otimes \left(\rho_B^i\right)^{\otimes n}$$

"symmetric" n-extension $\boxed{[I_A \otimes R_\pi, \rho] = 0}$

IF NOT SYMM: SYMMETRIZE!

→ $\boxed{\text{Pset}}$

Claim: If ρ_{AB_1} is symm. n-extendible then $O(\frac{1}{n})$ close to SEP!



- GOOD ENTANGLEMENT TEST!
  - ↳ semidefinite program
- Optimal? → $\boxed{\text{PSET}}$