Lecture 4

Oct 6, 2025

② If we apply $\mathcal{U}$ then each state updates to $\mathcal{U}|\psi_a\rangle$. So

$$\rho' = \sum_a p_a \, \mathcal{U} \, |\psi_a\rangle\langle\psi_a| \, \mathcal{U}^\dagger$$

$$= \mathcal{U}\left(\sum_a p_a |\psi_a\rangle\langle\psi_a|\right)\mathcal{U}^\dagger \quad \text{linearity}$$

$$= \mathcal{U}\rho\,\mathcal{U}^\dagger.$$

③ Considering measuring $|\psi_a\rangle$.

$$\Pr(\text{meas} = 0) = |\langle 0| \otimes \mathbb{1} \, |\psi_a\rangle|^2$$

$$= \| \, |0\rangle\langle 0| \otimes \mathbb{1} \, |\psi_a\rangle \|^2 \qquad P^2 = P \text{ for proj.}$$

$$= \langle\psi_a| \left(|0\rangle\langle 0| \otimes \mathbb{1}\right)\underbrace{\left(|0\rangle\langle 0| \otimes \mathbb{1}\right)}_{\text{proj.}} |\psi_a\rangle$$

$$= \langle\psi_a| \left(|0\rangle\langle 0| \otimes \mathbb{1}\right) |\psi_a\rangle$$

$$= \mathrm{tr}\left(\left(|0\rangle\langle 0| \otimes \mathbb{1}\right) |\psi_a\rangle\langle\psi_a|\right) \quad \text{cyclicity.}$$

$$\text{post-measurement} = \frac{\left(|0\rangle\langle 0| \otimes \mathbb{1}\right)|\psi_a\rangle}{\| \langle 0| \otimes \mathbb{1} \, |\psi_a\rangle \|}$$

$$\| \langle 0| \otimes \mathbb{1} |\psi_a\rangle \|^2 = \langle\psi_a| \left(|0\rangle\langle 0| \otimes \mathbb{1}\right) |\psi_a\rangle = \mathrm{tr}\left(|0\rangle\langle 0| \otimes \mathbb{1} \, |\psi_a\rangle\langle\psi_a|\right).$$

post-measurement d.m.

$$\rho'_a = \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})}{\mathrm{tr}(|0\rangle\langle 0| \otimes \mathbb{1}\, |\psi_a\rangle\langle\psi_a|)}.$$

put these 2 together, we get measurement of $|\psi_a\rangle\langle\psi_a|$ result. So now

ρ' ← post O measurement should be defined as

$$\rho' = \sum_a pr(a \mid x=0) \cdot \rho'_a$$

$$= \sum_a \frac{pr(a \mid x=0)}{pr(x=0 \mid a)} (|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})$$

$$= \sum_a \frac{pr(a)}{pr(x=0)} (|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})$$

$$= \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, \rho\, (|0\rangle\langle 0| \otimes \mathbb{1})}{\sum_a pr(x=0 \mid a)\, p_a}$$

$$= \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, \rho\, (|0\rangle\langle 0| \otimes \mathbb{1})}{\sum_a p_a\, \mathrm{tr}(|0\rangle\langle 0| \otimes \mathbb{1}\, |\psi_a\rangle\langle\psi_a|)} =$$

$$= \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})}{\mathrm{tr}\left((|0\rangle\langle 0| \otimes \mathbb{1})\, \rho\right)} .$$

Exercise Show that $\mathrm{tr}(\rho^2) = 1$ iff ρ is pure (i.e. $\rho = |\psi\rangle\langle\psi|$).

Pf. If $\rho = |\psi\rangle\langle\psi|$, then $\rho^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = \rho$.

So $\mathrm{tr}(\rho^2) = \mathrm{tr}(\rho) = 1$, proves $\Leftarrow$ direction.

For $\Rightarrow$ direction, write ρ in eigenbasis so $\rho = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$ with $\{|\psi_i\rangle\}$ orthonormal and $\sum \lambda_i = 1$ since $\mathrm{tr}(\rho) = 1$.

$$\mathrm{tr}(\rho^2) = \mathrm{tr}\left(\sum_{ij} \lambda_i \lambda_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|\right)$$

$$= \mathrm{tr}\left(\sum_i \lambda_i^2 |\psi_i\rangle\langle\psi_i|\right) = \sum \lambda_i^2 \leq \sum \lambda_i = 1$$

with equality only if $\lambda_i^2 = \lambda_i \ \forall i$. so $\lambda_1 = 1$
$\lambda_{2 \ldots} = 0$.

so $\rho = |\psi_1\rangle\langle\psi_1|$ pure.

Aside: $\rho = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$ means $|\psi_i\rangle$ w pr λ_i.

Aside: For $f: \mathbb{R} \to \mathbb{R}$, $f(\rho) := \sum_i f(\lambda_i) |\psi_i\rangle\langle\psi_i|$.

Why do we need to understand density matrices?

Density matrices help define the partial state of a system which is entangled.

For instance, when Alice & Bob hold an EPR pair, what is the state of Alice system by itself?

Notation If ρ_{AB} is the state of the system over $\underbrace{\mathbb{C}_A^{d_A}}_{\text{Alice's qubits}} \otimes \underbrace{\mathbb{C}_B^{d_B}}_{\text{Bob's qubits}}$, then call ρ_A the state on Alice's system.

ρ_B the state on Bob's system.

Easy cases: $\rho_{AB} = \rho_A \otimes \rho_B$.

Then ρ_A is obvious.

How about $\rho_{AB} = \sum p_i \rho_A^i \otimes \rho_B^i$ $\{p_i\}$ prob. dist.

Then we expect $\rho_A = \sum p_i \rho_A^i$

$$\rho_B = \sum p_i \rho_B^i .$$

It becomes harder when the states are entangled and not just prob. mixtures.

What are the properties that ρ_A should have?

① The statistics of measuring ρ_A should be identical to that of measuring only

Alice's qubits of ρ_{AB}.

(2) Let $\sigma_{AB} = \left(U_A \otimes \mathbb{1}\right) \rho_{AB} \left(U_A^{\dagger} \otimes \mathbb{1}\right)$

Then $\sigma_A = U_A \rho_A U_A^{\dagger}$. Meaning, unitary transform by Alice can be calculated from just ρ_A.

(3) Any action on Bob's qubits cannot change the state of Alice's qubits.

<u>Def</u> (Partial trace) Let $|b_1\rangle \ldots |b_{d_B}\rangle$ be a basis for Bob's qubits/system, then for <u>any</u> <u>matrix</u> ρ_{AB}

$$\mathrm{tr}_B(\rho_{AB}) := \sum_{i=1}^{d_B} \left(\mathbb{1}_A \otimes \langle b_i|\right) \rho_{AB} \left(\mathbb{1}_A \otimes |b_i\rangle\right).$$

If ρ_{AB} is a density matrix, what is the operational meaning of $\mathrm{tr}_B(\rho_{AB})$?

Ans: Bob measures his system according to basis $\{|b_i\rangle\}$

but does not tell Alice the outcome.

<u>Note</u> It remains to show that this def does not depend on the choice of basis.

<u>Ex</u>. $\rho_{AB} = |\Phi_{11}\rangle\langle\Phi_{11}|_{AB} = \frac{1}{2}\left(|01\rangle_{AB} - |10\rangle_{AB}\right)\left(\langle 01|_{AB} - \langle 10|_{AB}\right)$

$$\cancel{\rho_A} = \sum_{i=0}^{1} \left(\mathbb{1}_A \otimes \langle i|_B\right) \rho_{AB} \left(\mathbb{1}_A \otimes |i\rangle_B\right)$$

$$= \frac{1}{2}\Big[\left(\mathbb{1}\otimes\langle 0|\right)\left(|01\rangle - |10\rangle\right)\left(\langle 01| - \langle 10|\right)\left(\mathbb{1}\otimes|0\rangle\right)$$

$$+ \left(\mathbb{1}\otimes\langle 1|\right)\left(|01\rangle - |10\rangle\right)\left(\langle 01| - \langle 10|\right)\left(\mathbb{1}\otimes|1\rangle\right)\Big]$$

$$= \frac{1}{2}\left[\left(-|1\rangle\right)\left(-\langle 1|\right) + \left(|0\rangle\right)\left(\langle 0|\right)\right]$$

$$= \frac{1}{2}\mathbb{1}.$$

<u>Claim</u> $\rho_A = \mathrm{tr}_B(\rho_{AB})$.

Why is this the correct definition?

First let us prove that the def of partial trace does not depend on choice of $\{|b_i\rangle\}$.

<u>Ex</u>. If $\langle\psi|\rho|\psi\rangle = \langle\psi|\rho'|\psi\rangle$ for all unit vectors $|\psi\rangle$ then $\rho = \rho'$.

For any $|\psi\rangle$, let $\rho_B^\psi := (\langle\psi_A| \otimes \mathbb{1}_B)\, \rho_{AB} (|\psi_A\rangle \otimes \mathbb{1}_B)$.

Now,

$$\langle\psi|\, tr_B(\rho_{AB})\, |\psi\rangle$$

$$= \langle\psi_A| \left(\sum_{i=1}^{d_B} (\mathbb{1}_A \otimes \langle b_i|)\, \rho_{AB}\, (\mathbb{1}_A \otimes |b_i\rangle) \right) |\psi_A\rangle$$

$$= \sum_{i=1}^{d_B} \langle b_i|\, \rho_B^\psi\, |b_i\rangle = \sum_{i=1}^{d_B} tr(\rho_B^\psi)$$

which is independent of $\{|b_i\rangle\}$ as trace is basis indep.

① Let V_B be any unitary. Let $|1\rangle \dots |d_B\rangle$ be basis for B.

$$\mathrm{tr}_B\left((\mathbb{1}_A \otimes V_B) \rho_{AB} (\mathbb{1}_A \otimes V_B^\dagger) \right)$$

$$= \underbrace{\sum_{i=1}^{d_B} \left(\mathbb{1}_A \otimes \langle i | V_B \right) \rho_{AB} \left(\mathbb{1} \otimes V_B^\dagger | i \rangle \right)}_{\substack{\text{equivalent to taking partial trace} \\ \text{w.r.t. basis } \{V|i\rangle\}.}}$$

$$= \mathrm{tr}_B(\rho_{AB}) \quad \leftarrow \text{Bob's actions do not change } \rho_A.$$

② Let U_A be any unitary.

$$U_A \otimes \mathbb{1}_B \, \mathrm{tr}_B(\rho_{AB}) \, U_A^\dagger \otimes \mathbb{1}_B$$

$$= \sum_i \left(U_A \otimes \langle i |_B \right) \rho_{AB} \left(U_A \otimes | i \rangle_B \right)$$

$$= \sum_i \left(\mathbb{1}_A \otimes \langle i |_B \right) U_A \rho_{AB} U_A^\dagger \left(\mathbb{1}_A \otimes | i \rangle_B \right)$$

$$= \mathrm{tr}_B(U_A \rho_{AB} U_A^\dagger).$$

Def. The maximally mixed state in d-dimensions is $\frac{1}{d}\mathbb{1}_d$. For qubits, $\frac{1}{2^n}\mathbb{1}_{2^n}$.

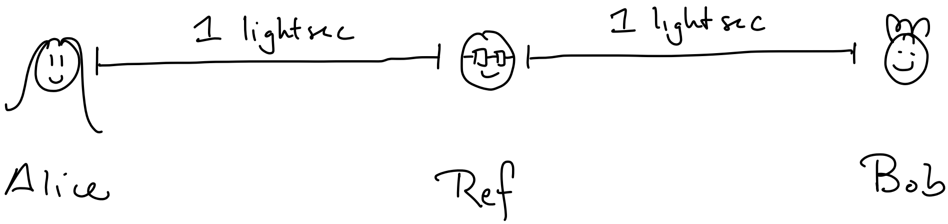
Def. A state ρ_{AB} between Alice and Bob each of n qubits is maximally entangled if $\rho_A = \frac{1}{2^n}\mathbb{1}_{2^n}$.

In class exercise: Every maximally entangled state is $\sum_{i=1}^{\leq 2^n} p_i \left(\mathbb{1}_A \otimes U_B^i\right)|\Phi\rangle\langle\Phi|\left(\mathbb{1}_A \otimes U_B^{i\dagger}\right)$

where $|\Phi\rangle = \sum_{i=1}^{2^n} \frac{1}{\sqrt{2^n}} |i\rangle|i\rangle$.

Today: The CHSH game and "spooky-action" at a distance.

Consider the following game:



Ref samples $x, y \in \{0, 1\}$ and sends x to Alice and y to Bob. He asks for answers $a, b \in \{0, 1\}$ from Alice and Bob, respectively.

Alice and Bob must answer in $2 + \epsilon$ lightsecs.

They win if $a \oplus b = x \cdot y$.

What is their opt. success prob.?

Space-seperation is just to force no communication.

If Alice and Bob employ classical strategies, the best strategy only wins w pr $= 3/4$.

But if they use quantum strategies, they can win with probabilities up to $\cos^2 \pi/8 \sim 0.878$.

Next two lectures: understand the quantum strategy, prove it is optimal, understand how it characterizes the state of Alice and Bob's q.c.'s.

Classical Best deterministic strategy $a = 0$, $b = 0$ independent of input.

What if Alice & Bob share classical randomness?

Let $A_r, B_r : \{0,1\} \to \{0,1\}$ be the strategies for rand. r.

Then

$$\Pr[\text{win}] = \Pr_{x,y,r}\left[A_r(x) \oplus B_r(y) = xy \right]$$

$$= \sum_r \Pr[r] \cdot \Pr_{x,y}\left[A_r(x) \oplus B_r(y) = xy \right]$$

$$\leq \max_{r} \Pr_{x,y}\left[A_r(x) \oplus B_r(y) = xy\right]$$

$$\leq 3/4.$$

<u>Quantum</u> What if Alice and Bob share an EPR pair?

<u>Idea</u> Depending on the input $x \in \{0,1\}$, Alice makes a measurement of her half of the EPR pair.

Strategy: $\{|\alpha_x^a\rangle \in \mathbb{C}^2\}$ for Alice

where $\langle {}^0_x | {}^1_x \rangle = 0$.

likewise $\{|\beta_y^b\rangle \in \mathbb{C}^2\}$ for Bob,

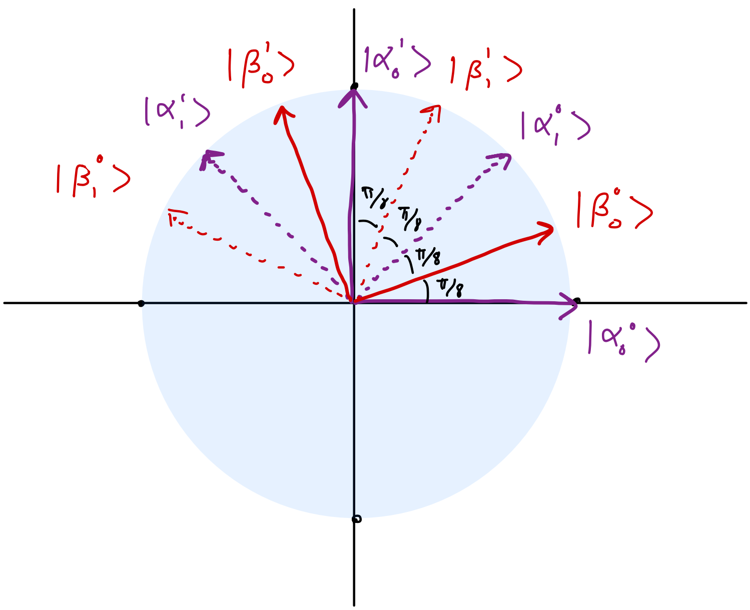
where $\langle \beta_x^0 | \beta_x^1 \rangle = 0$.

When Alice gets input x, she measures her half of the EPR pair with basis $|\alpha_x^0\rangle, |\alpha_x^1\rangle$ and answers accordingly. Likewise for Bob. So,

$$\Pr[a,b \mid x,y] = \left|\langle \alpha_x^a, \beta_y^b \mid EPR\rangle\right|^2.$$

Let us first write out the optimal strategy and then return to the more interesting part of proving it's optimality.

Easiest to draw a picture.



How do we analyze this?

① Recall from earlier lectures our def

$$|\theta\rangle := \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$

and $\langle \theta | \theta + \gamma \rangle = \cos \gamma$.

(2) For any basis $|v\rangle, |w\rangle$ of $\mathbb{C}^2$,

$$|EPR\rangle = \frac{1}{\sqrt{2}}\left(|v\rangle|v^*\rangle + |w\rangle|w^*\rangle \right)$$ (on hw 2)

Using these 2 facts and the angles between vectors we can analyze the success of this game.

$$\Pr[\text{win}] = \sum_{x,y} \Pr[x,y] \cdot \sum_{a,b} \Pr[a,b|x,y] \cdot \underbrace{\mathbb{1}\{a \oplus b = xy\}}_{\text{win condition}}$$

$$= \frac{1}{4}\Big[|\langle \alpha_0^0, \beta_0^0 | EPR\rangle|^2 + |\langle \alpha_0^1, \beta_0^1 | EPR\rangle|^2 \quad (x,y) = (0,0)$$

$$+ |\langle \alpha_0^0, \beta_1^0 | EPR\rangle|^2 + |\langle \alpha_0^1, \beta_1^1 | EPR\rangle|^2 \quad (x,y) = (0,1)$$

$$+ |\langle \alpha_1^0, \beta_0^0 | EPR\rangle|^2 + |\langle \alpha_1^1, \beta_0^1 | EPR\rangle|^2 \quad (x,y) = (1,0)$$

$$+ |\langle \alpha_1^0, \beta_1^1 | EPR\rangle|^2 + |\langle \alpha_1^1, \beta_1^0 | EPR\rangle|^2 \Big] \quad (x,y) = (1,1)$$

Recognize

$$\langle \alpha_x^a, \beta_y^b | EPR \rangle = \langle \alpha_x^a, \beta_y^b | \cdot \frac{|\beta_y^0\rangle|\beta_y^0\rangle + |\beta_y^1\rangle|\beta_y^1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}} \langle \alpha_x^a | \beta_y^b \rangle$$

$$= \frac{1}{\sqrt{2}} \cos\theta \leftarrow \text{angle between } |\alpha_x^a\rangle, |\beta_y^b\rangle$$

Notice by design, all terms in $\Pr[\text{win}]$ evaluate to $\pm \frac{1}{\sqrt{2}} \cos \pi/8$.

So $\Pr[\text{win}] = \frac{1}{4}\left[8 \cdot \frac{1}{2} \cos^2 \pi/8 \right] = \cos^2 \pi/8$

$= 0.854.$

So Alice and Bob can win game with quantum strategies with higher prob than classical.

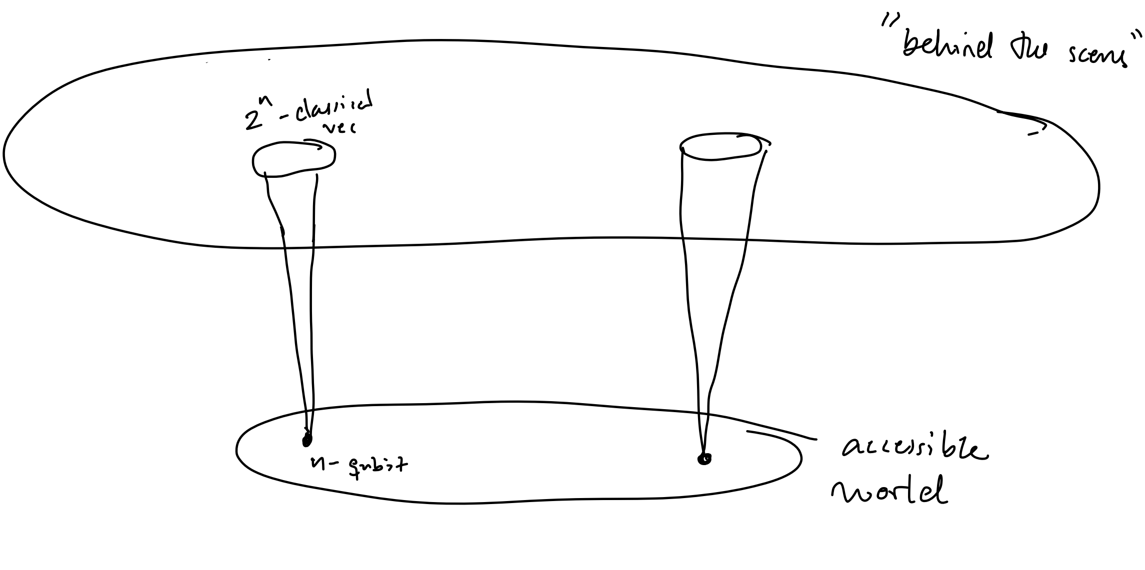
"Clauser, Hauser, Shimony, Holt" (CHSH) experiment.

aka Bell inequality experiment.

aka a non-local game.

We know that q. mechanics says that n-qubit states can be described by a 2^n-dim vector. Meaning, that if nature is doing a lot of computation "behind the scenes"

But where is that info stored?



CHSH game proves that ↑ picture is incorrect!

The information about the state of the system <u>cannot be held locally</u> assuming a speed limit on information.

This is because local info could not produce the statistics needed to win the game with prob. > $3/4$.

To describe the state of the system, we need to have a global description.

Indeed $\rho = |EPR\rangle\langle EPR|_{AB}$, then $\rho_A = \rho_B = \frac{1}{2}\mathbb{1}_2$.

The key is that the coins are correlated!

Can we experimentally verify CHSH?

Can actually conduct this and has been done!

Does it prove that quantum mechanics is <u>correct</u>?

<u>No</u>. Since the q. advantage is only probabilistic

it is <u>evidence</u> that our world isn't classical.

Suppose a ref observes Alice & Bob winning the game 80% of the time. How many games would they have to play before he is convinced with $1-10^{-9}$ confidence that the world isn't classical?

Chernoff bounds: $X = \sum_i^n X_i \leftarrow$ per game success

$$\Pr\left[X \geq (1+\delta)\mu \right] \leq \exp\left(-\frac{\delta^2 \mu}{2+\delta} \right)$$

here $\mu = 0.75n$ $\quad \delta = \frac{0.8}{0.75} < 1.07$

$$\Pr\left[X \geq 0.8n\right] \leq \exp\left(-0.27n\right)$$

want $\quad \exp\left(-0.27n\right) \leq 10^{-9}$

$$0.27n \geq 9 \ln 10$$

$$n \geq 77.$$

Does it prove the world is quantum? No.

For all we know, there is a stronger theory consistent with quantum mechanics.

Ex. Noisy telepathy! Alice and Bob are telepathic with a success rate of 80%. Perfect telepathy and they win with probability 1.

Is $\cos^2 \pi/8$ the optimal quantum strategy?

Can we do better if Alice and Bob share multiple EPR pairs?