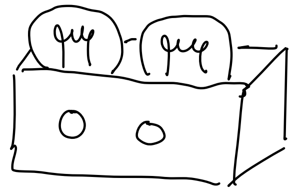
Lecture 3

Oct 1, 2025

Deutsch-Josza game

Say there is a box 

two lights & two buttons.

Press a button and one of the two lights turns on (deterministically).

How many (button presses) are required to decide if actions of the two buttons are same/different?

Classically 2. Also learn which light.

Quantumly 1. Don't know which light.

Need to be able to query box in superposition

Box: $f : \{0,1\} \longrightarrow \{0,1\}$.

Want to know if $f(0) = f(1)$ or not.

Consider unitary U_f s.t. $\forall\, x, y \in \{0,1\}$

$$|x\rangle|y\rangle \overset{U_f}{\longmapsto} |x\rangle|y \oplus f(x)\rangle$$

U_f is defined everywhere by linearity.

<u>Algorithm</u>

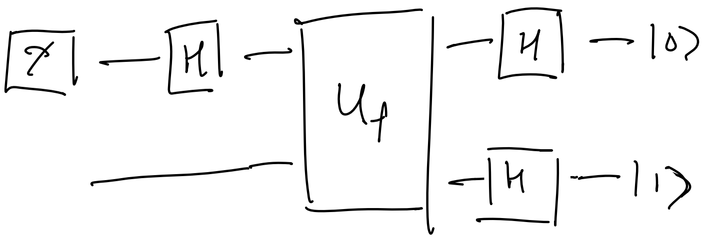
① Start with $|0\rangle \otimes |1\rangle$.

② Apply $H \otimes H$ $\qquad\qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

③ Apply U_f.

④ Apply $H \otimes \mathbb{1}$

⑤ Measure 1st qubit.



$$|0\rangle|1\rangle \xmapsto{H\otimes H} \frac{1}{2}\sum_{x\in\{0,1\}} |x\rangle \otimes \left(|0\rangle - |1\rangle\right)$$

$$\xmapsto{U_f} \frac{1}{2}\sum_{x\in\{0,1\}} |x\rangle \otimes \underbrace{\left(|f(x)\rangle - |1\oplus f(x)\rangle\right)}_{\begin{cases} f(x)=0 \Rightarrow |0\rangle - |1\rangle \\ f(x)=1 \Rightarrow |1\rangle - |0\rangle \end{cases}}$$

$$= \frac{1}{\sqrt{2}}\sum_{x\in\{0,1\}} (-1)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\underbrace{\qquad\qquad\qquad\qquad}$$

$$\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}$$

$$= (-1)^{f(0)}\left(\frac{|0\rangle + (-1)^{f(0)+f(1)}|1\rangle}{\sqrt{2}}\right)$$

$$\xmapsto{H\otimes \mathbb{1}} (-1)^{f(0)}\,|f(0)+f(1)\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Measmement outputs $f(0)+f(1)$ with certainty!

Today: The power of entanglement.

$|\psi\rangle$ a state on $(n_1 + n_2)$ - qubits.

$$\in (\mathbb{C}^2)^{\otimes n_1} \otimes (\mathbb{C}^2)^{\otimes n_2}.$$

Does $|\psi\rangle$ necessarily equal $\underset{(\mathbb{C}^2)^{\otimes n_1}}{\underset{\cap}{|a\rangle}} \otimes \underset{(\mathbb{C}^2)^{\otimes n_2}}{\underset{\cap}{|b\rangle}}$?

No!

Ex. $$|EPR\rangle = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Pf. $$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}.$$

If $|EPR\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, then

$\alpha \cdot \gamma = \frac{1}{\sqrt{2}} \Rightarrow \alpha \neq 0, \gamma \neq 0.$

$\beta \delta = \frac{1}{\sqrt{2}} \Rightarrow \beta \neq 0, \delta \neq 0.$

So then $\alpha\delta \neq 0$, $\beta\gamma \neq 0$, a contradiction.

<u>A stronger intuition from counting states</u>:

Recall from pset 1 that for any $\epsilon > 0$,

we can find 2^{2^n} n-qubit phase states of which $\exists$ subset of size $2^{(\Omega(\epsilon^2 2^n))}$ which are ϵ-orthogonal.

within a $(2n)$ qubit space there are $2^{(\Omega(\epsilon^2 2^{2n}))}$ such states. How many states are in tensor product?

$$\left[\#\text{ of states of type } |\psi_f\rangle \otimes |\psi_{f'}\rangle\right] = 2^{2^n} \cdot 2^{2^n} = 2^{2^{n+1}}.$$

$$\frac{\#\text{ of tensor product states}}{\text{size of } \epsilon\text{-orthogonal set}} = \frac{2^{2^n+1}}{2^{\Omega(\epsilon^2 2^{2n})}} = 2^{2^n+1-\Omega(\epsilon^2 2^{2n})}$$

$$= 2^{-\Omega(2^n)} \text{ for } \epsilon < 2^{-n/10}.$$

Def. A state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is entangled if $|\psi\rangle$ cannot be expressed as a product state.

What is so special about an entangled state?

Case Study: The EPR states.

What are the only measurements possible?
In standard basis:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \Rightarrow \begin{array}{l} |00\rangle \text{ w pr } \frac{1}{2} \\ |11\rangle \text{ w pr } \frac{1}{2}. \end{array}$$

measure first qubit in $|+\rangle, |-\rangle$ basis.

$$\frac{|+\rangle|+\rangle + |-\rangle|-\rangle}{\sqrt{2}} = \frac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle) + (|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}$$

$$= \frac{2|0\rangle|0\rangle + 0\,|0\rangle|1\rangle + 0\,|1\rangle|0\rangle + 2|1\rangle|1\rangle}{2\sqrt{2}}$$

$$= \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} = |EPR\rangle$$

So $\Pr[\text{measuring } |+\rangle] = \frac{1}{2}$ and resulting state $\propto$

$$(\langle +| \otimes \mathbb{1}) \frac{|+\rangle|+\rangle + |-\rangle|-\rangle}{\sqrt{2}} = \frac{|+\rangle}{\sqrt{2}} + 0 \implies$$ 2^{nd} qubit is then $|+\rangle$.

Likewise, $\Pr[\text{measuring } |-\rangle] = \frac{1}{2}$ and 2^{nd} qubit is then $|-\rangle$.

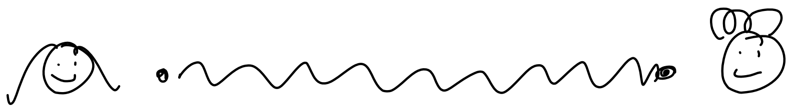
<u>Rmk</u> EPR $\neq$ mixture over $|0,0\rangle$ and $|1,1\rangle$.

<u>Pf.</u> If we measure first qubit of $|00\rangle$ in $|+\rangle, |-\rangle$ basis then $\Pr(X = |+\rangle) = \frac{1}{2}$ but 2^{nd} qubit state is $|0\rangle$. and $\Pr(X = |-\rangle) = \frac{1}{2}$ but 2^{nd} qubit state is $|0\rangle$.

If we measure first qubit of $|11\rangle$ in $|+\rangle, |-\rangle$ basis then $\Pr(X = |+\rangle) = \frac{1}{2}$ but 2^{nd} qubit state is $|1\rangle$ and $\Pr(X = |-\rangle) = \frac{1}{2}$ but 2^{nd} qubit state is $|1\rangle$.

Therefore, x is uniformly random but on outcome $|+\rangle$, 2^{nd} qubit is a prob. mixture over $|0\rangle$ and $|1\rangle$ and not $|+\rangle$. So, we can distinguish $|EPR\rangle$ from $|0,0\rangle$ & $|1,1\rangle$ mixture.

Alice & Bob and EPR

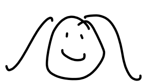


Thm

Alice measures her qubit in basis $|b_0\rangle, |b_1\rangle$. Her measurement will be uniformly random $i \in \{0,1\}$, but Bob's state will be $|b_i\rangle$.

No, this does not allow faster than light communication.

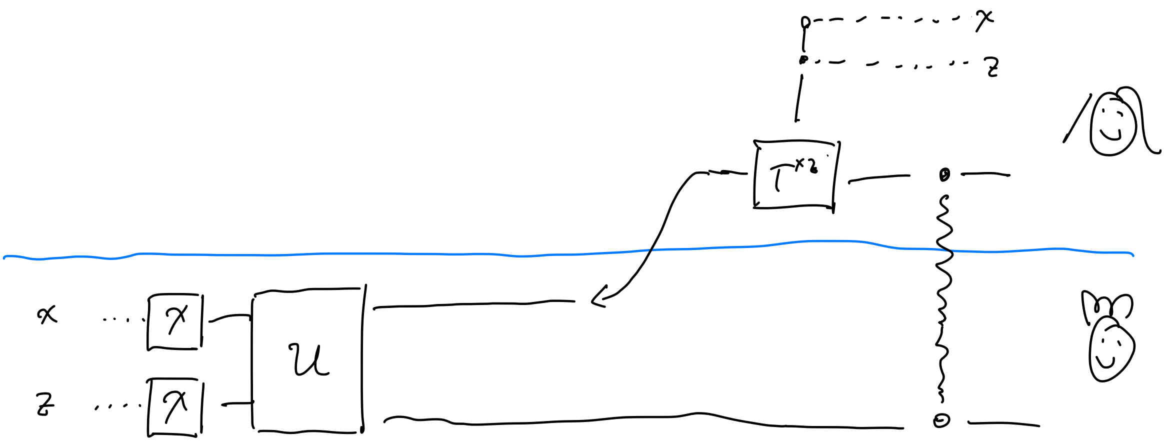
Superdense coding.

 wants to send messages to , who is leaving for a trip far away. Can they save on postage using q.m.?

Classically m bits requires m communication.

Quantum With some preparation, only $m/2$ bits of communication.

2 bits for the price of 1.

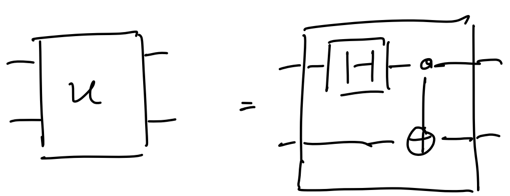


Claim $T^{xz} = X^x Z^z$.

$$|\Phi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\Phi_{01}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Phi_{10}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\Phi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

orthogonal states.



state of Alice & Bob is a 2-qubit state $\in \mathbb{C}^4$.

There are 4 orthogonal states $\in \mathbb{C}^4$.

Alice can switch the global state to any of the 4 of them.

Since they are orthogonal, there exists a distinguishing measurement.

<u>Lesson</u> $|EPR\rangle \neq \underbrace{|+\rangle \otimes |+\rangle}_{\text{unentangled}}$.

$$|EPR\rangle \neq \begin{cases} \frac{1}{2} \text{ prob } |00\rangle \\ \frac{1}{2} \text{ prob } |11\rangle \end{cases}$$ shared randomness.

Dealing with entanglement and randomness at the same time: density matrix.

For a state $|\psi\rangle$, corresponding density matrix is $|\psi\rangle\langle\psi|$.

For a prob mixture p_0 of $|\psi_0\rangle$ and

p_1 of $|\psi_1\rangle$, density matrix

$$\rho = p_0 |\psi_0\rangle\langle\psi_0| + p_1 |\psi_1\rangle\langle\psi_1|.$$

In general $\rho = \sum_a p_a |\psi_a\rangle\langle\psi_a|.$

Properties:

① $tr(\rho) = 1.$

② $\rho = \rho^\dagger$ and $\rho \succeq 0.$

Not:

If $\rho = |\psi\rangle\langle\psi|$ (rank 1) called "pure state" else "mixed state".

Strong converse: given every d.m. ρ, $\exists$ a prob. mixture $\{p_a\}$ and states $\{|\psi_a\rangle\}$ s.t. $\rho = \sum p_a |\psi_a\rangle\langle\psi_a|.$

Pf: eigendecomposition of ρ gives p_a and $|\psi_a\rangle$.

$\sum$ eigenvalues $=$ tr and positivity gives $p_a \geq 0$.

Examples

$$|0\rangle \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad |1\rangle \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|+\rangle \Rightarrow \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad |-\rangle \Rightarrow \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$\text{coin flip} \Rightarrow \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$\text{EPR} \Rightarrow \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{shared randomness} \Rightarrow \frac{1}{2}\begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 1 \end{pmatrix}.$$

$$|+\rangle \otimes |+\rangle \Rightarrow \frac{1}{4}\left(\text{all ones}\right).$$

The <u>derived</u> consequence of q. computation.

① n-qubit state is a density matrix in $\mathcal{L}((\mathbb{C}^2)^{\otimes n})$.

② update by unitary transformations

$$\rho \mapsto \mathcal{U} \rho \mathcal{U}^\dagger$$

(3) measurement of a single qubit:

$$\rho \mapsto (|0\rangle\langle 0| \otimes \mathbb{1}) \rho (|0\rangle\langle 0| \otimes \mathbb{1})$$
$$+ (|1\rangle\langle 1| \otimes \mathbb{1}) \rho (|1\rangle\langle 1| \otimes \mathbb{1})$$

$$\Pr(\text{measuring } 0) = \mathrm{tr}\left(\left[|0\rangle\langle 0| \otimes \mathbb{1}\right] \rho\right)$$

$$\Pr(\text{measuring } 1) = \mathrm{tr}\left(\left[|1\rangle\langle 1| \otimes \mathbb{1}\right] \rho\right).$$

[State conditioned on outcome 0] =

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

In class: verify that this state has trace 1.

(4) If with probability p_a, first state is ρ_a and second state is σ_a, then overall state is

$$\sum p_a \cdot (\rho_a \otimes \sigma_a).$$

Pf that density matrix computations follow from the axioms.

Consider mixture of states $\{|\psi_a\rangle\}$ with prob. p_a s.t. $\sum_a p_a = 1$.

① The corresponding matrix is $\rho = \sum_a p_a |\psi_a\rangle\langle\psi_a|$.

① $\rho \geq 0$ b.c. sum of positive matices.

② $\rho = \rho^\dagger$ b.c. sum of Herm. matrices.

③ $$\begin{aligned} tr(\rho) &= tr\left(\sum_a p_a |\psi_a\rangle\langle\psi_a|\right) \\ &\text{linearity of tr} \\ &= \sum_a p_a \, tr\left(|\psi_a\rangle\langle\psi_a|\right) \\ &\text{cyclicity of tr} \\ &= \sum_a p_a \, tr\left(\langle\psi_a|\psi_a\rangle\right) \\ &= \sum_a p_a = 1. \end{aligned}$$

So ρ is a density matrix.