F, 04/10/2020

Portland State U

S′20 CS 410/510

Intro to quantum computing

Fang Song

Week 2

- Multiple qubits, tensor product
- Quantum circuit model
- Quantum superdense coding
- Quantum teleportation

Credit: based on slides by Richard Cleve

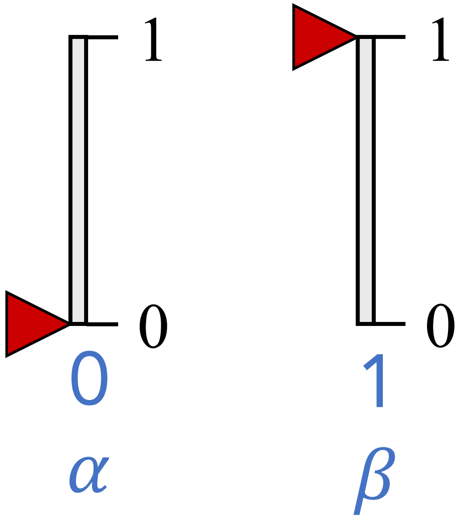
Logistics

- HW1 due Sunday
  - Work in groups, write up individually

- Project
  - Form groups of 2-3 persons by next week

- Workflow
  - Work on pre-class materials: 80% success depends on it!
  - In-class: practice what you studied and extend to new topics
  - Post-class: review and reinforce

Review: qubit



Superposition

- Amplitudes $\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$
- Explicit state is $\binom{\alpha}{\beta} \in \mathbb{C}^2$
  (2-norm / Euclidean norm = 1)

- *Cannot* explicitly extract α and β
  (only statistical inference)

Dirac bra/ket notation

- **Ket:** $|\psi\rangle$ always denotes a column vector

  Convention: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

  Ex. $|\psi\rangle = \begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_d\end{pmatrix}$

- **Bra:** $\langle\psi|$ always denotes a row vector that is the conjugate transpose of $|\psi\rangle$

  Ex. $\langle\psi| = (\alpha_1^*, \alpha_2^*, \dots, \alpha_d^*)$

- **Inner product:** $\langle\psi|\phi\rangle$ denotes $\langle\psi| \cdot |\phi\rangle$
  - Vectors to scalar

  Ex. $\langle 0|1\rangle = (1\ \ 0)\begin{pmatrix}0\\1\end{pmatrix} = 0$

- **Outer product:** $|\psi\rangle\langle\phi|$ denotes $|\psi\rangle \cdot \langle\phi|$
  - Vectors to matrix

  Ex. $|0\rangle\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}(0\ \ 1) = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$

Basic operations on a qubit

0. Initialize qubit to $|0\rangle$ or to $|1\rangle$
1. Apply a unitary operation U ($U^\dagger U = I$)

Linear map A ↔ matrix A
Apply A to $|\psi\rangle$ ↔ matrix mult. $A|\psi\rangle$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle$$

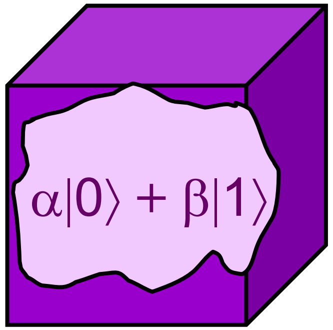
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H|0\rangle = |+\rangle, H|1\rangle = |-\rangle$$

Basic operations on a qubit

0. Initialize qubit to $|0\rangle$ or to $|1\rangle$

1. Apply a unitary operation U $(U^\dagger U = I)$

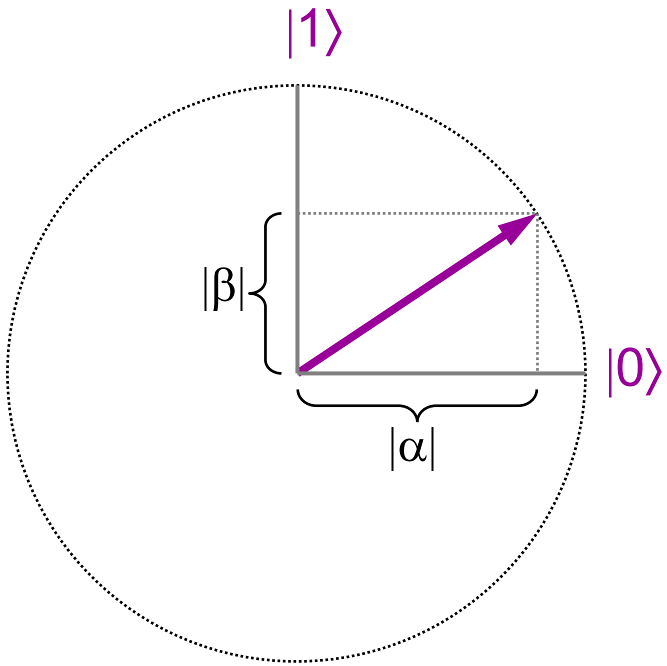
2. Perform a "standard" measurement:



$$\mapsto \begin{cases} 0 \text{ with prob } |\alpha|^2 \\ 1 \text{ with prob } |\beta|^2 \end{cases}$$

	posterior state
0 with prob $|\alpha|^2$	$|0\rangle$
1 with prob $|\beta|^2$	$|1\rangle$

… and the quantum state collapses



N.B. There exist other quantum operations, but they can all be "simulated" by the aforementioned types

A few tips

- Linearity. Let A be a linear map. Any $v_i \in \mathbb{C}^d, c_i \in C, i = 1, \dots, k$

$$A\left(\sum_i c_i \cdot v_i\right) = \sum_i c_i \cdot A(v_i)$$

→ A is uniquely determined by its action on a basis

  - Let $u_1, \dots, u_d \in \mathbb{C}^d$ be a basis → $\forall\, v \in \mathbb{C}^d$ can be expressed by $v = \sum_i c_i u_i$
  - Given $A(u_i) = w_i, i = 1, \dots, d$ → $Av = A(\sum_i c_i u_i) = \sum_i c_i A(u_i) = \sum_i c_i w_i$

- When Dirac notation unclear, convert to vectors/matrices

- When Dirac notation unclear, convert to vectors/matrices

Two qubits: composed system

$$\alpha|0\rangle + \beta|1\rangle \otimes \alpha'|0\rangle + \beta'|1\rangle = \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

- Tensor product $\otimes$

$$[A]_{m\times n} \otimes [B]_{k\times \ell} = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \cdots & \cdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}_{mk\times n\ell}$$

Two qubits: composed system

$$[A]_{m\times n} \otimes [B]_{k\times\ell} = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \dots & \dots \\ a_{m1}B & a_{m2}B & & a_{mn}B \end{pmatrix}_{mk\times n\ell}$$

Ex. $|00\rangle := |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix} 1\cdot\begin{pmatrix}1\\0\end{pmatrix} \\ 0\cdot\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$

$|01\rangle = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

$|\psi\rangle|\phi\rangle := |\psi\rangle \otimes |\phi\rangle$

General n-qubit systems

- **Probabilistic states**

$$\forall x \in \{0,1\}^n, p_x \geq 0$$

$$\sum_x p_x = 1$$

$$\begin{pmatrix} p_{000} \\ p_{001} \\ p_{010} \\ p_{011} \\ p_{100} \\ p_{101} \\ p_{110} \\ p_{111} \end{pmatrix}$$

- **Quantum states**

$$\forall x \in \{0,1\}^n, \alpha_x \in \mathbb{C}$$

$$\sum_x |\alpha_x|^2 = 1$$

$$\begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

Dirac notation: $|000\rangle, |001\rangle, |010\rangle, \dots, |111\rangle$ are basis vectors

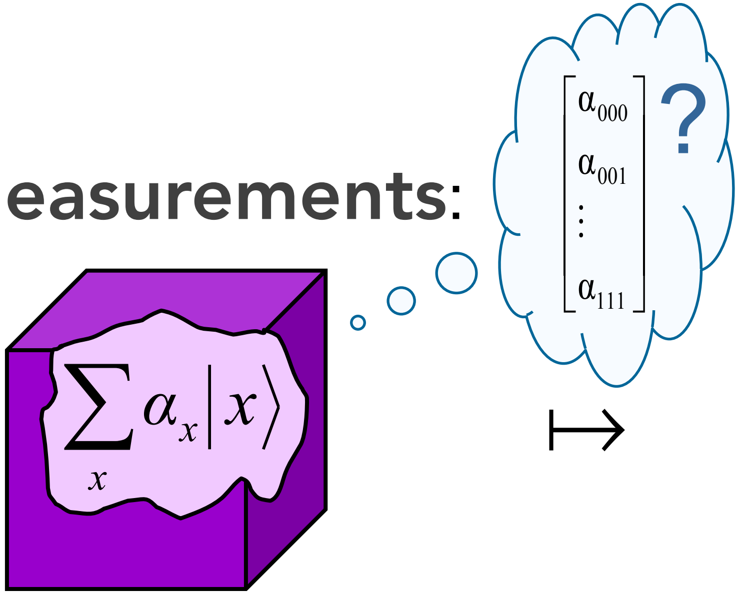
➔ Any state can be written as $|\psi\rangle = \sum_x \alpha_x |x\rangle$

Operations on n-qubit states

- **Unitary operations:** $\sum_x \alpha_x |x\rangle \mapsto U\left(\sum_x \alpha_x |x\rangle\right)$

  $(U^\dagger U = I)$

- **Measurements:**



$\mapsto$

		posterior state
000	with prob $\lvert\alpha_{000}\rvert^2$	$\lvert 000\rangle$
001	with prob $\lvert\alpha_{001}\rvert^2$	$\lvert 001\rangle$
$\vdots$	$\vdots$	$\vdots$
111	with prob $\lvert\alpha_{111}\rvert^2$	$\lvert 111\rangle$

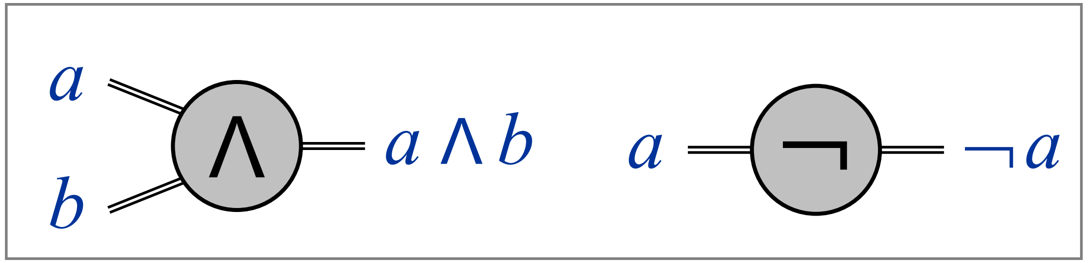
… and the quantum state collapses

Model of computation

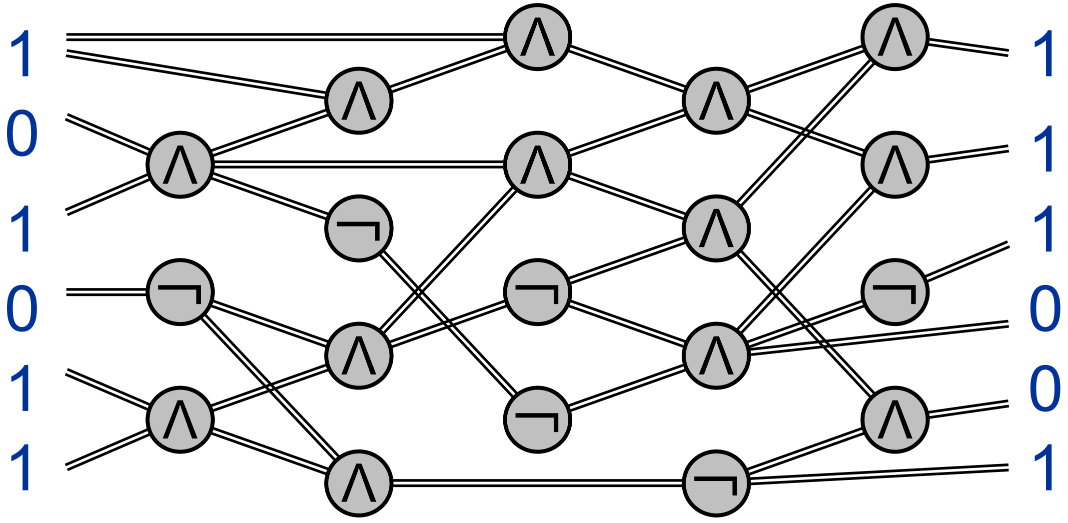
Classical Boolean circuits

Bit 0/1

Data flow



Classical circuits:



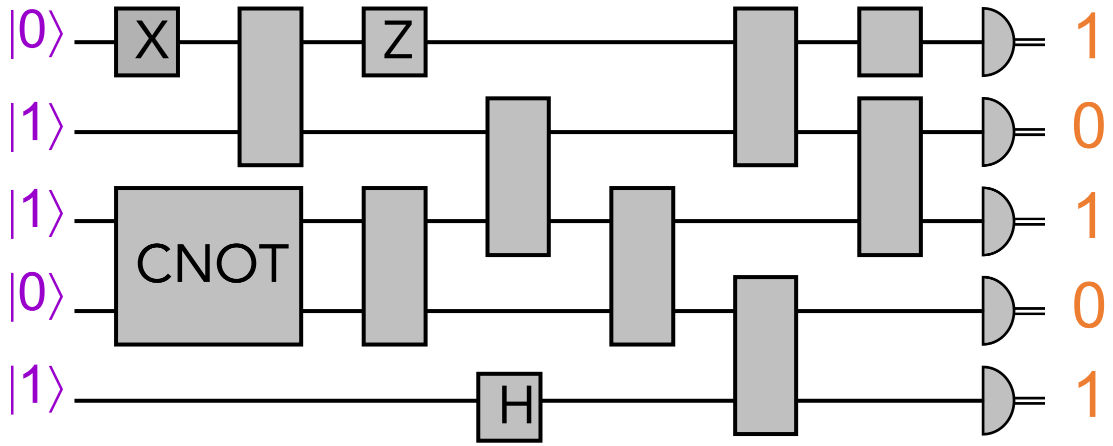
Quantum circuit model

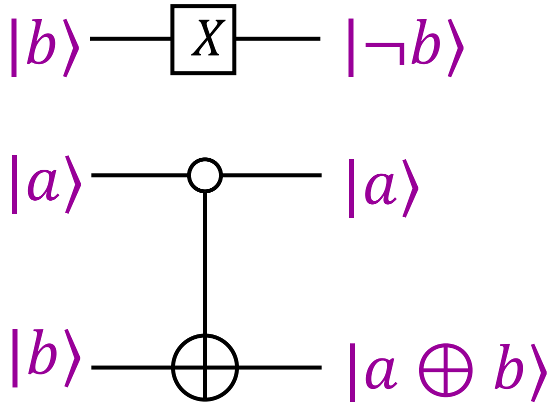
Qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

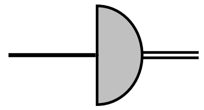
Data flow →

Quantum circuits:





$$|a\rangle|b\rangle \mapsto |a\rangle|a \oplus b\rangle$$



(standard) Measure

The power of computation

- Computability: can you solve it, in principle?

[Given program code, will this program terminate or loop indefinitely?]

Uncomputable!

Church-Turing Thesis. A problem can be computed in any ***reasonable*** model of computation iff. it is computable by a **Boolean circuit**.

- Complexity: can you solve it, under resource constraints?

[Can you factor a 1024-bit integer in 3 seconds?]

Extended Church-Turing Thesis. A function can be computed efficiently in any *reasonable* model of computation iff. it is efficiently computable by a **Boolean circuit**.

✓ Quantum computer — Disprove ECTT?

Product state vs. entangled state

- Product state $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$

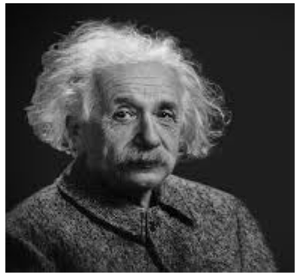
$$|\psi\rangle_{AB} = \alpha|0\rangle + \beta|1\rangle \otimes \alpha'|0\rangle + \beta'|1\rangle$$

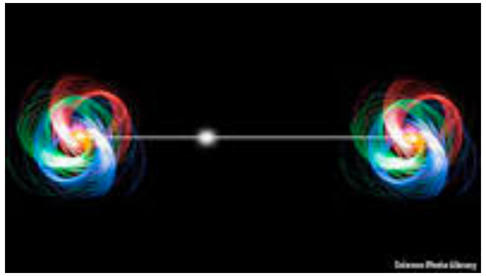
- $|\psi\rangle_{AB}$ an arbitrary 2-qubit state:
  Can we always write it as $|\psi\rangle_A \otimes |\psi\rangle_B$ for some $|\psi\rangle_{\mathrm{A}}$ and $|\phi\rangle_B$?

Product state vs. entangled state

- Entangled state: $|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$ for any $|\psi\rangle_{\mathrm{A}}$ and $|\phi\rangle_B$

Ex. $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ EPR (Einstein–Podolsky–Rosen) pair





- Mathematically, not surprising: A & B correlated
- Physically, non-classical correlation, "spooky" action at a distance

- Cor. need to speak of state of entire system than individuals

Exercise: correlation & entanglement

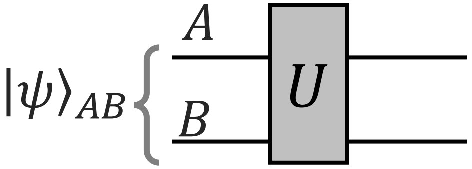
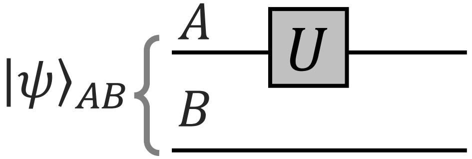
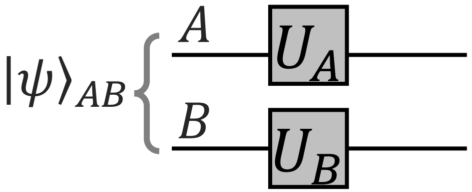
1. Consider two bits $a\&b$ whose joint state (i.e., prob. distribution) is described by probabilistic vector $v = \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix}$.
   - What is the probability that $ab = 11$?
   - Does there exist two-dimensional probabilistic vectors u_A and u_B such that $v = u_A \otimes u_B$?

Exercise: correlation & entanglement

2. Prove that the EPR state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be written as $|\psi\rangle \otimes |\phi\rangle$ for any choice of $|\psi\rangle, |\phi\rangle \in \mathbb{C}^2$.

Two-qubit gates

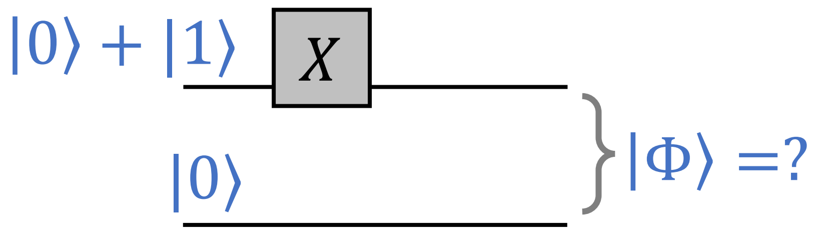
Given two qubits in state $|\psi\rangle_{AB}$

Description	Algebra	Circuit
Apply unitary U to $|\psi\rangle_{AB}$	$U|\psi\rangle_{AB}$	
Apply unitary U to qubit A	$U \otimes I|\psi\rangle_{AB}$	
Apply unitary U_A to qubit A & unitary U_B to qubit B	$U_A \otimes U_B|\psi\rangle_{AB}$	

- Facts
  - Given unitary U, V, $U \otimes V$ is also unitary.
  - $(U \otimes V)(A \otimes B) = UA \otimes VB$

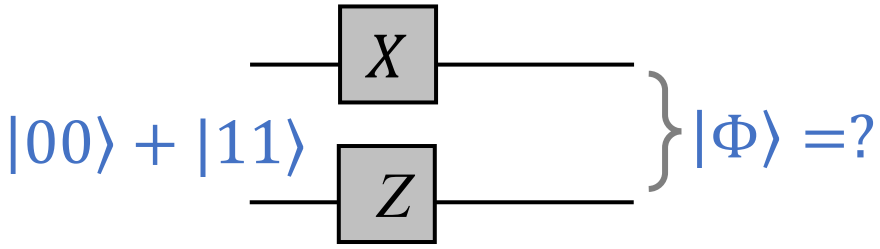
Exercise: two-qubit gates

1



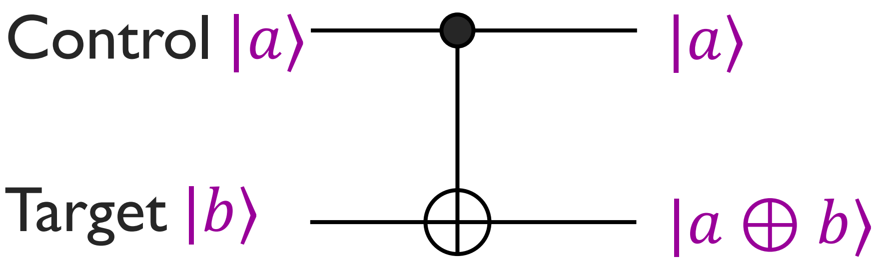
i.e. $|\Phi\rangle = X \otimes I((|0\rangle + |1\rangle)_A \otimes |0\rangle_B)$
$=?$

2



i.e. $|\Phi\rangle = X \otimes Z(|00\rangle + |11\rangle)$
$=?$

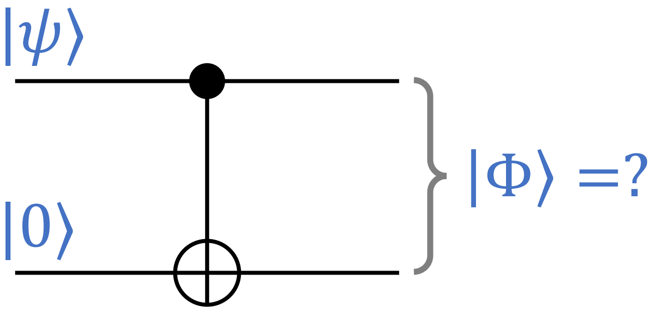
Exercise: CNOT



$$\text{CNOT}: |00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |00\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

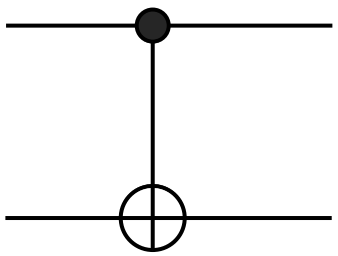
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

1



$\vert\psi\rangle$	$\vert\Phi\rangle$
$\vert 0\rangle + \vert 1\rangle$	?
$\vert 0\rangle - \vert 1\rangle$	?

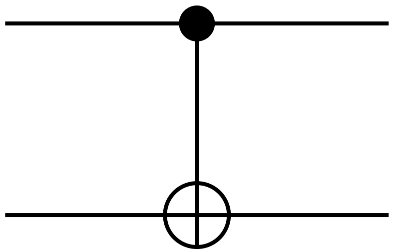
Exercise: CNOT



$$\text{CNOT}: |00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |00\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

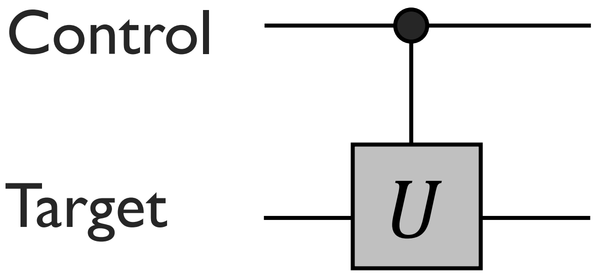
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2



N.B. "control" qubit may change on some input state

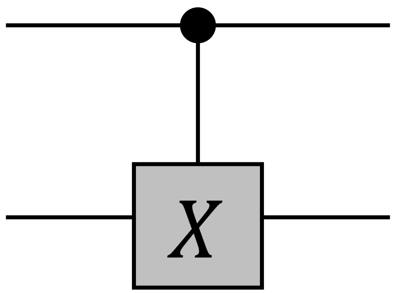
Exercise: controlled unitary



$$C\!-\!U: \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |00\rangle \\ |10\rangle \mapsto |1\rangle U|0\rangle \\ |11\rangle \mapsto |1\rangle U|1\rangle \end{array}$$

$$C\!-\!U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

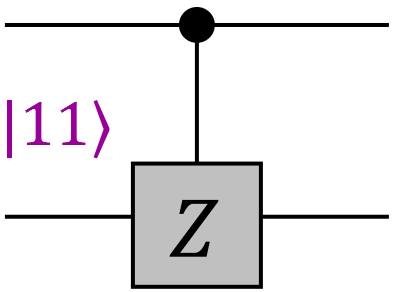
1



$\equiv ?$

2

$|00\rangle + |11\rangle$



$= ?$

Apps of Entanglement

1. Superdense coding

How much classical information in n qubits?

- $2^n - 1$ complex numbers apparently needed to describe an arbitrary n-qubit state:

  $\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \ldots + \alpha_{111}|111\rangle$

- Does this mean that an exponential amount of classical information is somehow "stored" in n qubits?

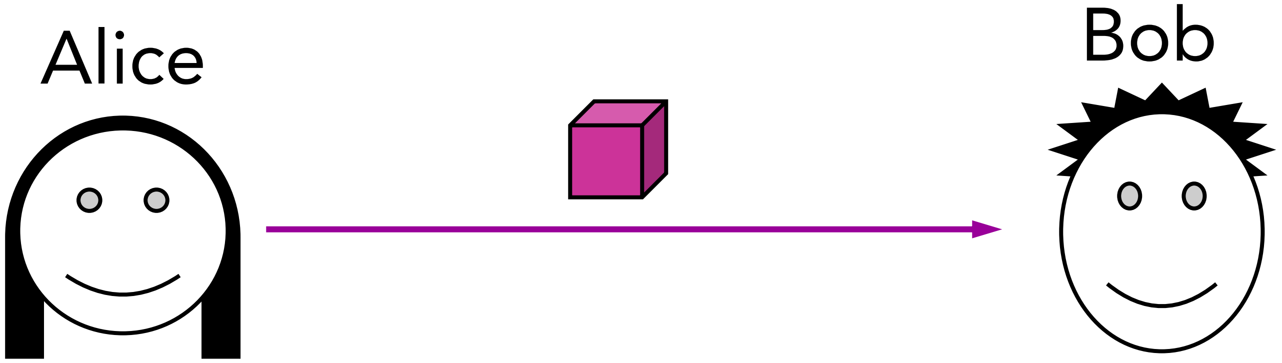
  Not in an operational sense ...

  Holevo's Theorem (from 1973) implies: one cannot convey more than n classical bits of information in n qubits

Superdense coding (prelude)

Goal: Alice wants to convey ***two*** classical bits to Bob sending just ***one*** qubit

$a, b \leftarrow \{0,1\}$



$ab?$

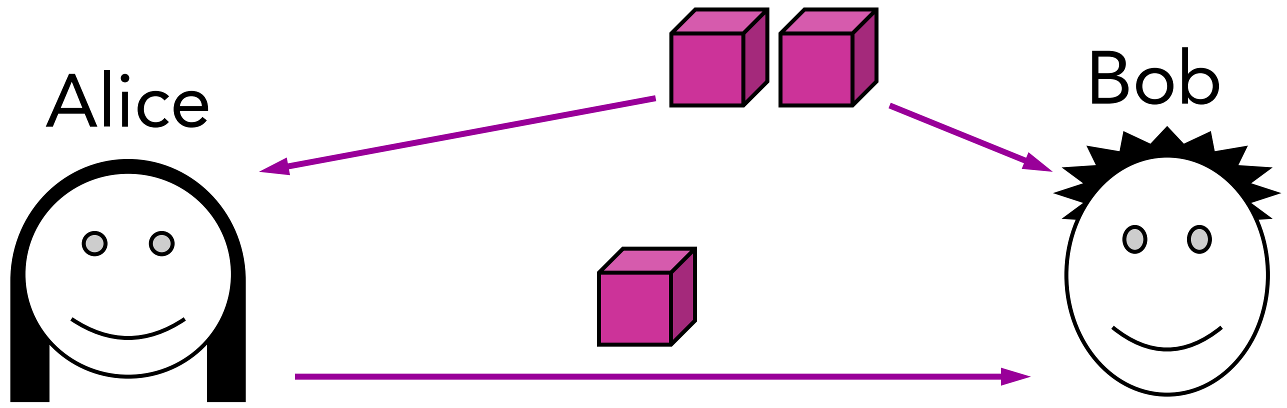
By Holevo's Theorem, this is **impossible!**

Superdense coding with shared EPR

Yes, if they pre-share EPR!

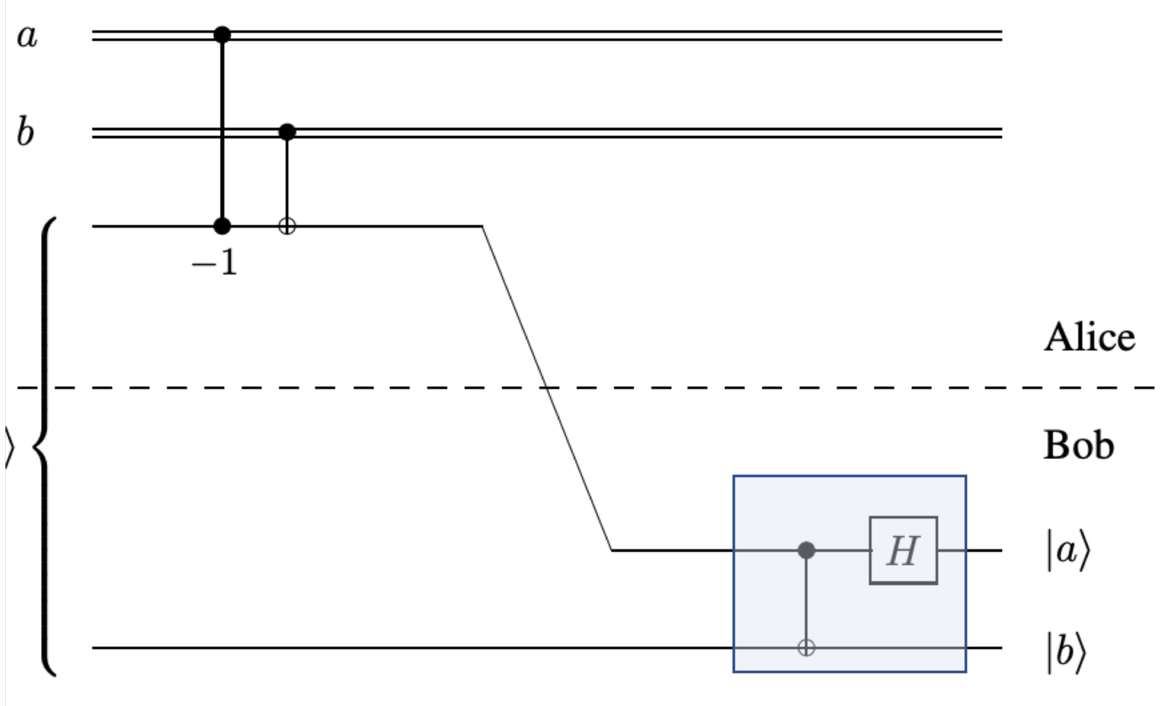
$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$a, b \leftarrow \{0,1\}$



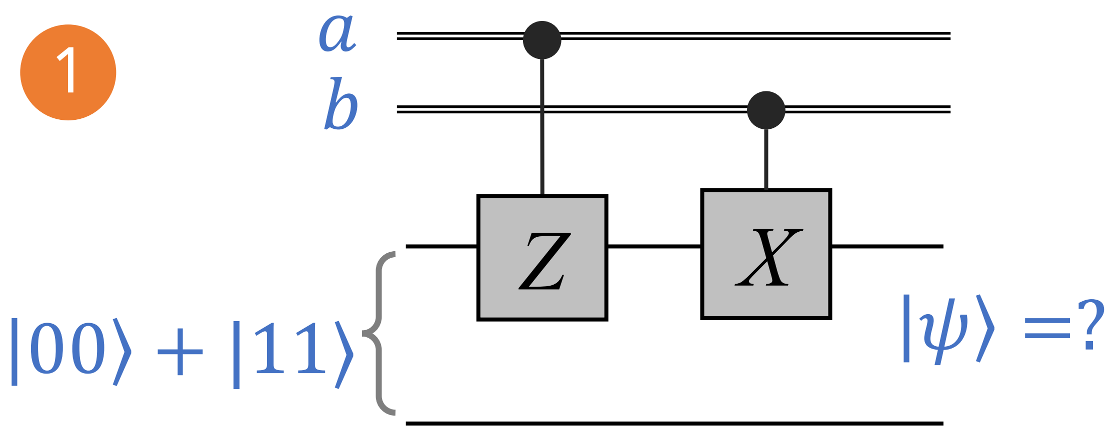
✓ ab

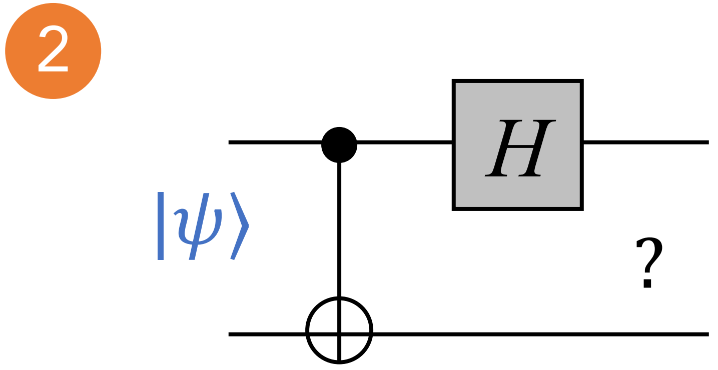
Superdense coding protocol

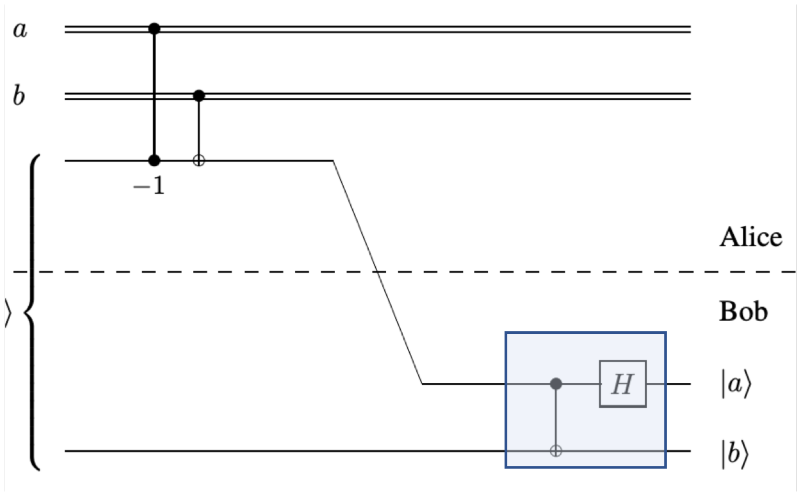


1. Bob: create $|00\rangle + |11\rangle$ and send the first qubit to Alice
2. Alice:
   - if $a = 1$ then apply Z to qubit
   - if $b = 1$ then apply X to qubit
   - send the qubit back to Bob
3. Bob: apply the "gadget" and measure the two qubits

Analysis







ab	$\vert\psi\rangle$
00	?
01	?
10	?
11	?

Input	Output
$\vert 00\rangle + \vert 11\rangle$	?
$\vert 01\rangle + \vert 10\rangle$	?
$\vert 00\rangle - \vert 11\rangle$	?
$\vert 01\rangle - \vert 10\rangle$	?

Bell states

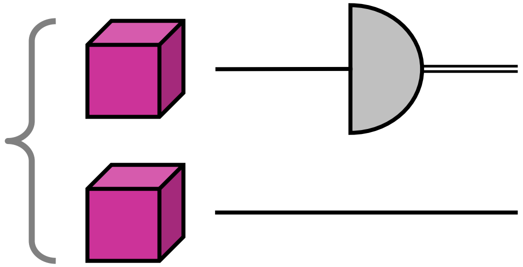
Apps of Entanglement

2. Quantum teleportation

Partial measurement

- Measuring the first qubit of a two-qubit system

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$



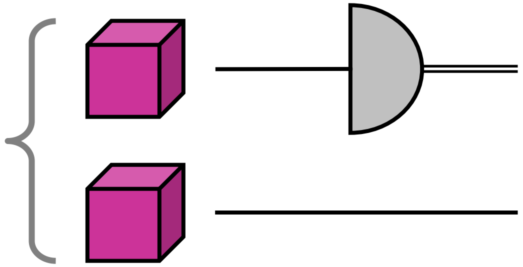
- Result

See	With probability	posterior state (renormalized!)
0	$p_0 := \lvert\alpha_{00}\rvert^2 + \lvert\alpha_{01}\rvert^2$	$\frac{\alpha_{00}\lvert 00\rangle + \alpha_{01}\lvert 01\rangle}{\sqrt{\lvert\alpha_{00}\rvert^2 + \lvert\alpha_{01}\rvert^2}}$
1	$p_1 := \lvert\alpha_{10}\rvert^2 + \lvert\alpha_{11}\rvert^2$	$\frac{\alpha_{10}\lvert 10\rangle + \alpha_{11}\lvert 11\rangle}{\sqrt{\lvert\alpha_{10}\rvert^2 + \lvert\alpha_{11}\rvert^2}}$

Partial measurement: Exercise

- Measuring the first qubit of a two-qubit system

$$|\psi\rangle = \frac{1}{2}|00\rangle - \frac{i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

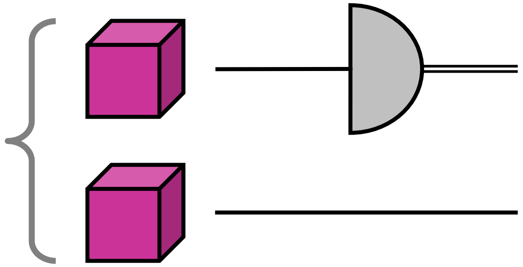


See	With probability	posterior state (renormalized!)
0		
1		

Partial measurement: Exercise

- Measuring the first qubit of a two-qubit system

$$|\psi\rangle = \frac{1}{2}|00\rangle - \frac{i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$



- A trick

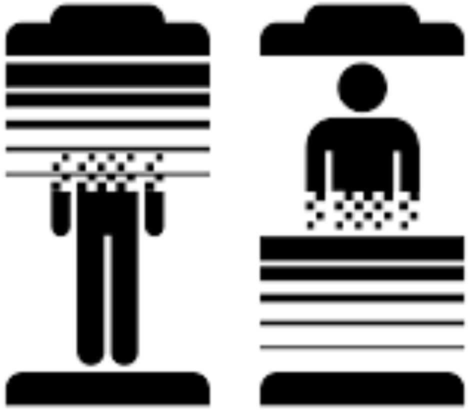
See	With probability	posterior state (renormalized!)
0 1		

Transmitting qubits by classical bits

Goal: Alice conveys a qubit to Bob by sending just classical bits

- If Alice knows $\alpha, \beta \in \mathbb{C}$, requires infinitely many bits for perfect precision
- If Alice doesn't know α or β, she can at best acquire one bit by measurement

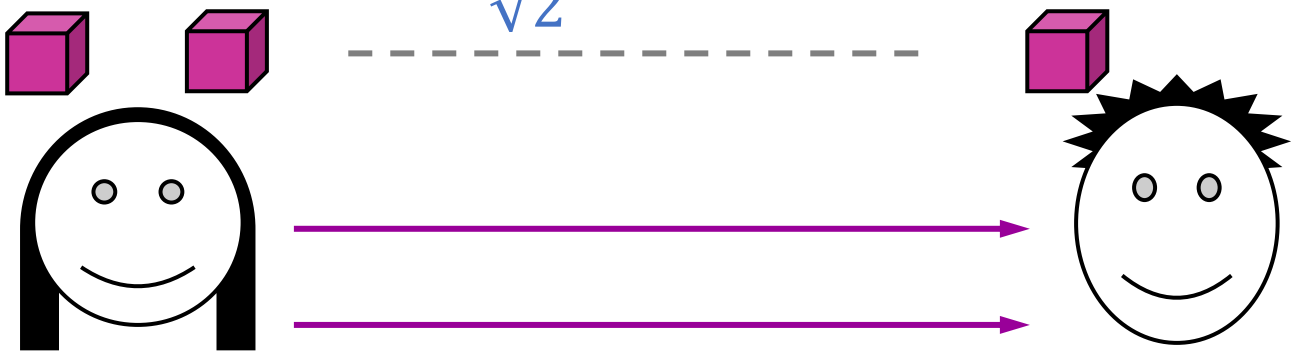
Teleportation



Theorem. two classical bit enough if pre-share EPR

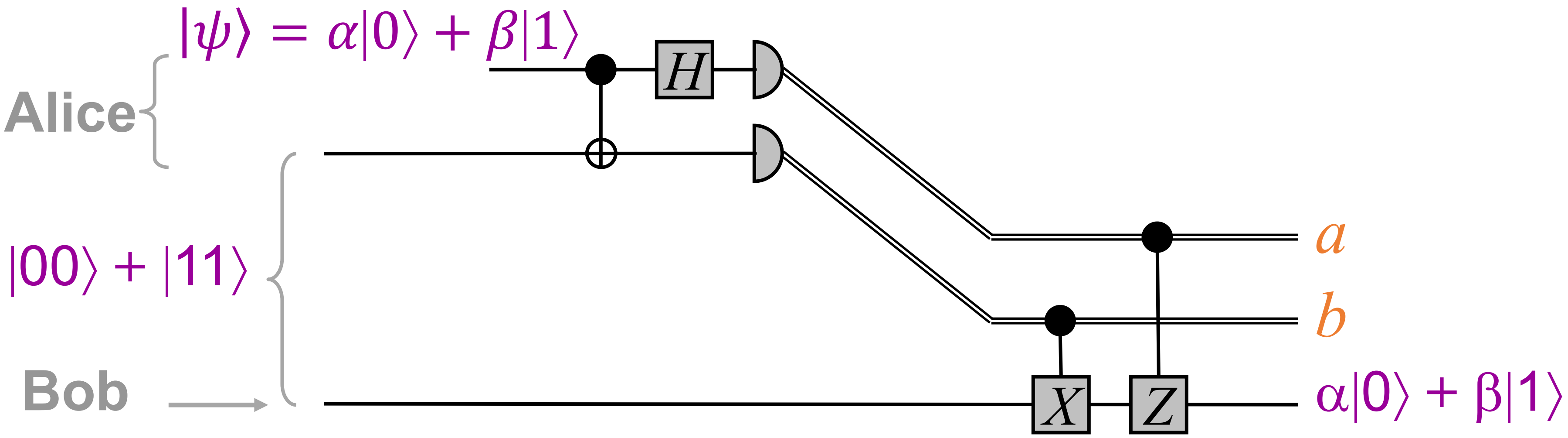
$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\alpha|0\rangle + \beta|1\rangle$$



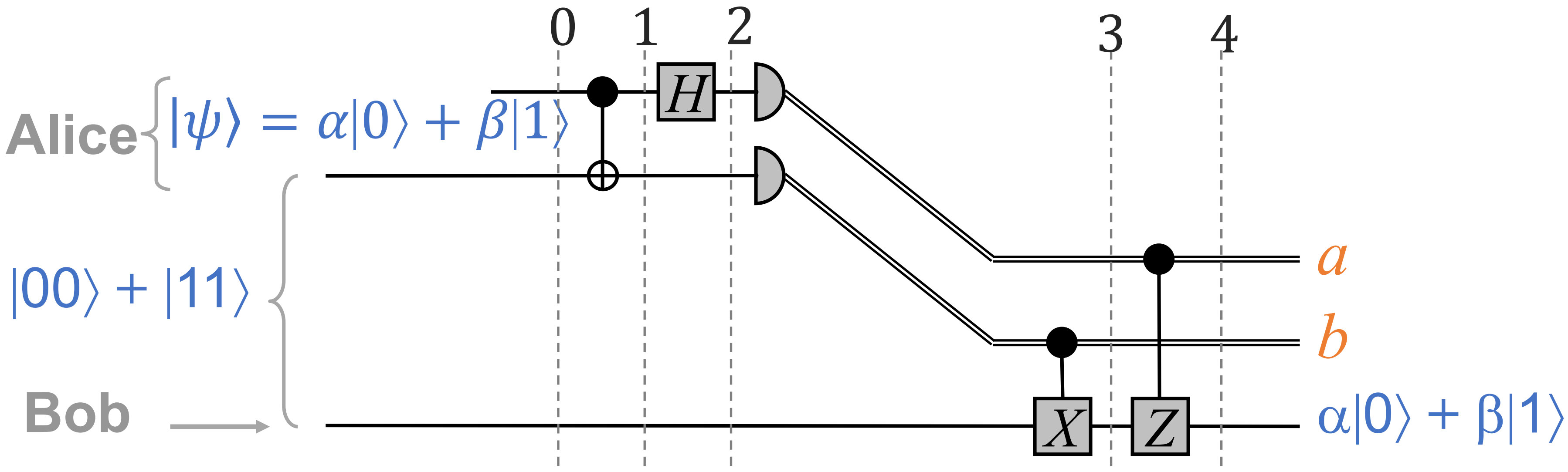
Teleportation: protocol

Theorem. two classical bit enough if pre-share EPR



- Does Alice still hold $|\psi\rangle$ at the end?
- Communicating faster than the speed of light?

Teleportation: analysis



Questions?

- Use zoom chat and campuswire DM/chatroom to mingle and identify potential group members
- Ask me if you want a Zoom breakout room

Scratch