#### F, 04/10/2020



## Week 2

#### S'20 CS 410/510

## Intro to quantum computing

Fang Song

#### 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

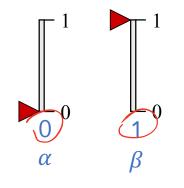
Project

• 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  $\alpha$  and  $\beta$ 
  - (only statistical inference)

• Ket:  $|\psi\rangle$  always denotes a c

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

- Bra:  $\langle \psi |$  always denotes a row vector that the conjugate transpose of  $|\psi\rangle$
- Inner product:  $\langle \psi | \phi \rangle$  denotes  $\langle \psi | \cdot | \phi \rangle$ 
  - Vectors to scalar
- Outer product:  $|\psi\rangle\langle\phi|$  denotes  $|\psi\rangle\cdot\langle\phi|$ 
  - Vectors to matrix

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

$$\mathsf{E}_{\mathsf{X}} \langle \psi | = (\alpha_1^*, \alpha_2^*, \dots, \alpha_d^*)$$

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

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

is 
$$E_{x}(\psi) = (\alpha_{1}^{*}, \alpha_{2}^{*}, ..., \alpha_{d}^{*})$$

**Dirac bra/ket notation** 

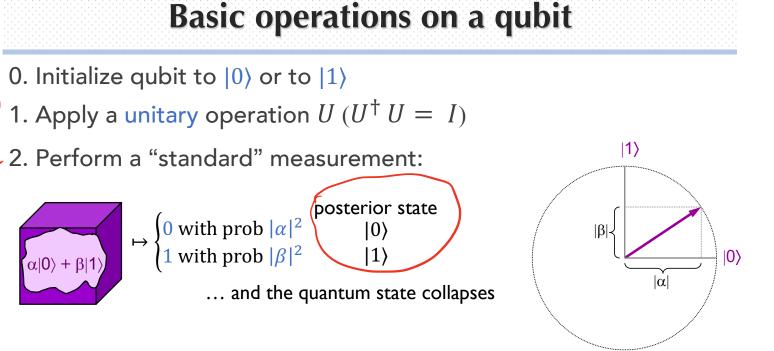
## **Basic operations on a qubit**

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

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

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

Linear map 
$$A \leftrightarrow \text{matrix } A$$
  
Apply  $A$  to  $|\psi\rangle \leftrightarrow \text{matrix mult. } A|\psi\rangle$ 



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, ..., k

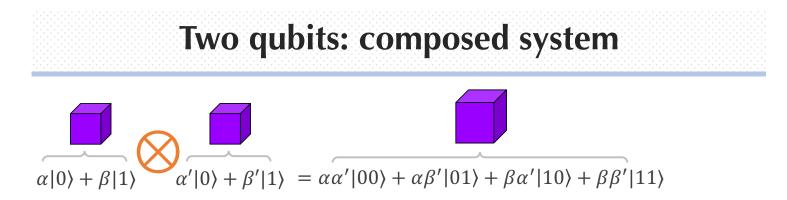
$$A\left(\sum_{i}c_{i}\cdot v_{i}\right) = \sum_{i}c_{i}\cdot A(v_{i})$$

 $\rightarrow$  A is uniquely determined by its action on a basis

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

When Dirac notation unclear, convert to vectors/matrices

When Dirac notation unclear, convert to vectors/matrices



#### • Tensor product $\otimes$

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

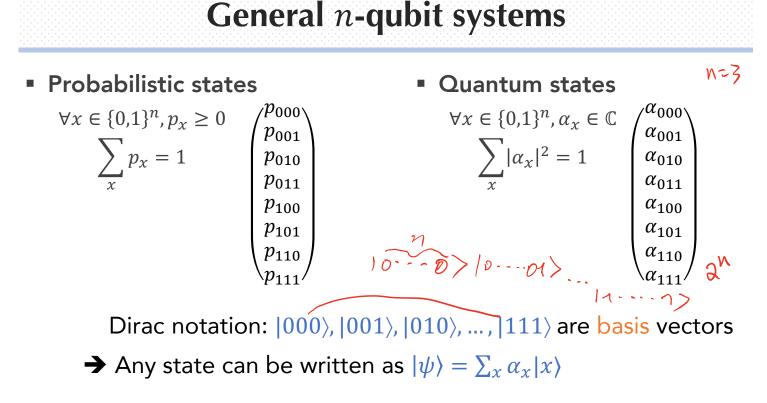
$$[A]_{m \times n} \otimes [B]_{k \times \ell} = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \dots & \dots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}_{mk \times n\ell}$$

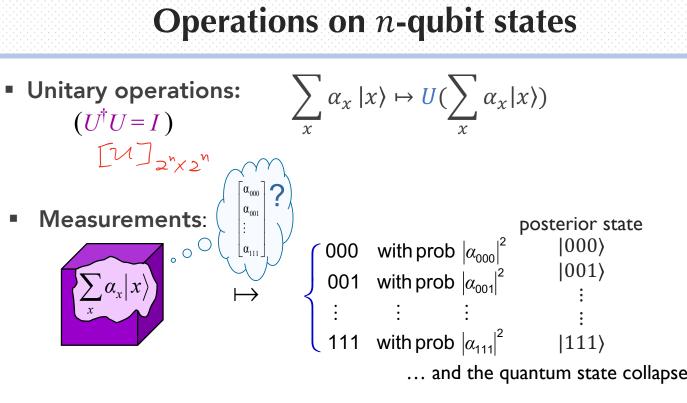
**Two qubits: composed system** 

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

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

 $|\psi\rangle|\phi\rangle\coloneqq|\psi\rangle\otimes|\phi
angle$ 

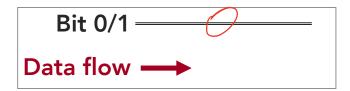




... and the quantum state collapses

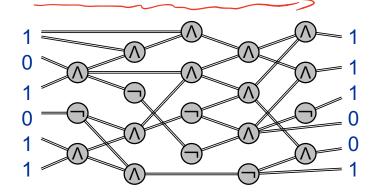
# **Model of computation**

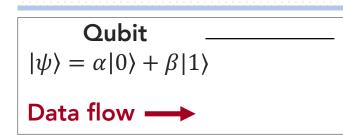
## **Classical Boolean circuits**



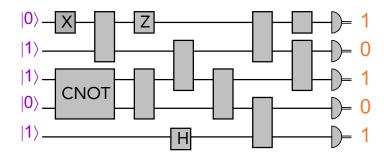


#### **Classical circuits:**

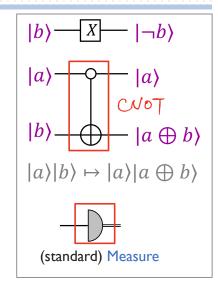




#### Quantum circuits:



Quantum circuit model



## 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 $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$

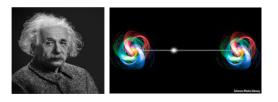
$$|\psi\rangle_{AB} = \alpha |0\rangle + \beta |1\rangle \bigotimes \alpha' |0\rangle + \beta' |1\rangle$$

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

**Product state vs. entangled state** 

## • Entangled state: $|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$ for any $|\psi\rangle_A$ and $|\phi\rangle_B$ Ex. $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ EPR (Einstein–Podolsky–Rosen) pair

**Product state vs. entangled state** 



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

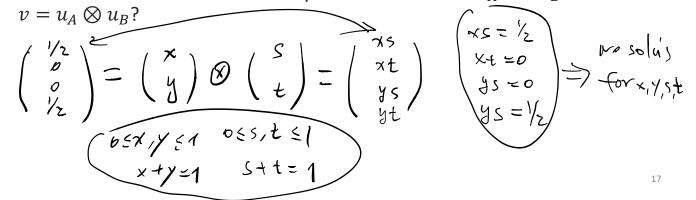
Cor. need to speak of state of entire system than individuals

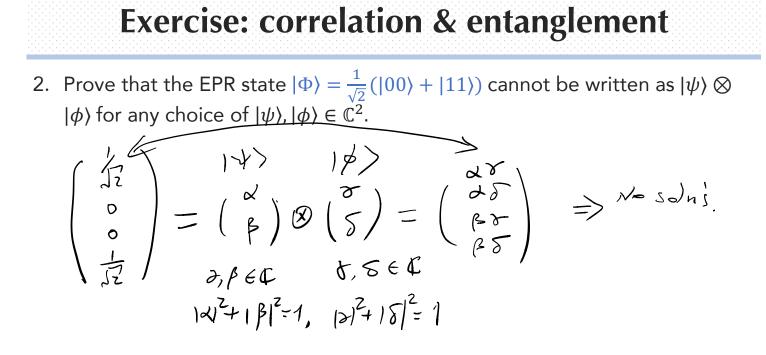
## **Exercise: correlation & entanglement**

1. Consider two bits a&b whose joint state (i.e., prob. distribution) is

described by probabilistic vector  $v = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ .  $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ 

- What is the probability that ab = 11?  $P_r(ab = 11) = \frac{1}{2}$
- Does there exist two-dimensional probabilistic vectors  $u_A$  and  $u_B$  such that





## **Two-qubit gates**

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

Description	Algebra	Circuit
Apply unitary $U$ to $ \psi angle_{AB}$	$U \psi angle_{AB}$	$ \psi\rangle_{AB} \left\{ \begin{array}{c} A \\ \underline{B} \end{array} \right\} U$
Apply unitary <i>U</i> to qubit <i>A</i>	$U \otimes I  \psi\rangle_{AB}$	$ \psi\rangle_{AB} \left\{ \begin{array}{c} \underline{A} & \underline{U} \\ \underline{B} \end{array} \right\}$
Apply unitary $U_A$ to qubit $A$ & unitary $U_B$ to qubit $B$	$U_A \otimes U_B  \psi\rangle_{AB}$	$ \psi\rangle_{AB} \left\{ \begin{array}{c} A & U_A \\ \hline B & U_B \end{array} \right\}$

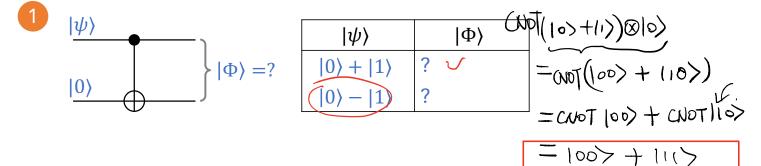
#### Facts

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

**Exercise: two-qubit gates** 2  $|\Phi\rangle = ?$  $|00\rangle + |11\rangle$ i.e.  $|\Phi\rangle = X \otimes I((|0\rangle + |1\rangle)_A \otimes |0\rangle_B)$ i.e.  $|\Phi\rangle = X \otimes Z(|00\rangle + |11\rangle)$  $=? \times @ Z (00 > + \times @ Z ||) >$  $\otimes (I | 0 \rangle_{\rm S} \rangle$  $\left(X\left(10\right)+11\right)_{A}$  $= (\chi_{0}) \otimes (\chi_{0}) + (\chi_{1}) \otimes (\chi_{1})$  $= (\chi | 0 > + \chi | 1 >)_{A} \otimes | 0 > B$   $= (11 > + (0))_{A} \otimes | 0 > B$  $= 11 \otimes 10 + 10 \otimes (-11)$ 107B = 1107 - 101> 20

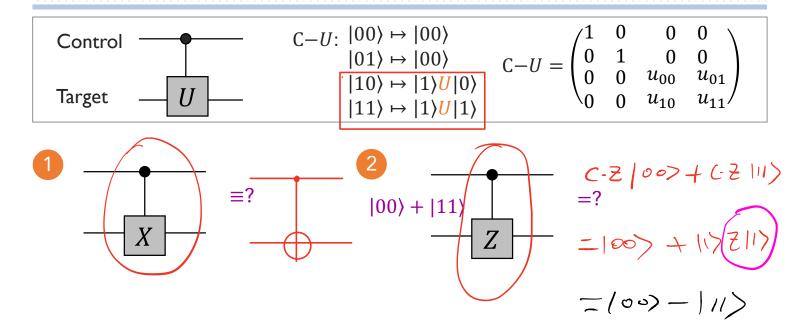
Control 
$$|a\rangle$$
 $|a\rangle$ 
 CNOT:  $|00\rangle \mapsto |00\rangle$ 

 Target  $|b\rangle$ 
 $|a \oplus b\rangle$ 
 $CNOT: |00\rangle \mapsto |00\rangle$ 
 $|01\rangle \mapsto |0\rangle\rangle$ 
 $|10\rangle \mapsto |11\rangle$ 
 $|10\rangle \mapsto |11\rangle$ 
 $|11\rangle \mapsto |10\rangle$ 



#### **Exercise: CNOT** $CNOT:|00\rangle \mapsto |00\rangle$ $\begin{array}{c} |01\rangle \mapsto |00\rangle \\ |10\rangle \mapsto |11\rangle \end{array} \quad \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ Control $|a\rangle$ $|a\rangle$ Target $|b\rangle$ $|a \oplus b\rangle$ $|11\rangle \mapsto |10\rangle$ $(10)+11)\otimes(10)-11)$ $|0\rangle + |1\rangle$ 2 = 10>10>+10>(-11>) + 11>10> + 11>/-11>) = 1007-1017+1107-1117 $|0\rangle - |1\rangle$ CNOT: 5 7. $\rightarrow 100 - 101 + 111 - 110 = (10) - 10)$ **N.B.** "control" qubit may change on some input state $= \frac{10}{(10) - 10} + \frac{10}{(10) - 10} + \frac{10}{(10) - 10}$ 22

## **Exercise: controlled unitary**



## **Apps of Entanglement**

# 1. Superdense coding

# How much classical information in n qubits?

 2<sup>n</sup>-1 complex numbers apparently needed to describe an arbitrary *n*-qubit state:

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

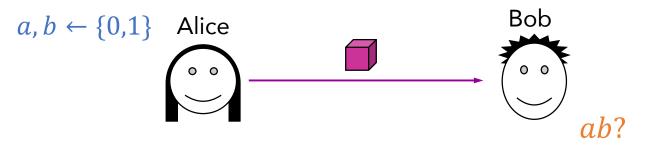
Does this mean that an exponential amount of classical information is somehow "stored" in n qubits?

#### Not in an operational sense ...

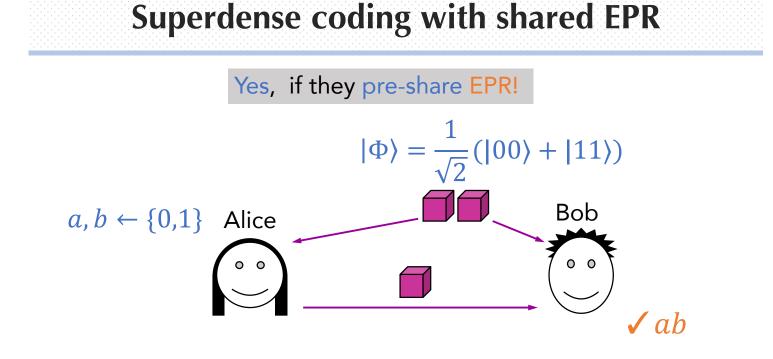
Holevo's Theorem (from 1973) implies: one cannot convey more than n classical bits of information in n qubits

## Superdense coding (prelude)

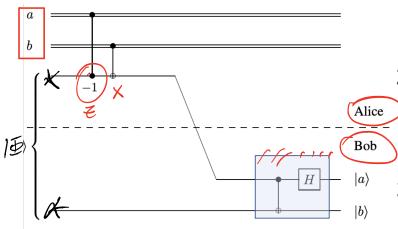
Goal: Alice wants to convey *two* classical bits to Bob sending just *one* qubit



By Holevo's Theorem, this is impossible!



## **Superdense coding protocol**

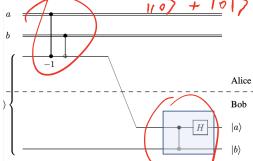


1. Bob: create  $|00\rangle + |11\rangle$  and send the first qubit to Alice

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 a 0 H $|\psi|$ 7 ? L $|\psi\rangle = ?$ 07



	ab	$ \psi angle$	
	00	?100>+111>	
-	<b>→</b> 01	? 110>+101>	N
	10	? 100>-111>	$\leq$
	11	? 1107 -101)	

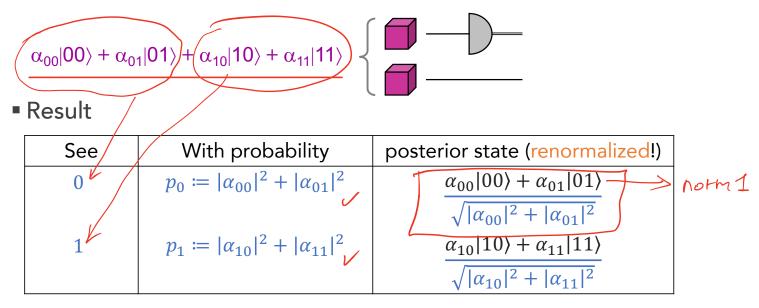
	Input	Output
	$ 00\rangle +  11\rangle$	? (00>
>	01 angle+ 10 angle	? 01>
	00 angle -  11 angle	? (10)
	01 angle -  10 angle .	2>1117

**Bell states** 

## **Apps of Entanglement**

# 2. Quantum teleportation

## Measuring the first qubit of a two-qubit system

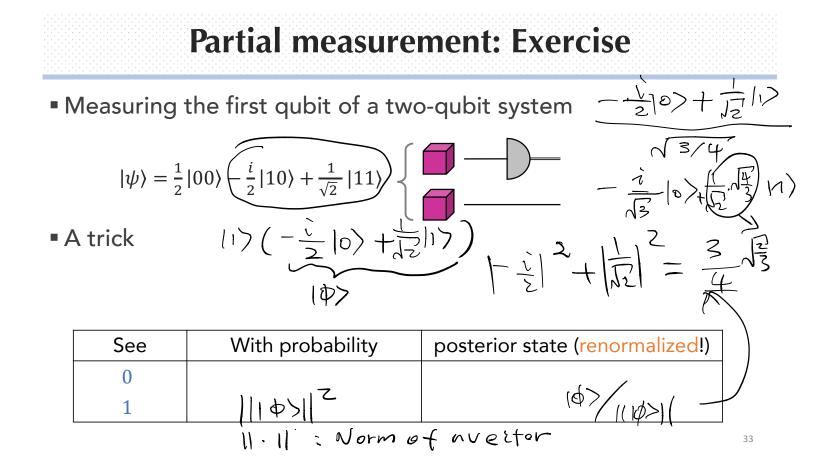


Partial measurement

## **Partial measurement: Exercise**

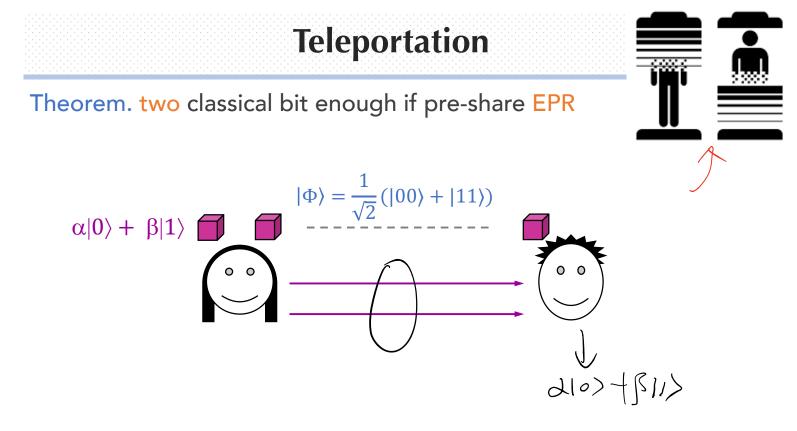
Measuring the first qubit of a two-qubit system

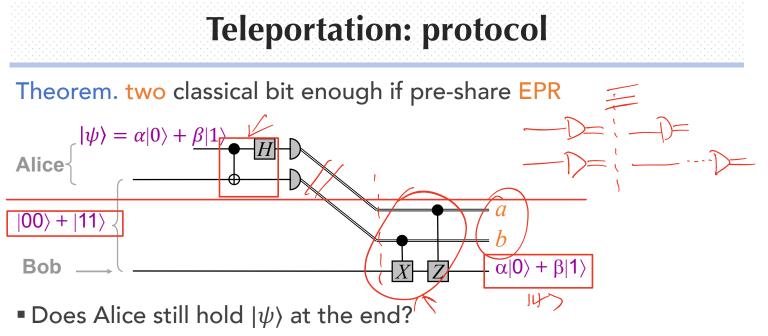
See	With probability	posterior state (renormalized!)
0	1/4	100>
1	3/4	$\left(-\frac{1}{2}\left(10\right)+\frac{1}{\sqrt{2}}\left(10\right)/\frac{3}{4}\right)$
		$= \frac{1}{\sqrt{2}}  10\rangle + \frac{1}{\sqrt{2}}  11\rangle$



## **Transmitting qubits by classical bits** Goal: Alice conveys a qubit to Bob by sending just classical bits Bob Alice $\alpha |0\rangle + \beta |1\rangle$ (••) $\alpha |0\rangle + \beta |1\rangle$

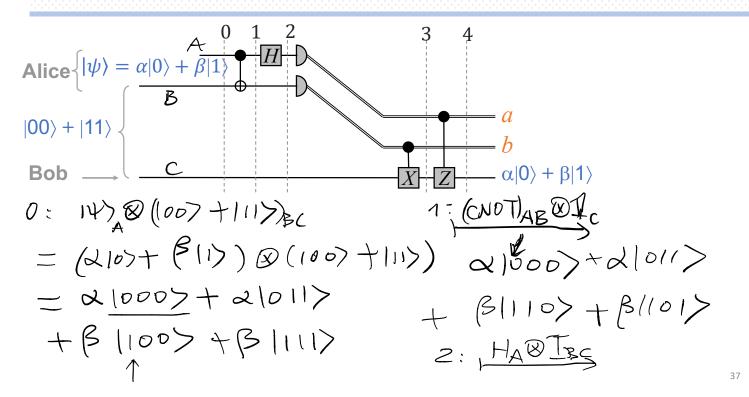
- If Alice knows  $\alpha, \beta \in \mathbb{C}$ , requires infinitely many bits for perfect precision
- If Alice doesn't know  $\alpha$  or  $\beta$ , she can at best acquire one bit by measurement

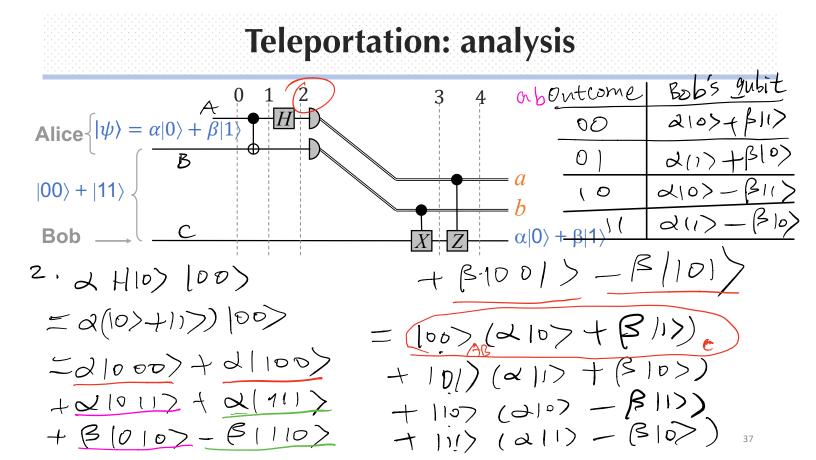




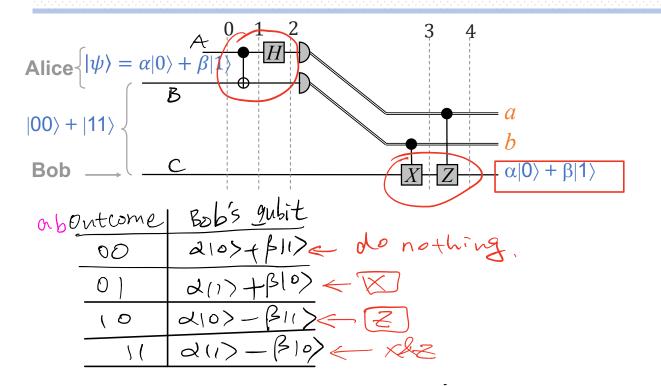
Communicating faster than the speed of light?

### **Teleportation: analysis**





### **Teleportation: analysis**



# Scratch 39

## **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 39