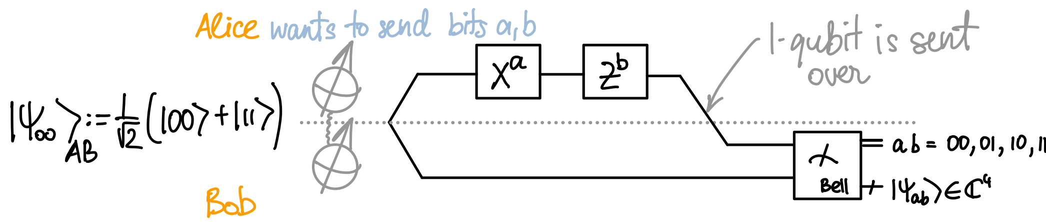
LECTURE 2.2

SUPER-DENSE CODING

Shared entanglement allows Alice to communicate 2 classical bits by sending just 1 qubit.



- Alice & Bob have pre-shared an EPR-pair $|\Psi_{00}\rangle_{AB}$
- Alice wants to send 2 classical bits $a, b \in \{0,1\}$ to Bob

Protocol

1) Alice applies X^a, followed by Z^b to her qubit

   $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $X^0 = \mathbb{1} = Z^0$

2) Alice sends her qubit to Bob

3) Bob measures his 2 qubits in Bell basis

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = (Z \otimes \mathbb{1})|\Psi_{00}\rangle$$
$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = (X \otimes \mathbb{1})|\Psi_{00}\rangle$$
$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = (Z \otimes \mathbb{1})|\Psi_{10}\rangle = (ZX \otimes \mathbb{1})|\Psi_{00}\rangle$$

$$\boxed{|\Psi_{ab}\rangle = (Z^b X^a \otimes \mathbb{1})|\Psi_{00}\rangle}$$

Key property: we can convert one Bell state into any another by applying a LOCAL(!) unitary.

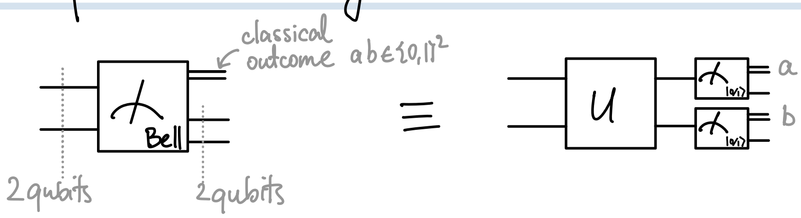
Observe: Given any two quantum states $|\psi\rangle$ and $|\varphi\rangle$ in $\mathbb{C}^d$ we can find a unitary U that sends $|\psi\rangle$ to $|\varphi\rangle$.

Analysis (correctness of the protocol)

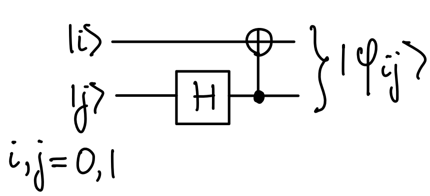
- After step 3) Bob has Bell state $|\Psi_{ab}\rangle$
- Note: $\langle \Psi_{ab} | \Psi_{a'b'} \rangle = \begin{cases} 1 & \text{if } a=a' \text{ and } b=b' \\ 0 & \text{otherwise} \end{cases}$
- Bob's measurement outcome always yields the bits that Alice wanted to send.

Note: Protocol consumes the shared entanglement

What if we are only able to measure in $|0/1\rangle$-basis?



We need U to map Bell basis to standard basis: $|\Psi_{ab}\rangle \xmapsto{U} |a\rangle|b\rangle$



Q: Compute $|\varphi_{ij}\rangle$

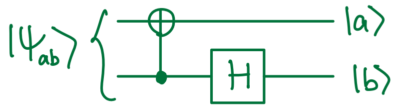
Ans: $|ij\rangle \xmapsto{1 \otimes H} = |i\rangle \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^j |1\rangle\right)$

$\xmapsto{CNOT} \underbrace{\frac{1}{\sqrt{2}}\left(|i0\rangle + (-1)^j |\bar{i}1\rangle\right)}_{|\Psi_{ij}\rangle}$

The circuit does almost what we wanted.

What is the circuit for mapping $|\psi_{ab}\rangle$ to $|ab\rangle$?

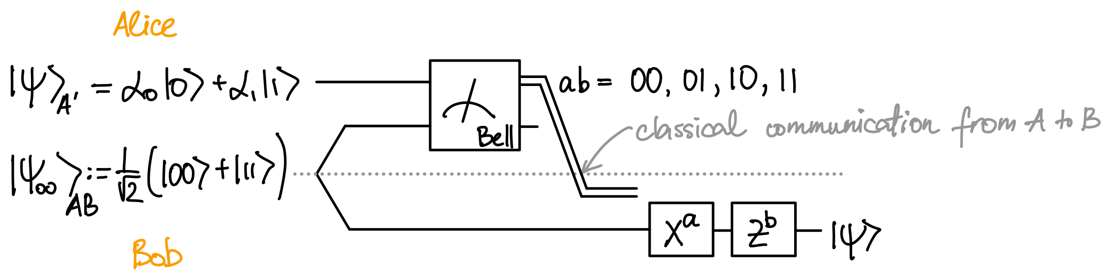
Ans:



in general, we not only need to "flip" the circuit but also take $U^\dagger$ for each of the gates.
in our case: $H^\dagger = H$ and $CNOT^\dagger = CNOT$.

Quantum Teleportation

Shared entanglement allows Alice to send 1 qubit to Bob using 2 bits of classical communication.



- Alice and Bob share an EPR-pair $|\Psi_{00}\rangle_{AB}$
- Alice has an unknown qubit state $|\psi\rangle_{A'}$ that she wants to send to Bob.

Protocol

1) Alice measures her two qubits in Bell basis
2) She sends the measurement outcome (2 bits ab) to Bob
3) Bob applies X^a followed by Z^b to his qubit

Analysis (correctness of the protocol)

Initial state: $|\psi\rangle_{A'}|\Psi_{00}\rangle_{AB}$

Measurement on the joint system is given by projectors

$$M_{ab} := |\Psi_{ab}\rangle\langle\Psi_{ab}|_{A'A} \otimes \mathbb{1}_B$$

$$|\psi\rangle_{A'}|\Psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}\left[\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|100\rangle + \alpha_1|111\rangle\right] =$$

$$|00\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle + |\Psi_{01}\rangle\right)$$
$$|11\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle - |\Psi_{01}\rangle\right)$$
$$|01\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{10}\rangle + |\Psi_{11}\rangle\right)$$
$$|10\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{10}\rangle - |\Psi_{11}\rangle\right)$$

$$= \frac{1}{2}\Big[\left(|\Psi_{00}\rangle + |\Psi_{01}\rangle\right)\otimes\alpha_0|0\rangle + \left(|\Psi_{10}\rangle + |\Psi_{11}\rangle\right)\otimes\alpha_0|1\rangle\Big) +$$
$$+ \left(|\Psi_{10}\rangle - |\Psi_{11}\rangle\right)\otimes\alpha_1|0\rangle\Big) + \left(|\Psi_{00}\rangle - |\Psi_{01}\rangle\right)\otimes\alpha_1|1\rangle\Big]$$

$$= \frac{1}{2}\Big[|\Psi_{00}\rangle\otimes\overbrace{\left(\alpha_0|0\rangle + \alpha_1|1\rangle\right)}^{|\psi\rangle} + |\Psi_{01}\rangle\otimes\overbrace{\left(\alpha_0|0\rangle - \alpha_1|1\rangle\right)}^{Z|\psi\rangle} +$$
$$+ |\Psi_{10}\rangle\otimes\underbrace{\left(\alpha_1|0\rangle + \alpha_0|1\rangle\right)}_{X|\psi\rangle} + |\Psi_{11}\rangle\underbrace{\left(-\alpha_1|0\rangle + \alpha_0|1\rangle\right)}_{XZ|\psi\rangle}$$

$$= \frac{1}{2}\sum_{a',b'=0}^{1} |\Psi_{a'b'}\rangle_{AA'}\otimes\left(X^{a'}Z^{b'}\right)|\psi\rangle_B =: |\varphi\rangle$$

What state are Alice & Bob left with after Alice measures her 2 qubits in Bell basis and obtains outcome ab?

Ans: Their state is proportional to

$$\underbrace{\left(|\Psi_{ab}\rangle\langle\Psi_{ab}|\otimes \mathbb{1}_B\right)|\varphi\rangle}_{\frac{1}{2}\sum_{a',b'}\underbrace{\langle\Psi_{ab}|\Psi_{a'b'}\rangle}_{0 \text{ unless } a=a' \text{ and } b=b'}\otimes\mathbb{1}_B\left(X^{a'}Z^{b'}\right)_B|\psi\rangle_B} = \frac{1}{2}|\Psi_{ab}\rangle_{AA'}\left(X^aZ^b|\psi\rangle_B\right)$$

$$= \frac{1}{2}X^aZ^b|\psi_B\rangle$$

- At the end Bob applies (Z^bX^a) and obtains $|\psi\rangle$.

QUANTUM INFORMATION CANNOT BE COPIED

(aka "no-cloning theorem")

This is very different from classical information, which can easily be copied

($\Rightarrow$ schemes for unforgeable quantum money & copy-protection)

For contradiction, assume there is a 2-qubit unitary U, such that

$$U|\psi,0\rangle = |\psi,\psi\rangle$$

for all 1-qubit states $|\psi\rangle$

In particular,

$$U|00\rangle = |00\rangle \qquad (\star)$$
$$U|10\rangle = |11\rangle$$

Now we'll compute $U|+,0\rangle$ in two different ways

1) Since U copies any 1-qubit state: $U|+,0\rangle = |++\rangle$

2) $U|+,0\rangle = \frac{1}{\sqrt{2}}\left(U|00\rangle + U|10\rangle\right)$

by $(\star)$ $= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

not the same!

Contradiction

QUANTUM STATE DISCRIMINATION

We are given a 1-qubit state that is prepared in state $|0\rangle$ or $|+\rangle$ with equal probability.

$|0\rangle$ or $|+\rangle$?

Task: Guess which state it is

Q: What would be your strategy?

Example strategy: Measure in $|0/1\rangle$ basis.

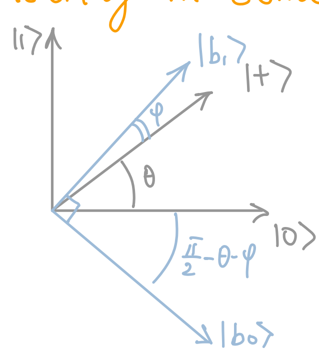
Outcome 1: guess $|+\rangle$

Outcome 0: guess $|0\rangle$

Probability of success

$$
\begin{aligned}
P_{succ} &= \Pr(|\psi\rangle = |0\rangle \text{ and measure } 0) + \Pr(|\psi\rangle = |+\rangle \\
&= \Pr(|\psi\rangle = |0\rangle) \cdot \Pr(\text{measure } 0 \mid |\psi\rangle = |0\rangle) + \\
&\qquad \Pr(|\psi\rangle = |+\rangle) \cdot \Pr(\text{measure } 1 \mid |\psi\rangle = |+\rangle) \\
&= \frac{1}{2} \cdot |\langle 0|0\rangle|^2 + \frac{1}{2} |\langle 1|+\rangle|^2 \\
&= \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}
\end{aligned}
$$

Can we do better by measuring in some (other) basis $\{|b_0\rangle, |b_1\rangle\}$?

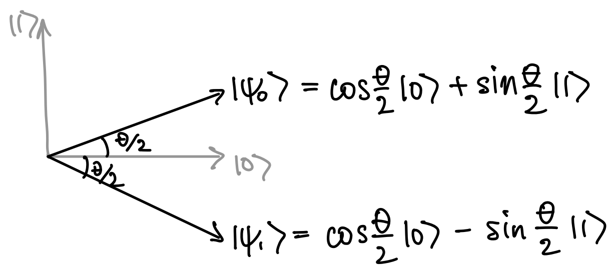


$|\langle b_1|+\rangle|^2 = \cos^2(\varphi)$

$|\langle b_0|0\rangle|^2 = \cos^2\left(\frac{\pi}{2} - \theta - \varphi\right)$

The success probabilities we can reach only depend on the angle, θ, between the two states to be discriminated.

So instead of analyzing $|0\rangle$ vs $|+\rangle$, we can look at $|\psi_0\rangle$ vs $|\psi_1\rangle$ for $\theta = \frac{\pi}{4}$



Protocol: measure in basis $\{|b_0\rangle, |b_1\rangle\}$
On outcome i, guess state $|\psi_i\rangle$

$$p_{succ} = \sum_{i=0}^{1} \Pr(\text{state is } |\psi_i\rangle \,\&\, \text{get outcome } i)$$

$$= \sum_{i=0}^{1} \Pr(\text{state is } |\psi_i\rangle)\,(\text{get outcome } i \mid \text{state is } |\psi_i\rangle)$$

$$= \sum_{i=0}^{1} \frac{1}{2} \cdot |\langle b_i|\psi_i\rangle|^2 =$$

$$|\langle b_i|\psi_i\rangle|^2 = \mathrm{Tr}(\langle\psi_i|b_i\rangle\langle b_i|\psi_i\rangle)$$
$$= \mathrm{Tr}(|b_i\rangle\langle b_i| \cdot \underbrace{|\psi_i\rangle\langle\psi_i|}_{=:\rho_i})$$

$$|b_0\rangle\langle b_0| + |b_1\rangle\langle b_1| = \mathbb{1}$$

$$= \frac{1}{2}\sum_{i=0}^{1} \mathrm{Tr}(|b_i\rangle\langle b_i|\rho_i)$$

$$= \frac{1}{2}\left[\mathrm{Tr}(|b_0\rangle\langle b_0|\rho_0) + \mathrm{Tr}(\overbrace{(\mathbb{1} - |b_0\rangle\langle b_0|)}^{|b_1\rangle\langle b_1|}\rho_1)\right]$$

$$= \frac{1}{2}\mathrm{Tr}(|b_0\rangle\langle b_0|(\rho_0 - \rho_1)) + \frac{1}{2}\cdot\underbrace{\mathrm{Tr}(\rho_1)}_{1}$$

$$\rho_0 - \rho_1 = |\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1| =$$

$$= \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix} - \begin{pmatrix} \cos^2\frac{\theta}{2} & -\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix}$$

$$= 2\cos\frac{\theta}{2}\sin\frac{\theta}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sin\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \frac{1}{2}\sin\theta \, \mathrm{Tr}\left(|b_0\rangle\langle b_0| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right) + \frac{1}{2}$$

$$= \frac{1}{2}\sin\theta \, \langle b_0| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |b_0\rangle + \frac{1}{2}$$

Which choice of $|b_0\rangle$ will maximize the expression?