# CPEN 400Q Lecture 05
# Our first quantum algorithms

Monday 22 January 2024

# Announcements

$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $\quad |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$

$|0\rangle$ w/prob $|\alpha|^2$

$|\langle \phi | \psi \rangle|^2$

- Quiz 2 today
- Assignment 1 due Fri 02 Feb at 23:59
- Midterm in class on Wed 31 Jan - see Piazza post 14 for practice strategies; covers "the basics", i.e., lectures 01-07

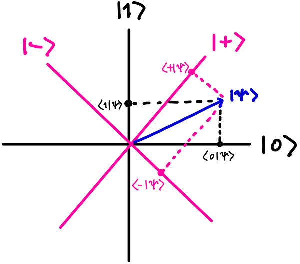
# Last time

We took single-qubit measurements in different orthonormal bases.

$\{|b_1\rangle, |b_2\rangle\}$

$|0\rangle \rightarrow |b_1\rangle$

$|1\rangle \rightarrow |b_2\rangle$




```
def convert_to_y_basis():
    qml.Hadamard(wires=0)
    qml.S(wires=0)

def my_quantum_function():
    ...
    qml.adjoint(convert_to_y_basis)()
    ...
```

Image credit: Codebook node I.9

Measuring in a different basis can help us distinguish states.

**Example:** Prepare $|+\rangle$ or $|-\rangle$, then measure in the comp. basis.

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

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

**Example:** Prepare $|+\rangle$ or $|-\rangle$, then measure in the Hadamard ($|+\rangle/|-\rangle$) basis.

$$\{|+\rangle, |-\rangle\}$$

# Last time

We began working with more than one qubit.

Hilbert spaces combine under the *tensor product*. If

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\phi\rangle = \gamma|0\rangle + \delta|1\rangle$$

then

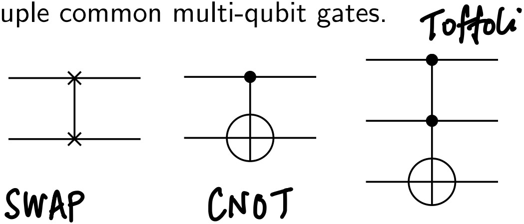
$$|\psi\rangle \otimes |\phi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

$$= \alpha\gamma|00\rangle + \beta\gamma|10\rangle + \alpha\delta|01\rangle + \beta\delta|11\rangle$$

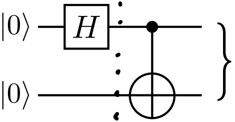
But not all multi-qubit states are tensor products:

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

We saw a couple common multi-qubit gates.




We saw that CNOT is an *entangling gate*. → sends something separable to stg. entangled

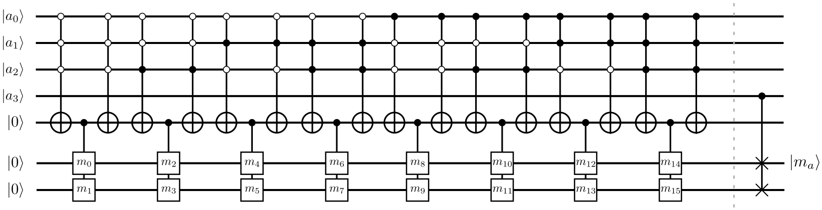



$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$|+\rangle \otimes |0\rangle$

# Last time

Any unitary operation can be turned into a controlled operation, controlled on any state.




Most common controls are controlled-on-$|1\rangle$ (filled circle), and controlled-on-$|0\rangle$ (empty circle).

```
qml.ctrl(qml.RX, control=0)(x, wires=1)
qml.CRX(x, wires=[0, 1])
```

# Learning outcomes

- Measure a two-qubit state in the Bell basis
- Outline and implement the superdense coding algorithm
- Prove that arbitrary quantum states cannot be cloned
- Teleport a quantum state

# Review: single-qubit measurements

Given a state

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

- the probability of measuring and observing the qubit in state $|0\rangle$ is $|\langle 0|\psi\rangle|^2 = |\alpha|^2$
- the probability of measuring and observing the qubit in state $|1\rangle$ is $|\langle 1|\psi\rangle|^2 = |\beta|^2$
- we can measure in different bases by "remapping" those basis states to the computational basis

We can do all this in the multi-qubit case as well.

Let

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

If we measure in the computational basis, the outcome probabilities are:

- $|\alpha|^2$ for $|00\rangle$ $= |\langle 00|\psi\rangle|^2$
- $|\beta|^2$ for $|01\rangle$ $= |\langle 01|\psi\rangle|^2$
- ...

# Multi-qubit measurement outcome probabilities

Let

$$|\psi\rangle = \underset{\substack{\Downarrow \\ |\alpha|^2}}{\alpha|00\rangle} + \underset{\substack{\Downarrow \\ |\beta|^2}}{\beta|01\rangle} + \gamma|10\rangle + \delta|11\rangle$$

We can measure *just one qubit*:

- The probability of the first qubit being in state $|0\rangle$ is
  $|\alpha|^2 + |\beta|^2$
- The probability of the second qubit being in state $|1\rangle$ is
  $|\beta|^2 + |\delta|^2$

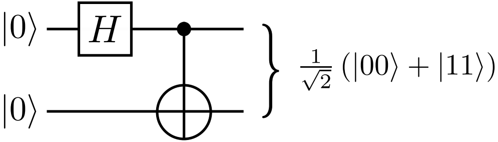
We can also measure multiple qubits in other bases.

## Bell states

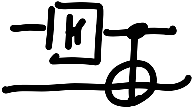
Remember how we created

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

from the $|00\rangle$ state:



**Exercise**: Apply the same circuit to the other 3 computational basis states? What is special about these four states?




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

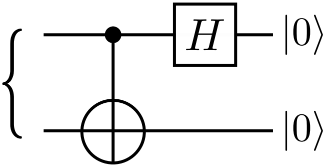
$$|01\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|1\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|10\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)|0\rangle \to \frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

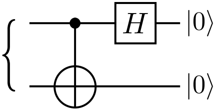
$$|11\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)|1\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

We can measure in this basis by applying the circuit in reverse:

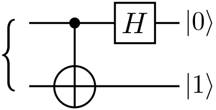
$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$



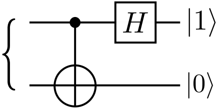
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



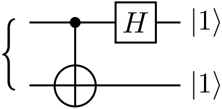

$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$




$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$




$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$




Two famous quantum algorithms, **superdense coding** and **teleportation** work by performing a measurement in the Bell basis.

Suppose Alice wants to send Bob two classical bits of information, say '1' and '0'.

Q1: How many classical bits must she send to Bob to do this?

2

# Superdense coding

Suppose Alice wants to send Bob two classical bits of information, say ‘1’ and ‘0’.

Q1: How many classical bits must she send to Bob to do this?
A1: 2.

# Superdense coding

Suppose Alice wants to send Bob two classical bits of information, say ‘1’ and ‘0’.

Q1: How many classical bits must she send to Bob to do this?
A1: 2.

Q2: How many *qubits* must she send to Bob to do this?

Suppose Alice wants to send Bob two classical bits of information, say ‘1’ and ‘0’.

Q1: How many classical bits must she send to Bob to do this?
A1: 2.

Q2: How many *qubits* must she send to Bob to do this?
A2: Only 1!

Alice and Bob start the protocol with this shared entangled state:

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

Next, depending on her bits, Alice performs one of the following operations on her qubit:

$$\begin{aligned} 00 &\rightarrow I \\ 01 &\rightarrow X \\ 10 &\rightarrow Z \\ 11 &\rightarrow ZX \end{aligned}$$

# Superdense coding

What happened to the entangled state?

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

It will transform to:

$$\begin{aligned}
00 &\quad \rightarrow_{I} \quad \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
01 &\quad \rightarrow_{X} \quad \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right) \\
10 &\quad \rightarrow_{Z} \quad \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\
11 &\quad \rightarrow_{ZX} \quad \frac{1}{\sqrt{2}}\left(-|10\rangle + |01\rangle\right)
\end{aligned}$$

Bob can now perform a measurement to determine with certainty which state he has, and correspondingly which bits Alice sent him.

Alternatively, Bob can perform a basis transformation from the Bell basis back to the computational basis:

$$
\begin{aligned}
(H \otimes I)\mathrm{CNOT} \cdot \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= |00\rangle \\
(H \otimes I)\mathrm{CNOT} \cdot \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) &= |01\rangle \\
(H \otimes I)\mathrm{CNOT} \cdot \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) &= |10\rangle \\
(H \otimes I)\mathrm{CNOT} \cdot \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &= |11\rangle
\end{aligned}
$$

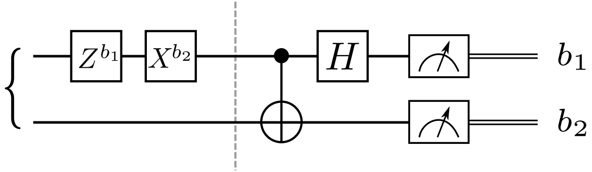
Start

$$
\begin{array}{ccc}
 & \boxed{\text{Factory}} & \\
\swarrow & & \searrow \\
A & & B \\
\text{qubit 0} & & \text{qubit 1}
\end{array}
= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)
$$

# Hands-on: superdense coding

Let's go implement it!

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

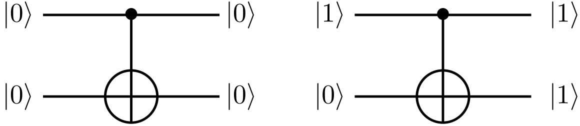


# Copying quantum states

$$|\psi\rangle|??\rangle \to |\psi\rangle|\psi\rangle$$

Suppose you found a really cool quantum state, and you want to send a copy to a friend. Can you?

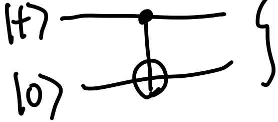
Idea: CNOT sends $|00\rangle$ to $|00\rangle$, and $|10\rangle$ to $|11\rangle$, thus copying the first qubit's state to the second.




Everything is linear, so will this work in general?

Very easy to find a state for which this fails:

$|+0\rangle$




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

$\neq |++\rangle$

# (Not) copying quantum states

**The no-cloning theorem**

It is impossible to create a copying circuit that works for arbitrary quantum states.

In other words, there is no circuit that sends

$$\underbrace{|\psi\rangle \otimes |s\rangle}_{\text{can be anything}} \rightarrow |\psi\rangle \otimes |\psi\rangle$$

for any arbitrary $|\psi\rangle$.

can be anything

Suppose we want to clone a state $|\psi\rangle$. We want a unitary operation that sends

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

where $|s\rangle$ is some arbitrary state.

Let's suppose we find one. If our cloning machine is going to be universal, then we must also be able to clone some other state, $|\varphi\rangle$.

$$U\left(|\varphi\rangle \otimes |s\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle$$

$$\langle |\psi_1\rangle, |\psi_2\rangle \rangle = \langle \psi_1 | \psi_2 \rangle$$

We purportedly have:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Take the inner product of the LHS of both equations:

→ exercise

$$\underbrace{\left(\langle\psi|\otimes\langle s|\right)U^\dagger}_{\langle\psi_1|}\overset{"\mathbb{1}"}{\,}\underbrace{U\left(|\varphi\rangle\otimes|s\rangle\right)}_{|\psi_2\rangle} = \left(\langle\psi|\otimes\langle s|\right)\left(|\varphi\rangle\otimes|s\rangle\right)$$
$$= \langle\psi|\varphi\rangle\cdot\langle s|s\rangle = \langle\psi|\varphi\rangle$$

Now take the inner product of the RHS of both equations:

$$\left(\langle\psi|\otimes\langle\psi|\right)\left(|\varphi\rangle\otimes|\varphi\rangle\right) = \langle\psi|\varphi\rangle\cdot\langle\psi|\varphi\rangle$$
$$= \left(\langle\psi|\varphi\rangle\right)^2$$

equal?

$|a|^2 = \alpha\alpha^* \neq \alpha^2$ in general

# Proof of the no-cloning theorem

For what states does

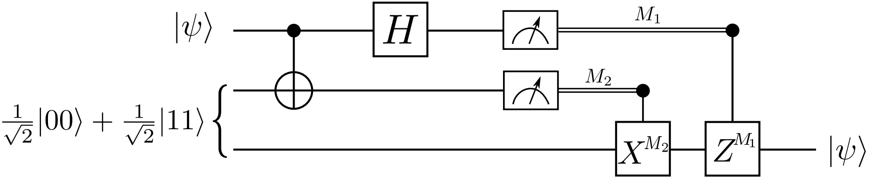
$$(\langle\psi|\varphi\rangle)^2 = \langle\psi|\varphi\rangle$$

Need a complex number that squares to itself... but the only numbers that square to themselves are 0 and 1!

So either the two states are orthogonal, or are just the same state. They can't be arbitrary!

# Teleportation

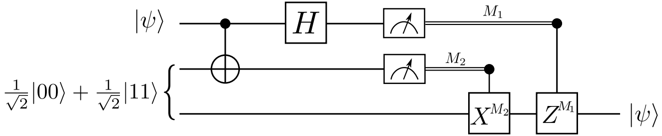
We cannot clone arbitrary qubit states, but we *can* teleport them!




stopped here: will start on Wed.

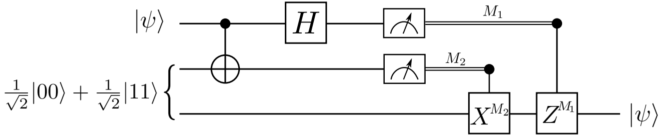
# Quantum teleportation: the details

Let's go one gate at a time.



# Quantum teleportation: the details

Let's go one gate at a time.



# Quantum teleportation: the details

Before measurements, the combined state of the system is (removing the $\frac{1}{2}$ for readability):

$$\begin{aligned}
|00\rangle &\otimes (\alpha|0\rangle + \beta|1\rangle) + \\
|01\rangle &\otimes (\alpha|1\rangle + \beta|0\rangle) + \\
|10\rangle &\otimes (\alpha|0\rangle - \beta|1\rangle) + \\
|11\rangle &\otimes (\alpha|1\rangle - \beta|0\rangle)
\end{aligned}$$

This is a *uniform* superposition of 4 distinct terms. If we measure the first two qubits in the computational basis, we are equally likely to obtain each of the four outcomes.

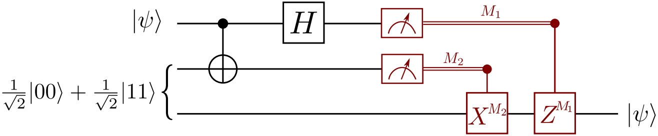
You can see that Bob's state is always some variation on the original state of Alice:

$$
\begin{aligned}
|00\rangle &\otimes (\alpha|0\rangle + \beta|1\rangle) + \\
|01\rangle &\otimes (\alpha|1\rangle + \beta|0\rangle) + \\
|10\rangle &\otimes (\alpha|0\rangle - \beta|1\rangle) + \\
|11\rangle &\otimes (\alpha|1\rangle - \beta|0\rangle)
\end{aligned}
$$

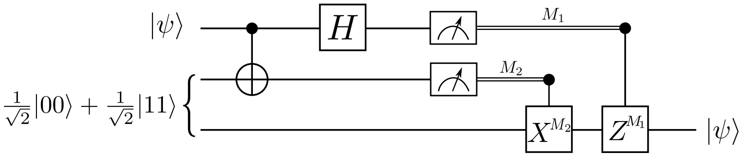
# Quantum teleportation: the details

Alice measures in the computational basis and sends her results to Bob. Once Bob knows the results, he knows exactly what term of the superposition they had, and can adjust his state accordingly.

$$
\begin{aligned}
00 &: I(\alpha|0\rangle + \beta|1\rangle) = (\alpha|0\rangle + \beta|1\rangle)\\
01 &: X(\alpha|1\rangle + \beta|0\rangle) = (\alpha|0\rangle + \beta|1\rangle)\\
10 &: Z(\alpha|0\rangle - \beta|1\rangle) = (\alpha|0\rangle + \beta|1\rangle)\\
11 &: ZX(\alpha|1\rangle - \beta|0\rangle) = (\alpha|0\rangle + \beta|1\rangle)
\end{aligned}
$$



## Hands on: let's teleport a state



# Recap

- Measure a two-qubit state in the Bell basis
- Outline and implement the superdense coding algorithm
- Prove that arbitrary quantum states cannot be cloned
- Teleport a quantum state

# Next time

Content:

- Measurement part 2: expectation values

Action items:

1. Assignment 1
2. Preparing for midterm

Recommended reading:

- Codebook nodes I.15, I.10
- Nielsen & Chuang 1.3.5-1.3.7, 1.4.2-1.4.4, 2.3