CPEN 400Q Lecture 05
Our first quantum algorithms

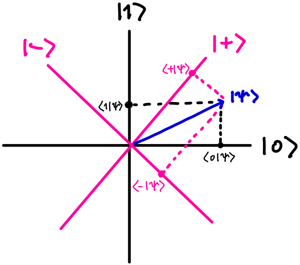
Monday 23 January 2023

Announcements

- Literacy assignment 1 due Wednesday 23:59
- Assignment 1 available
- Quiz 2 at the *end* of class today

Last time

We took single-qubit measurements in different orthonormal bases.




```
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.

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

We began working with more than one qubit.

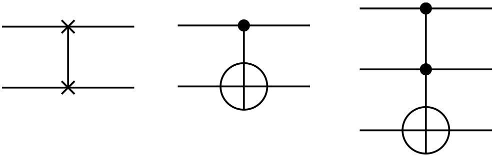
Hilbert spaces combine under the *tensor product*. If

then

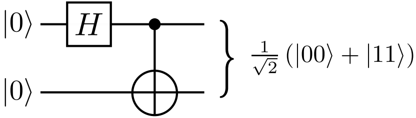
But not all multi-qubit states are tensor products:

Last time

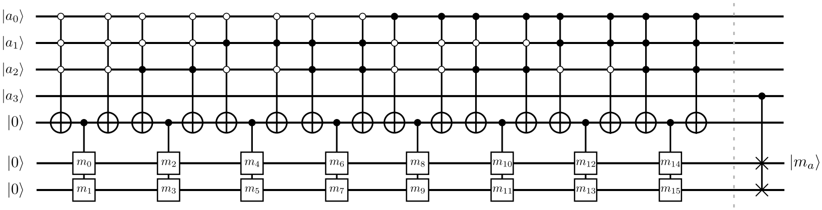
We saw a couple common multi-qubit gates.



We saw that CNOT is an *entangling gate*.



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])
```

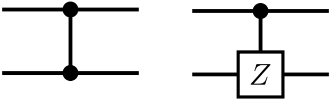
Learning outcomes

- Express two-qubit controlled gates as matrices
- Perform measurements on multiple qubits
- Measure a two-qubit state in the Bell basis

If we get there:

- Outline and implement the superdense coding algorithm
- Prove that arbitrary quantum states cannot be cloned
- Teleport a quantum state

What does this operation do?



PennyLane: `qml.CZ`

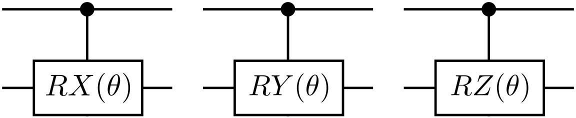
Image credit: Codebook node I.13

Example: controlled rotations (*RX*, *RY*, *RZ*)

Or this one?

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

Circuit elements:



PennyLane: `qml.CRX`, `qml.CRY`, `qml.CRZ`

Image credit: Codebook node I.14

There is a pattern here:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad CRY(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ 0 & 0 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

More generally,

$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix} = \begin{pmatrix} I_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & U \end{pmatrix}$$

Universal gate sets

In lecture 3, we learned that with just

- H and T
- any two of RX, RY, and RZ,

we can implement *any* single-qubit unitary operation up to arbitrary precision.

What about for two qubits?

Universal gate sets

What about for two qubits?

- H, T, and $CNOT$
- any two of RX, RY, RZ, and $CNOT$
- H and TOF

With just 2-3 gates, we can implement *any* two-qubit unitary operation up to arbitrary precision.

What about three or more qubits? (Same thing!)

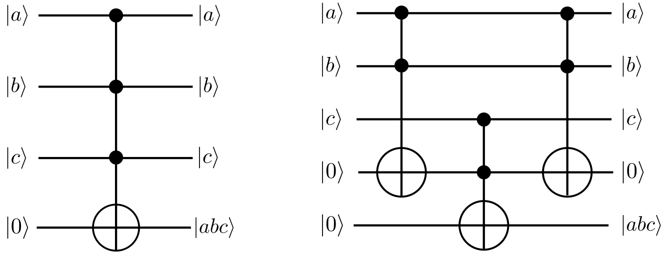
Universal gate sets

In general, finding such an implementation (*quantum circuit synthesis*, part of the quantum compilation pipeline) is computationally hard.

- sometimes we can do so for small cases (PennyLane has many decompositions pre-programmed)
- sometimes having **auxiliary** qubits around can simplify the decomposition

Auxiliary qubits

Auxiliary qubits are like "scratch", or "work" qubits. They start in state $|0\rangle$, and must be returned to state $|0\rangle$, but can be used to store intermediate results in a computation.



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
- the probability of measuring and observing the qubit in state $|1\rangle$ is
- 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.

Multi-qubit measurement outcome probabilities

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:

- for $|00\rangle$
- for $|01\rangle$
- ...

Multi-qubit measurement outcome probabilities

Let

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

We can measure *just one qubit*:

- The probability of the first qubit being in state $|0\rangle$ is
- The probability of the second qubit being in state $|1\rangle$ is

We can also measure multiple qubits in other bases.

The Bell basis

This entangled state,

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

has 3 siblings:

These 4 entangled states form an *orthonormal basis* for 2 qubits.

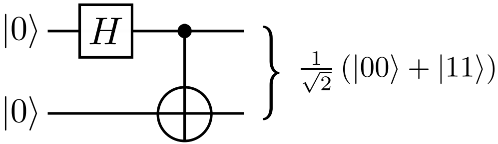
$$
\begin{aligned}
|\Psi_{00}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
|\Psi_{01}\rangle &= \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right) \\
|\Psi_{10}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\
|\Psi_{11}\rangle &= \frac{1}{\sqrt{2}}\left(-|10\rangle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

The Bell basis

Remember how we created

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

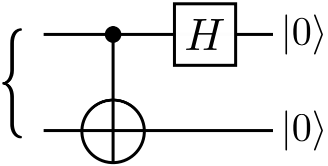
from the $|00\rangle$ state:



The Bell basis

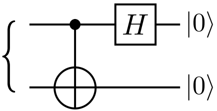
We can undo this by applying the operations in reverse:

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

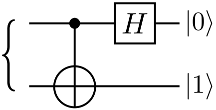


This sequence of operations actually corresponds to a basis rotation from the Bell basis to the computational basis...

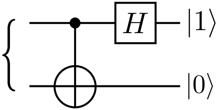
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



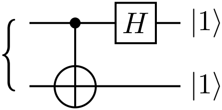
$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$



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



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



Two quantum algorithms, **superdense coding** and **teleportation** work by performing a measurement in the Bell basis (or, performing the above basis rotation, and measuring in the computational 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?

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.

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!

Superdense coding

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

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

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

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

What happened to the entangled state?

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

It will transform to:

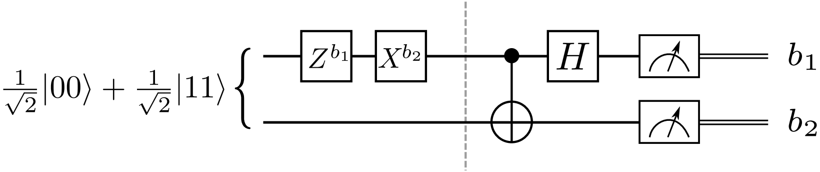
$$\begin{aligned} 00 &\rightarrow_I \\ 01 &\rightarrow_X \\ 10 &\rightarrow_Z \\ 11 &\rightarrow_{ZX} \end{aligned}$$

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:

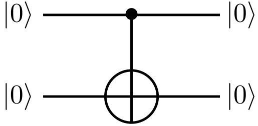
$$
\begin{aligned}
(H \otimes I)\mathsf{CNOT} \cdot \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= |00\rangle \\
(H \otimes I)\mathsf{CNOT} \cdot \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) &= |01\rangle \\
(H \otimes I)\mathsf{CNOT} \cdot \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) &= |10\rangle \\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

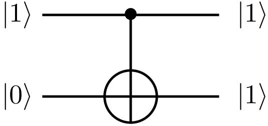
Let's go implement it!



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.

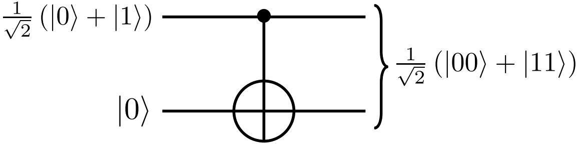




Everything is linear, so will this work in general?

Copying quantum states

Very easy to find a state for which this fails:



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

$$|\psi\rangle \otimes |s\rangle \to |\psi\rangle \otimes |\psi\rangle$$

for any arbitrary $|\psi\rangle$.

Proof of the no-cloning theorem

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

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, $|\varphi\rangle$.

We purportedly have:

$$
\begin{aligned}
U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle \\
U(|\varphi\rangle \otimes |s\rangle) &= |\varphi\rangle \otimes |\varphi\rangle
\end{aligned}
$$

Take the inner product of the LHS of both equations:

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

Proof of the no-cloning theorem

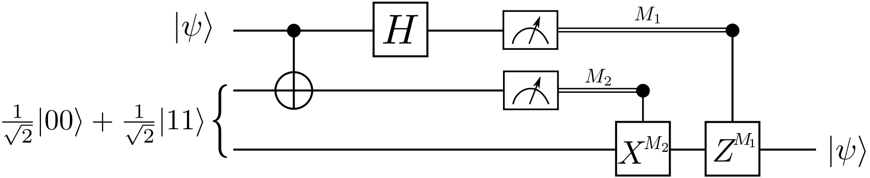
For what states does

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

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

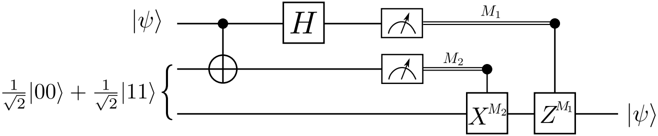
So either the two states are orthogonal, or are just the same state. They can't be arbitrary!

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



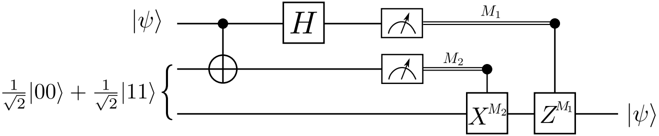
Quantum teleportation: the details

Let's go one gate at a time.



Quantum teleportation: the details

Let's go one gate at a time.



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

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

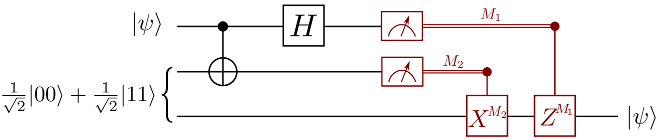
This is a *uniform* superposition of 4 distinct terms. If we measure the first two qubits in the computational basis, we are equally likely to obtain each of the four outcomes.

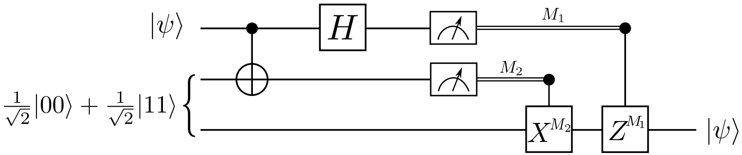
You can see that Bob's state is always some variation on the original state of Alice:

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

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.

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




$|\psi\rangle$
$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
H
M_1
M_2
X^{M_2}
Z^{M_1}
$|\psi\rangle$

Recap

- Express two-qubit controlled gates as matrices
- Perform measurements on multiple qubits
- Measure a two-qubit state in the Bell basis

If we get there:

- Outline and implement the superdense coding algorithm
- Prove that arbitrary quantum states cannot be cloned
- Teleport a quantum state

Next time

Content:

- Finish up remaining details about teleportation
- Our first variational algorithm: the variational quantum classifier

Action items:

1. Assignment 1
2. Literacy assignment 1

Recommended reading:

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