

Quantum Computing Refresher Tutorial

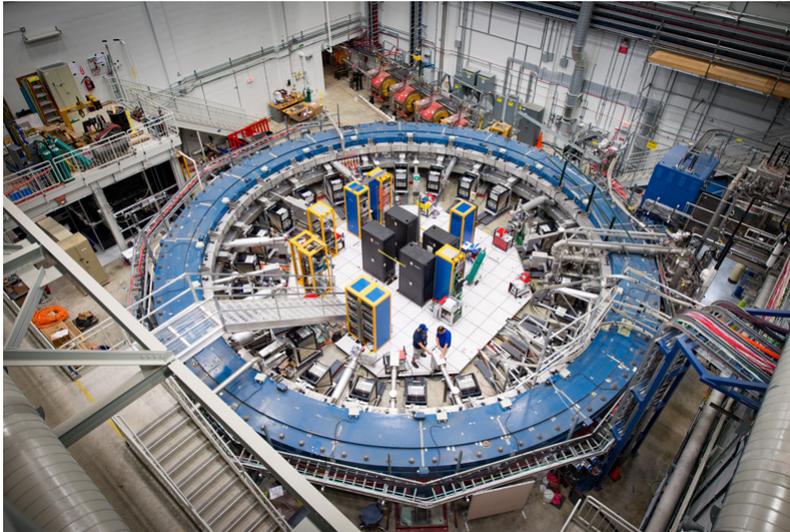
Adam Lyon/Fermilab SCD

September 13, 2018

Hi, I'm Adam...

I'm a Fermilab Senior Scientist.

I mostly work managing part of the Scientific Computing Division and am a scientist on the Muon g-2 Experiment.



I'm involved in Quantum Computing because it is applicable to my SCD role and I'm interested in how HEP researchers would use such systems (infrastructure, interfaces).

...and it's WAY COOL and new for me. Nothing like giving a tutorial to force yourself to learn something new.

We'll mostly follow the Argonne Workshop Tutorial (<https://github.com/zhenghh04/QCWorkshop/blob/master/IntroQM/QCWorkshopANL18.jp>) by Maththew Otten and Scott Aaronson's lecture notes (<https://www.scottaaronson.com/qclec/combined.pdf>) (errors in this talk are mine alone, of course).

Don't worry about the toolkits used here. Concentrate on the content.

Goal: Understand the basics of some quantum gates

This will be really fast - not meant at all to be a comprehensive introduction to QC nor will we go over all of the rules of QC. There are lots of good resources out there. Google (the search engine) can help you find them.

Let's go... Remember Probability..

Say we have coin that is either heads or tails.

A vector of classical probabilities can describe this system:

$$\begin{bmatrix} a \\ b \end{bmatrix} \begin{matrix} h \\ t \end{matrix} \text{ where } a, b \geq 0 \text{ and } a + b = 1$$

We can turn the coin over...

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}_t^h = \begin{bmatrix} b \\ a \end{bmatrix}_t^h$$

e.g. the transformation matrix is $\begin{bmatrix} P(\text{heads}|a) & P(\text{heads}|b) \\ P(\text{tails}|a) & P(\text{tails}|b) \end{bmatrix}$

so the old probability for heads is now the probability for tails and vice-versa

We can fairly flip the coin...

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}_t^h = \begin{bmatrix} \frac{1}{2}(a+b) \\ \frac{1}{2}(a+b) \end{bmatrix}_t^h = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix}_t^h$$

We can do fancier things, like flip the coin, and if we get heads flip again but if we get tails we turn it to heads

$$\begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}_t^h = \begin{bmatrix} \frac{1}{2}a + b \\ \frac{1}{2}a \end{bmatrix}_t^h \dots \text{remember} \begin{bmatrix} P(\text{heads}|a) & P(\text{heads}|b) \\ P(\text{tails}|a) & P(\text{tails}|b) \end{bmatrix}$$

If flip and get heads, then $a = 1, b = 0$. Flip again and final outcome is random $\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}_t^h$

If flip and get tails, then $a = 0, b = 1$. Turn over and always get heads. $\begin{bmatrix} 1 \\ 0 \end{bmatrix}_t^h$

Sum of column is 1.

Now two coins $\begin{bmatrix} a \\ b \end{bmatrix}_t^h$, $\begin{bmatrix} c \\ d \end{bmatrix}_t^h$

The combined probability is the **tensor product**

$$\begin{bmatrix} a \\ b \end{bmatrix}_t^h \otimes \begin{bmatrix} c \\ d \end{bmatrix}_t^h = \begin{bmatrix} P_{hh} \\ P_{ht} \\ P_{th} \\ P_{tt} \end{bmatrix}_{tt}^{hh} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}_{tt}^{hh}$$

Note that some products are impossible for independent coins, like

$$\begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}^{hh}_{tt}$$

Say we turn over the second coin only if the first coin is tails

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}_{tt}^{hh} = \begin{bmatrix} ac \\ ad \\ bd \\ bc \end{bmatrix}_{tt}^{hh} \quad (\text{Controlled not, CNOT})$$

Try starting with first coin random, second coin heads

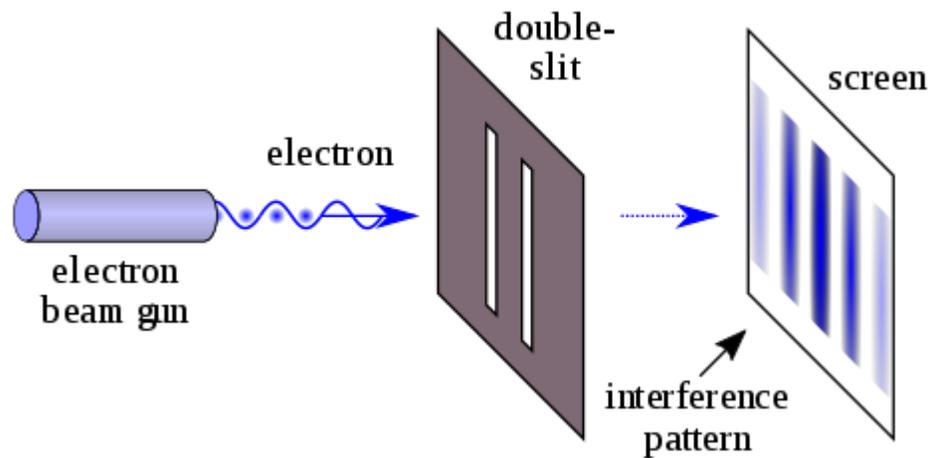
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1/2 \\ 0 \\ 1/2 \\ 0 \end{bmatrix}_{tt}^{hh} = \begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}_{tt}^{hh}$$

You can't get this with independent coins! They now must be correlated.

Amplitudes and Probabilities

A classical configuration is given by a probability for it occurring, $p \in [0, 1]$

A quantum configuration is given by a complex amplitude $\alpha \in \mathbb{C}$, probability of measuring the quantum system in that configuration is $p = |\alpha|^2$



(Wikipedia)

This is a key difference between classical and quantum systems!

So now using amplitudes...

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}_1^0 \text{ (for a two-state system - measured in state "0" or "1")}$$

The probability that a measurement shows the system is

in state 0 is $|\alpha|^2$ and is in state 1 is $|\beta|^2$

and $|\alpha|^2 + |\beta|^2 = 1$

System state described by unit vector in Hilbert space \mathcal{H}

We can simplify $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}_1^0$ with

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}_1^0 \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}_1^0 \text{ (these are basis vectors - the } \textit{Computational basis})$$

$$\text{So, } \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_1^0 = \alpha |0\rangle + \beta |1\rangle = |\psi\rangle$$

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ (ket - column vector)}$$

$$\langle\psi| = \alpha^* \langle 0| + \beta^* \langle 1| = [\alpha^* \ \beta^*] \text{ (bra - Hermitian conjugate - row vector)}$$

$\langle v|w\rangle$ is the inner product (projection of state w onto v)

$$\langle\psi|\psi\rangle = \alpha^* \alpha \langle 0|0\rangle + \beta^* \beta \langle 1|1\rangle = |\alpha|^2 + |\beta|^2 = 1$$

$$\langle 0|1\rangle = \langle 1|0\rangle = 0 \text{ (basis vectors are orthogonal)}$$

$$\langle v|w\rangle = \langle w|v\rangle^*$$

Linear transformation changes quantum states $U \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}$

U is **unitary** if $|\alpha|^2 + |\beta|^2 = |\alpha'|^2 + |\beta'|^2$ (preserves the norm)

A unitary matrix maps to a unitary transformation

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

Unitary transformations preserve the the norm

$$\langle \psi | \psi \rangle = \left(U | \psi \rangle \right)^\dagger U | \psi \rangle = \langle \psi | U^\dagger U | \psi \rangle$$

So, for any ψ , $U^\dagger U = I$ and thus $U^{-1} = U^\dagger$

and the rows of U form an ortho-normal unit basis

We can transform to other bases, such as,

$$|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \text{ (Hadamard Basis)}$$

$$|i\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \quad |-i\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$$

Rotating into other bases, for example,

$$R_\theta = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}, \text{ so } R_{\pi/4} = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$$

And

$$R_{\pi/4} |0\rangle = |+\rangle, R_{\pi/4} |+\rangle = |1\rangle$$

$$R_{\pi/4} |1\rangle = -|-\rangle,$$

This two state system is a *qubit*

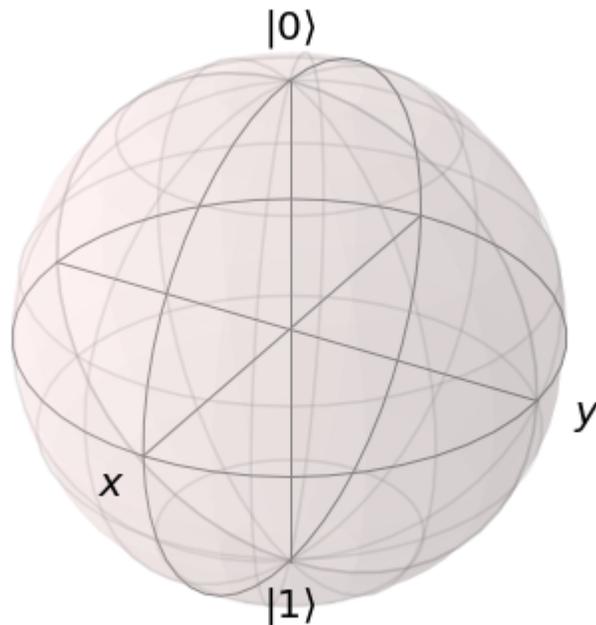
Like a classical bit, upon measurement it is either "0" or "1"

Unlike a classical bit, the qubit's amplitude makes for rich phenomena, like superposition

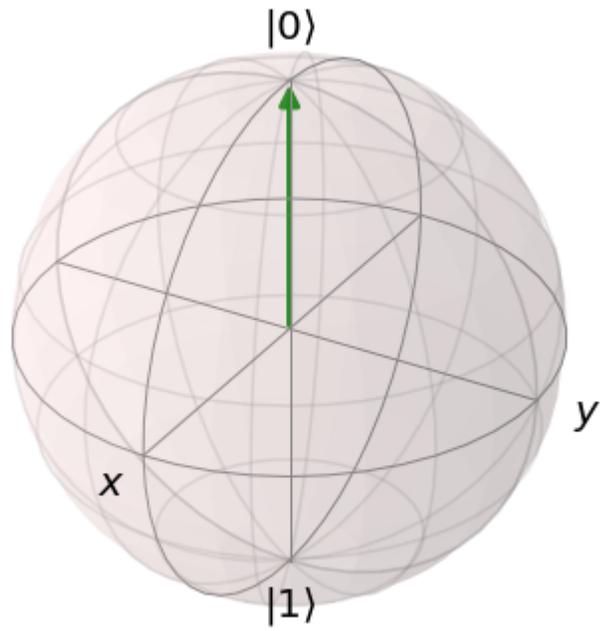
Bloch Sphere

Represent state of the qubit as $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$

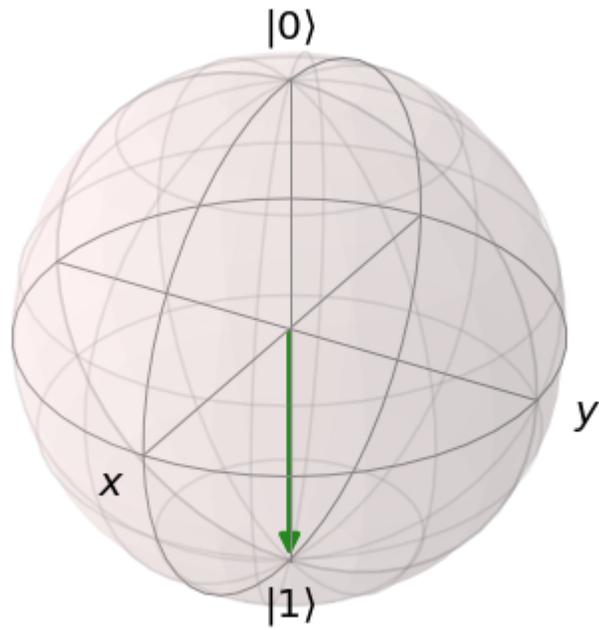
Plot this on a sphere. Note global phase. (Click on the sphere)



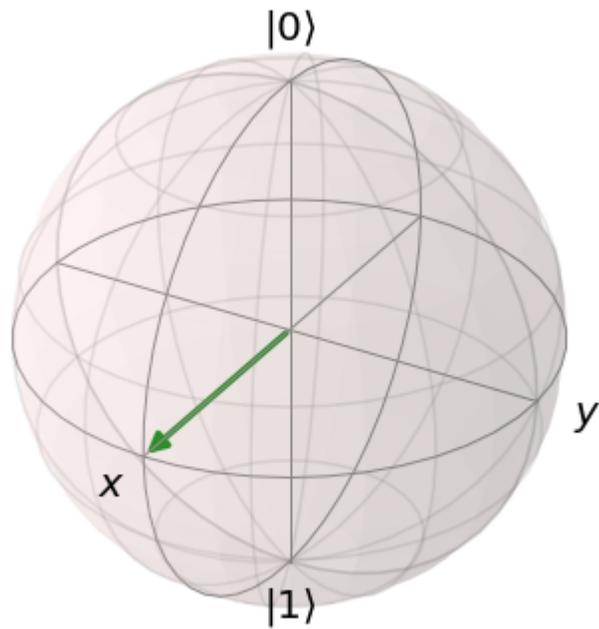
$$|\psi\rangle = |0\rangle$$



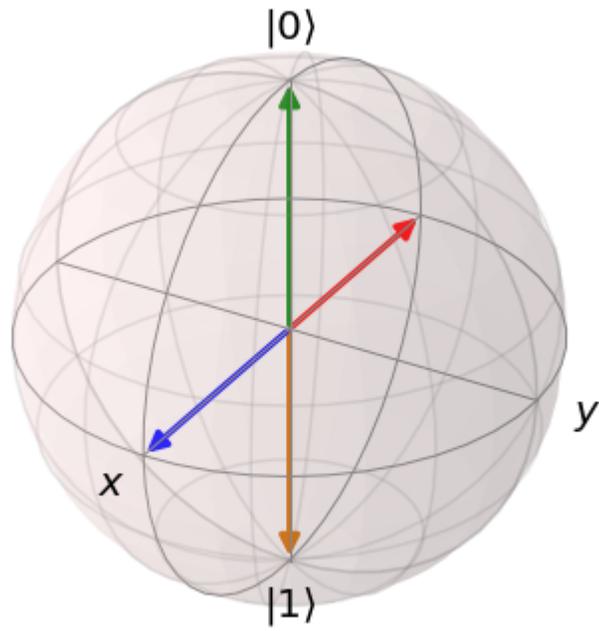
$$|\psi\rangle = |1\rangle$$



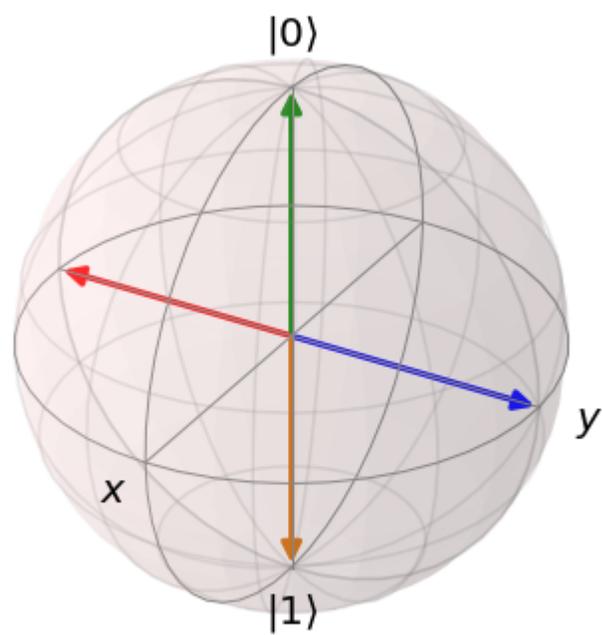
Superposition $|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$



$|+\rangle$ and $|-\rangle$



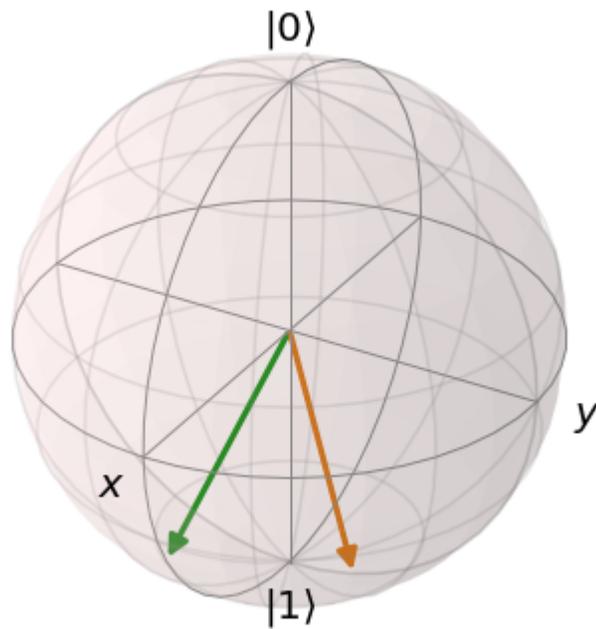
$|i\rangle$ and $|-i\rangle$



Another superposition:

$$|\psi\rangle = R_{\pi/3} |0\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle; P(0) = 1/4, P(1) = 3/4$$

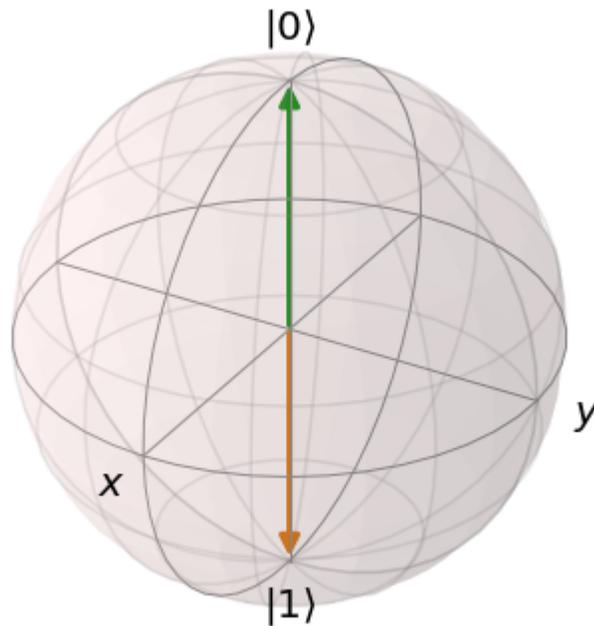
And add a phase... $|\psi'\rangle = \frac{1}{2}|0\rangle + \sqrt{\frac{3}{8}}(1+i)|1\rangle$



Transform states with *gates*. One-qubit gates include the Pauli gates:

$$\text{Pauli X: } \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \text{Pauli Y: } \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \text{Pauli Z: } \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

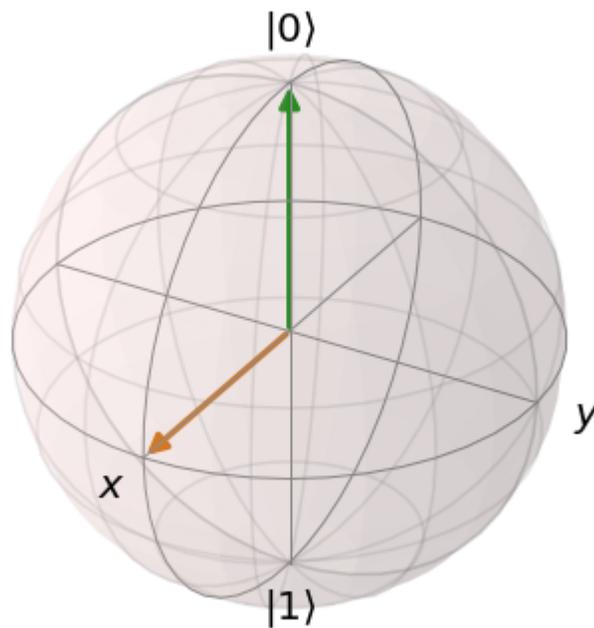
They just reflect about axes. Can also do with rotations. σ_x is also the NOT gate and is $(R_{\pi/4})^2$



An extremely important gate is the *Hadamard* gate... $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

It will put qubits into and out of the superposition state.

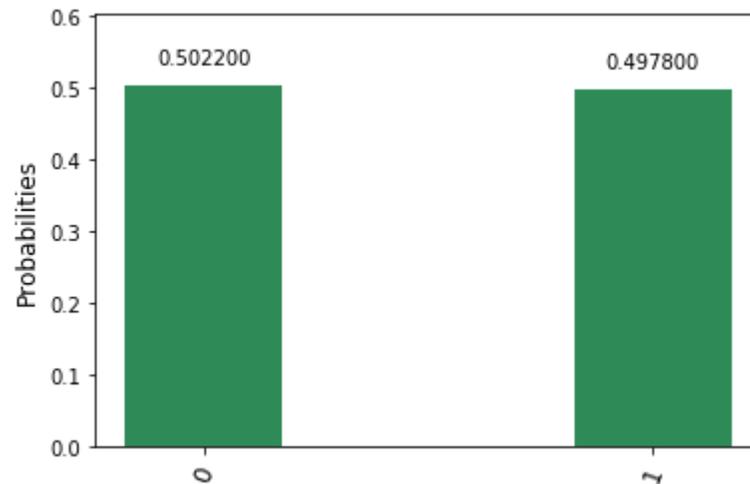
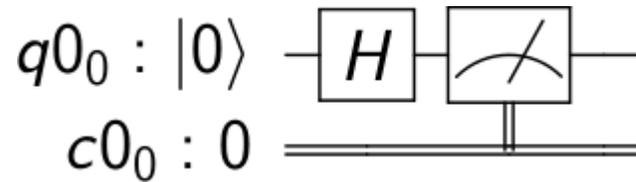
$$H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle, H |+\rangle = |0\rangle, H |1\rangle = |-\rangle, H |-\rangle = |1\rangle$$



A *circuit* is a series of gates on one or more qubits. Time goes to the right. The measurements are assumed to take place in the $|0\rangle, |1\rangle$ basis.

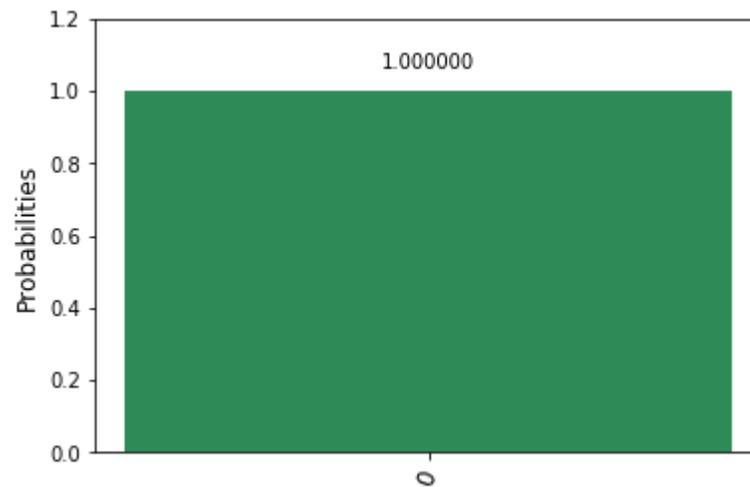
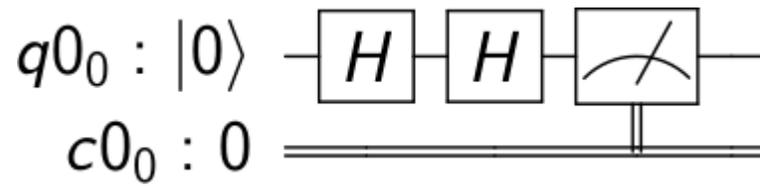
Let's do a Hadamard gate and measure the outcome.

Out[10]:



Let's try two...

Out[12]:



One qubit circuits are kinda boring. Add more qubits!

$$|\psi\rangle = |\text{qubit \#1 state}\rangle \otimes |\text{qubit \#2 state}\rangle$$

We'll use an efficient notation, e.g., $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |0, 0\rangle = |00\rangle$

$$|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle \dots \text{in vector form } \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}_{11}^{00}$$

Probability of, say, both qubits measure to be in 0 state, is $|\alpha|^2$

Probability of measuring the first qubit in the 0 state is $|\alpha|^2 + |\beta|^2$

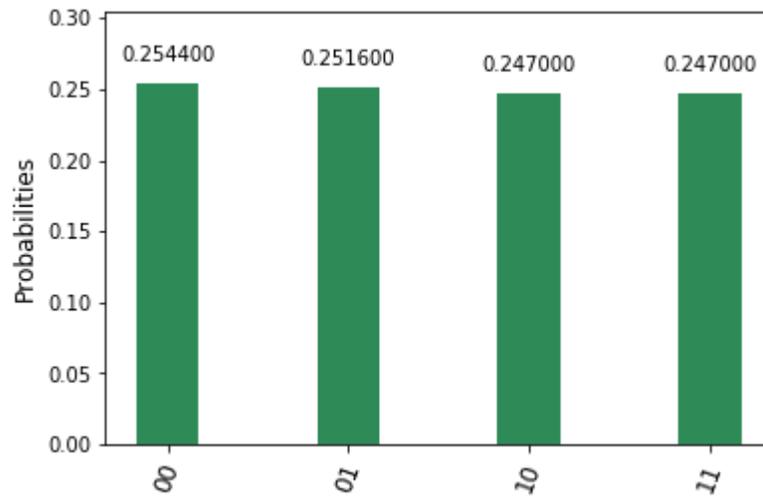
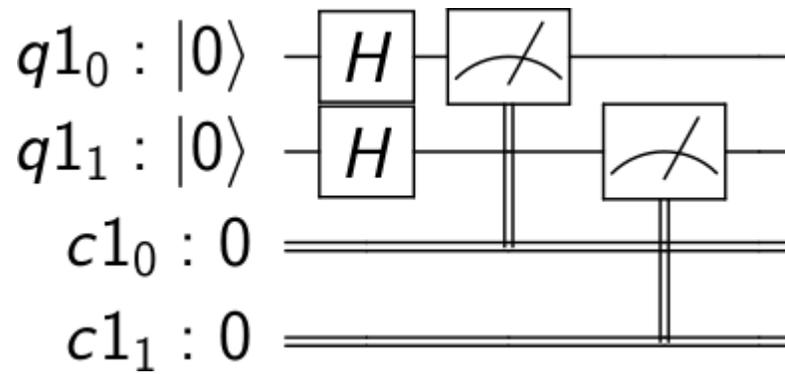
Probability of measuring the first qubit in the 1 state is $|\gamma|^2 + |\delta|^2$

If we measure the first qubit to be in 0, what is the state of the system now?

$$|\psi\rangle = |0\rangle \otimes \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}}$$

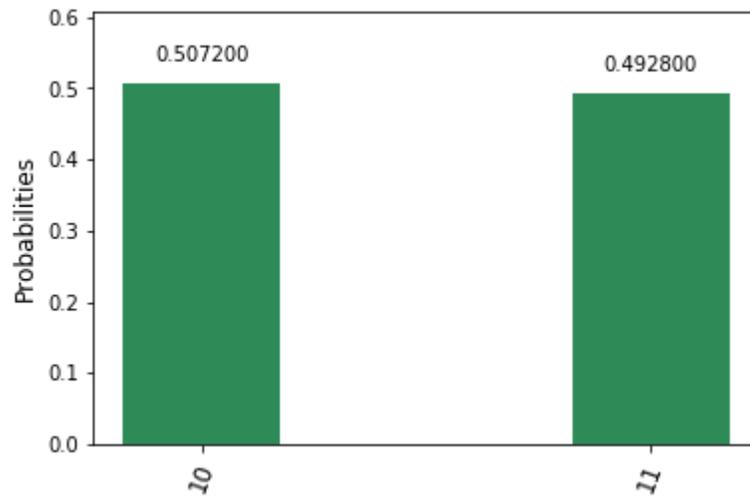
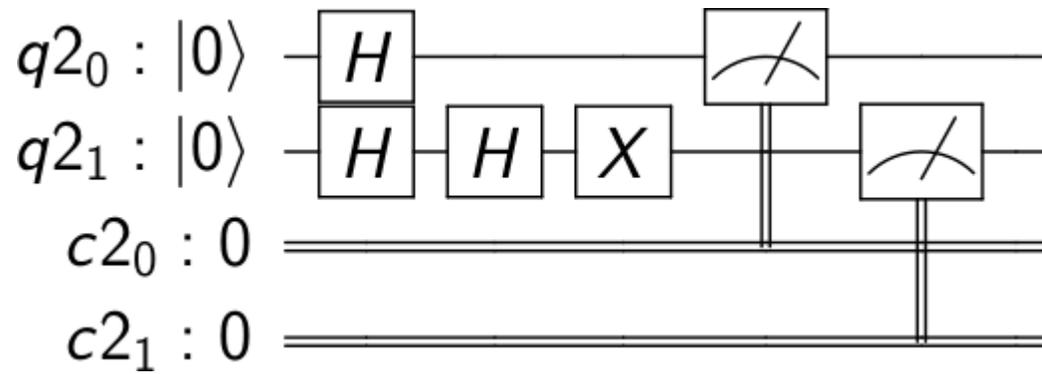
Let's make a full superposition

Out[14]:



A little more fancy (but kinda dumb)...

Out[16]:



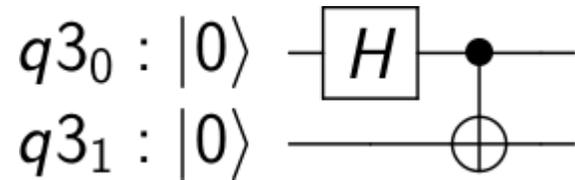
Qubits can "interact" via certain gates ... The *Controlled Not* (CNOT) gate (CX)...

Flip the second bit (target) if the first bit (control) is 1

$$CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

We've seen this before with the coins. There's CY, CZ, CPhase too.

Out[18]:



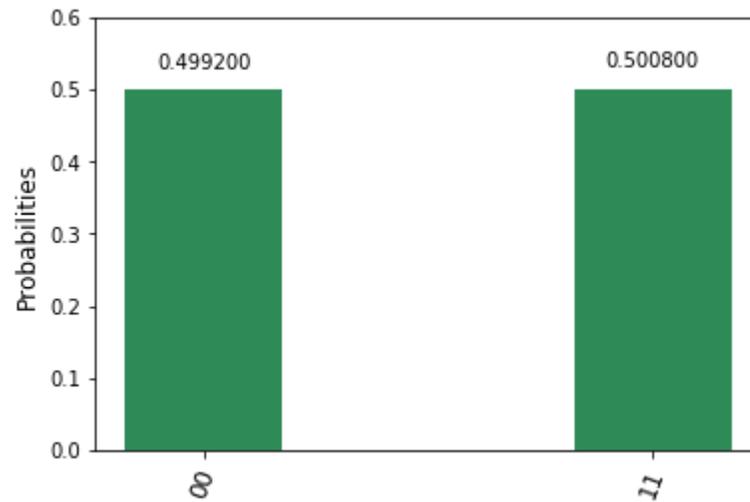
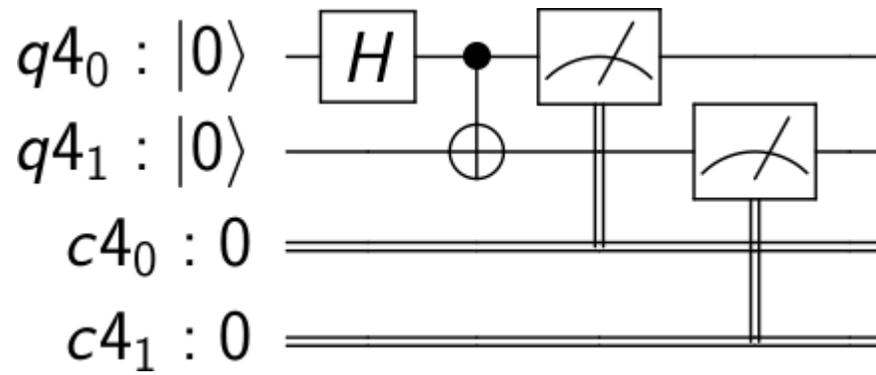
$$|00\rangle \rightarrow \frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

Final state is a Bell Pair (or EPR Pair) and is fully entangled (not decomposable into a tensor product). If you know one qubit, you know the other.

Let's try it

Out[19]:



Remember - we've looked at ideal quantum computers (no noise)

That's it from me.

There are more gates (e.g. parameterized rotations, controlled pauli gates, 3 qubit gates)

There are more rules and more stuff (sorry - wish I had time to write up an algorithm)

...but on to Cirq...