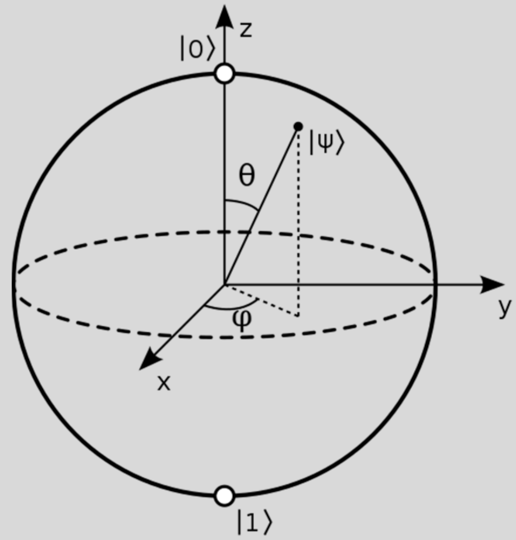


Quantum Gates, Circuits, and Algorithms

ECE 592/CSC 591 – Fall 2018

NC STATE UNIVERSITY Electrical & Computer Engineering

@NCStateECE

Quantum State (qubit)

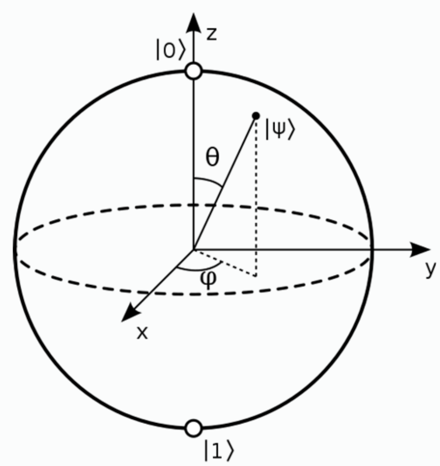
Mathematically represented as a vector, or a point on the surface of the Bloch sphere:

$$|\psi\rangle = \underbrace{\cos\left(\frac{\theta}{2}\right)}_{\alpha}|0\rangle + \underbrace{e^{i\varphi}\sin\left(\frac{\theta}{2}\right)}_{\beta}|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

Measurement = projection of state to a basis vector (changes the state – superposition is destroyed)

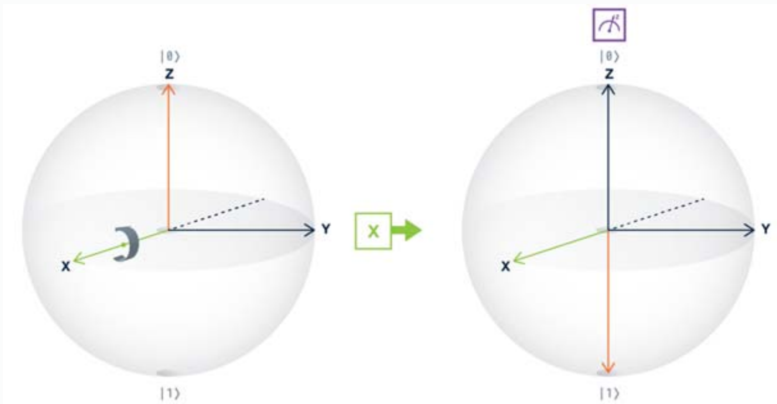
Quantum gate is a transformation from one qubit state to another. Single-qubit gate = rotation around Bloch sphere. Reversible. Represented by a matrix (unitary, ...) acting on the vector.

NOTE: There are many possible basis vector sets – any antipodal points on the Bloch sphere are orthogonal. "Standard" basis is {|0⟩,|1⟩}.



https://en.wikipedia.org/wiki/Bloch_sphere

X Gate: NOT

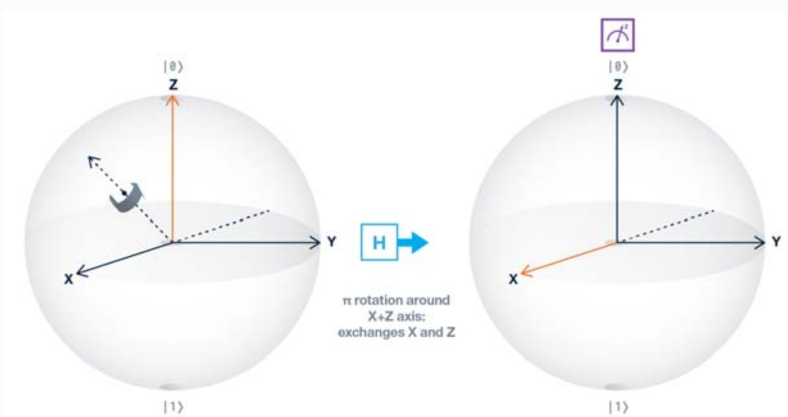


Start	End
$\lvert 0\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 0\rangle$
$\alpha\lvert 0\rangle + \beta\lvert 1\rangle$	$\beta\lvert 0\rangle + \alpha\lvert 1\rangle$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X\lvert 0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Hadamard (H) Gate: Superposition

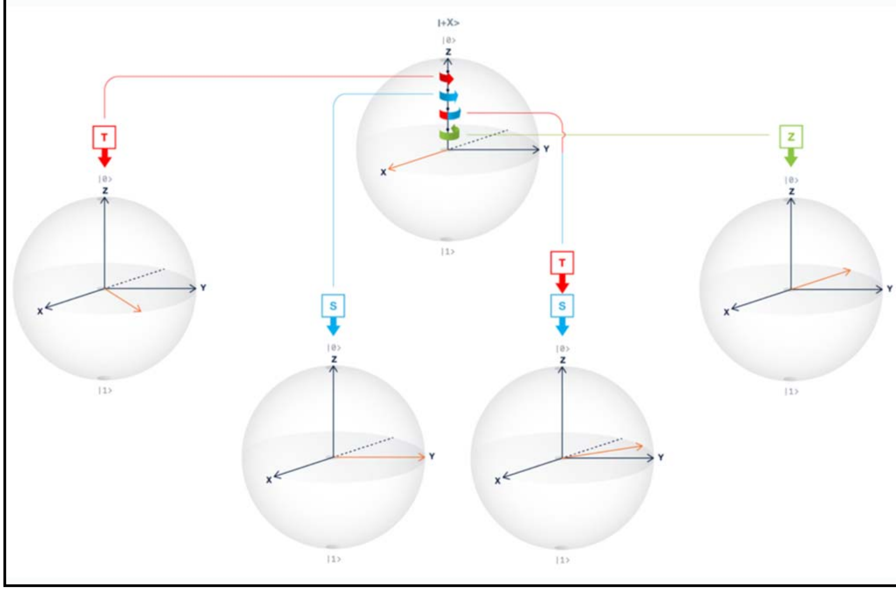


Start	End	AKA
$\lvert 0\rangle$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$	$\lvert +\rangle$
$\lvert 1\rangle$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)$	$\lvert -\rangle$

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$H\lvert 0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Phase: Z, S, T



Rotations around the Z axis

T = π/4
S = π/2
Z = π

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Phase: Z, S, T

Gate sequence	Rotation around Z	Probability of 0	Probability of 1
H H	0	1.0	0
H T H	$\pi/4$	0.85	0.15
H S H	$\pi/2$	0.50	0.50
H S T H	$3\pi/4$	0.15	0.85
H Z H	π	0	1

Create +X | Change qubit | Measure in

U Gates: u1, u2, u3

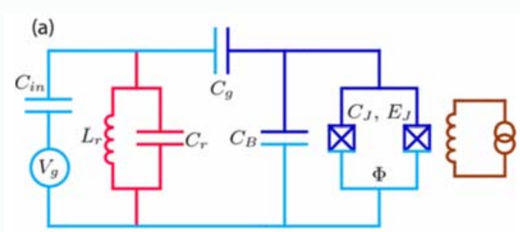
The most general unitary gate	IBM Gate	Used to generate…
$U(\theta,\varphi,\lambda)=\begin{pmatrix}\cos(\theta/2) & -e^{i\lambda}\sin(\theta/2)\\ e^{i\varphi}\sin(\theta/2) & e^{i\lambda+i\varphi}\cos(\theta/2)\end{pmatrix}$	u3(□,φ,λ)	
$U(0,0,\lambda)=\begin{pmatrix}1 & 0\\ 0 & e^{i\lambda}\end{pmatrix}$	u1(λ)	T, T†, S, S†, Z
$U(\pi/2,\varphi,\lambda)=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -e^{i\lambda}\\ e^{i\varphi} & e^{i\lambda+i\varphi}\end{pmatrix}$	u2(φ,λ)	H = u2(0,π)

A word about implementation…

Quotes from IBM Q material

The qubit we use is a fixed-frequency superconducting transmon qubit. It is a Josephson-junction-based qubit that is insensitive to charge noise.

The devices are made on silicon wafers with superconducting metals such as niobium and aluminum.



Koch, et al.
Phys. Rev. A **76**, 042319 –Oct 2007

Quantum gates are performed by sending electromagnetic impulses at microwave frequencies to the qubits through coaxial cables. These electromagnetic pulses have a particular duration, frequency, and phase that determine the angle of rotation of the qubit state around a particular axis of the Bloch sphere.

Multi-Qubit States

There are 2^n basis vectors for an *n*-qubit system. In the standard basis, these are:

$$|00\ldots000\rangle, |00\ldots001\rangle, |00\ldots010\rangle, \ldots, |11\ldots111\rangle$$

Also written as:

$$|0\rangle_n, |1\rangle_n, |2\rangle_n, \ldots, |x\rangle_n \ldots, |2^n - 1\rangle_n$$

A particular state is a superposition of the basis vectors:

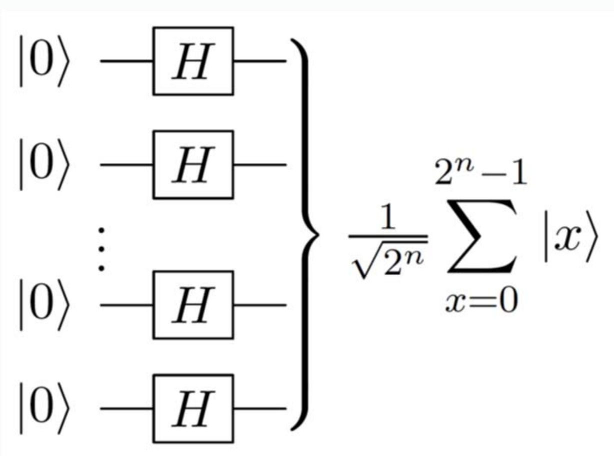
$$\sum_i \alpha_i |x_i\rangle, \; where \sum_i |\alpha_i|^2 = 1$$

For <u>many</u> states, we can no longer identify the pure state of an individual qubit.
These are known as entangled states.

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

There is no tensor product $|a\rangle \otimes |b\rangle$ that corresponds to this state.

Walsh-Hadamard Transform

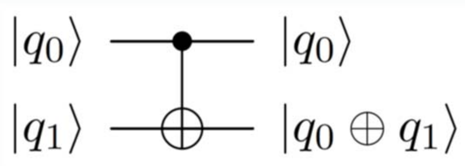


Used in the setup phase of algorithms, to create a **superposition of all inputs**.

Transformations occur on all components of the superposition. This is the source of **quantum parallelism**.

Two-qubit Gate: CNOT

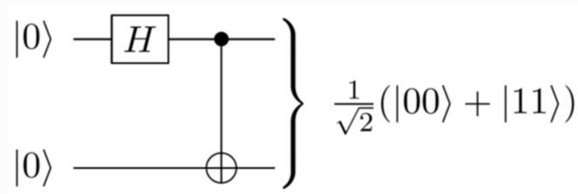
CNOT = controlled-NOT



Start	End
$\lvert 00\rangle$	$\lvert 00\rangle$
$\lvert 01\rangle$	$\lvert 11\rangle$
$\lvert 10\rangle$	$\lvert 10\rangle$
$\lvert 11\rangle$	$\lvert 01\rangle$

Be careful about notions of "control" and "target."
More about this later…

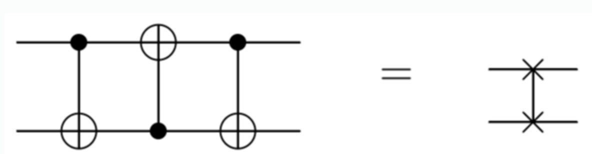
Entanglement: Bell Pair



There is no tensor product
$|a\rangle \otimes |b\rangle$
that corresponds to this state.

Other Two-Bit Gates (IBM Qiskit)

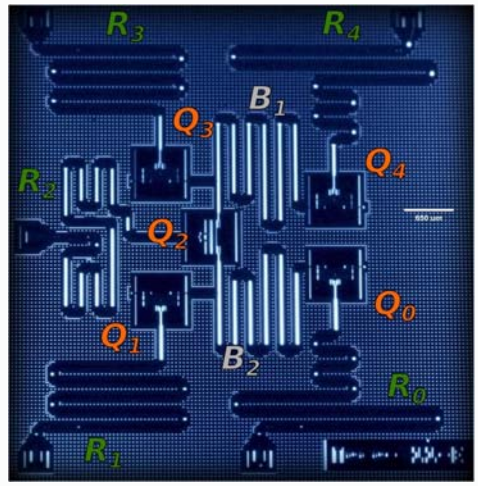
- controlled Pauli gates (X, Y, Z) – controlled X is CNOT
- controlled Hadamard gate
- controlled rotation gates (Rx, Ry, Rz)
- controlled phase gate (u1)
- controlled u3 gate
- swap gate



A word about implementation…

Quotes from IBM Q material

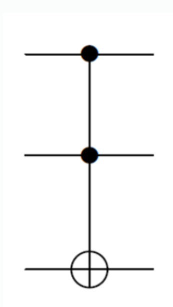
Two-qubit gates typically require tuning to calibrate the interaction between the two qubits during the gate duration, and minimizing the interaction at any other time. Since our qubits of choice are fixed-frequency transmons, we cannot tune the interaction by bringing them closer in frequency during the two-qubit gate. Instead, we exploit the cross-resonance effect, by driving one of the qubits (called control) with a microwave pulse tuned at the frequency of the second qubit (called target). By doing this, we can actively increase the strength of the coupling between them. The nature of the cross-resonance effect also allows us to perform rotations in the target qubit conditioned on the state of the control qubit, a key characteristic of the CNOT operation required for a universal quantum gate set.



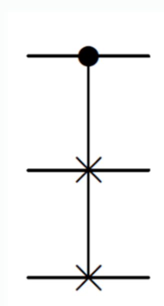
Hegade, et al. arXiv:1712.07326v1, 9 Jul 2018.

Three-qubit Gates

Toffoli: controlled CNOT

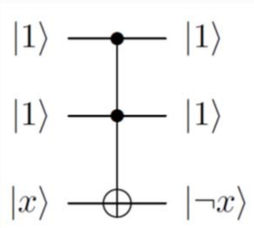


Fredkin: controlled swap

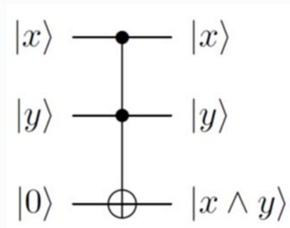


These are not implemented directly on the IBM Q. They are built from 1- and 2-qubit gates.

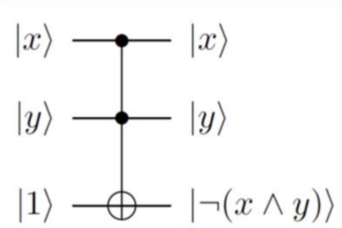
Toffoli: Reversible Classic Gates



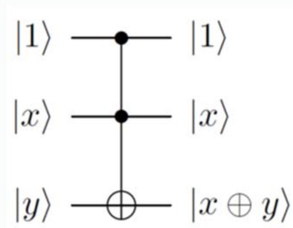
NOT



AND



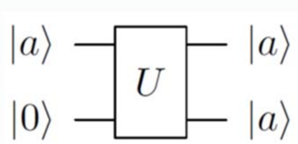
NAND



XOR

No-Cloning Principle (revisited)

Suppose we have a cloning transformation U, such that $\boldsymbol{U(|a\rangle|0\rangle) = |a\rangle|a\rangle}$ for any quantum state $|a\rangle$.



Let $|a\rangle$ and $|b\rangle$ be two orthogonal quantum states. Therefore,

$$U(|a\rangle|0\rangle) = |a\rangle|a\rangle$$
$$U(|b\rangle|0\rangle) = |b\rangle|b\rangle$$

Consider $|c\rangle = \frac{|a\rangle+|b\rangle}{\sqrt{2}}$.

By linearity:

$$U(|c\rangle|0\rangle) = \frac{1}{\sqrt{2}}\big(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)\big)$$
$$= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle)$$

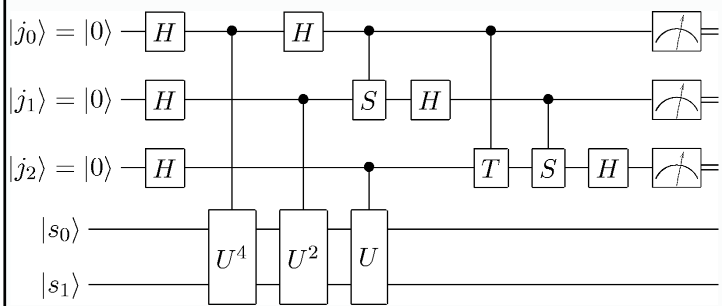
$$\neq$$

By definition of cloning transformation:

$$U(|c\rangle|0\rangle) = |c\rangle|c\rangle$$
$$= \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle) \otimes \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$$
$$= \frac{1}{2}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle)$$

These are not equal $\Rightarrow$ there is no U for which both can be true.

Quantum Circuit



Measurement.
Double line represents classical bit.

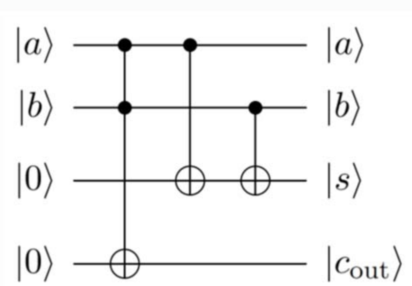
Time flows left to right.
Quantum gates (operators) are applied sequentially to qubit states, with result shown on the right.

Standard Circuit Model

- CNOT plus all single-bit transformations
- Measurement in the standard basis

Any quantum transformation can be realized in terms of the basic gates of the standard circuit model.

Example Circuit: Half Adder



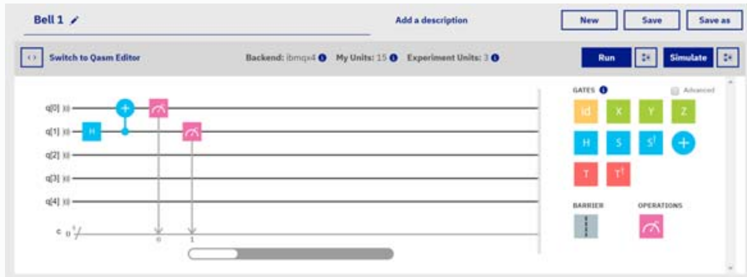
Start $\|ab00\rangle$	End $\|absc\rangle$
$\|0000\rangle$	$\|0000\rangle$
$\|0100\rangle$	$\|0110\rangle$
$\|1000\rangle$	$\|1010\rangle$
$\|1100\rangle$	$\|1101\rangle$

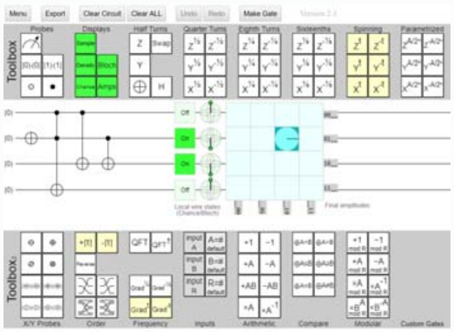
Using the standard basis states $|0\rangle$ and $|1\rangle$, this is a binary half adder.
What if the input qubits are general?

What if input is $|+000\rangle$? What would you expect if you measure all output qubits?

Experimenting with Circuits

- IBM Q Experience: Composer
- IBM Qiskit
- Quirk





Caution 1: Phases

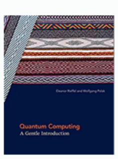
Quantum state transformations are specified in terms of actions in the vector space, not in terms of quantum state. (There's a difference.) Example – consider the controlled phase shift:

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to e^{i\theta}|10\rangle$$
$$|11\rangle \to e^{i\theta}|11\rangle$$

$|10\rangle$ and $e^{i\theta}|10\rangle$ represent exactly the same state. So is this equivalent to the identity transformation? No.

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

These are different states due to the relative phase.

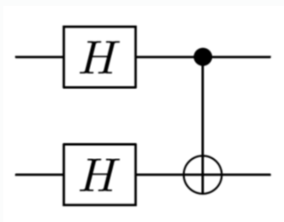


Rieffel and Polak, 2014.

Caution 2: Notion of Control

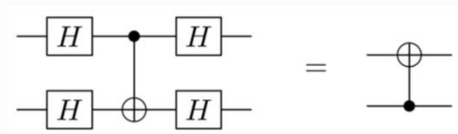
The notions of **control** and **target** bit is a carryover from the classical gate, and should not be taken too literally. Do not conclude that the control bit is never changed.

Consider the CNOT gate operating in the Hadamard basis:



Start	End
$\vert ++\rangle$	$\vert ++\rangle$
$\vert +-\rangle$	$\vert --\rangle$
$\vert -+\rangle$	$\vert -+\rangle$
$\vert --\rangle$	$\vert +-\rangle$

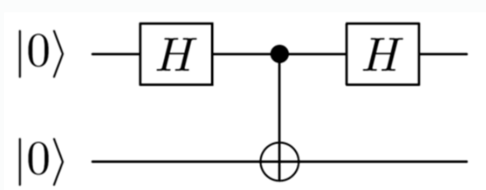
In this case, it's the first qubit that changes.



Caution 3: Reading Circuit Diagram

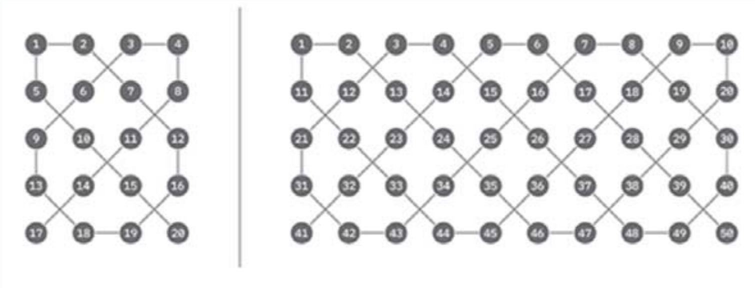
The graphical representation of a circuit can be misleading. Must "do the math" and figure out exactly what transformation is happening, even if all qubits are in the standard basis.

What is the output of the following circuit?



Because the H gate is its own inverse, you might think that the first qubit will be unchanged.
But the output is $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$ -- not obvious from the diagram.

Limited Connectivity



IBM Q (and other machines) do not provide full connectivity among qubits.
Can't arbitrarily perform CNOT between any two qubits.
Careful planning, using SWAP to move qubit state where it is needed. (Can't copy!)

https://www.ibm.com/blogs/research/2017/11/the-future-is-quantum/

Next Steps

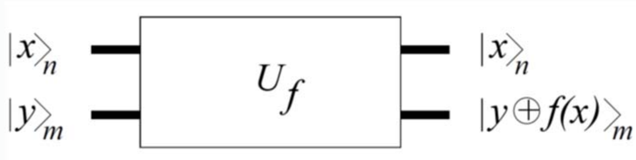
- Efficient quantum implementations of classical functions
  - Create reversible classical circuits
  - Convert to quantum
  - Undo entanglement

- Quantum algorithms

Quantum Parallelism

A typical transformation U_f :

$$U_f: |x, 0\rangle \rightarrow |x, f(x)\rangle$$



When this acts on a superposition,
it acts on each element of the superposition:

$$U_f: \sum_x a_x |x, 0\rangle \rightarrow \sum_x a_x |x, f(x)\rangle$$

But if you measure $|x, f(x)\rangle$, you're only going to get one value.
So have to do other things to make this useful.

Quantum Algorithm Strategies

Create superposition of states (quantum parallelism)

Apply transforms that amplify desirable values and diminish unwanted values

- Measure to get desired value with high probability.
  - Typically, execute many times ("shots") to identify high-probability value(s).
- Repeat calculation to learn about relationships among values.
- Measurements can yield information about the properties of values