A Very Quick Intro to Quantum Computing

John Lindsay Orr

March 7, 2019

Why do we care? (Reason 1)

RSA cryptography relies on the belief that finding a non-trivial factor of a large number N is (essentially) $O(N)$.

In 1994 Peter Shor presented an algorithm which found a factor of N using a quantum circuit in (essentially) $O(\log N)$ steps.

Why do we care? (Reason 2)

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

– Richard Feynman, 1982

Why do we care? (Reason 3)

Quantum Mechanics and Computer Science are arguably the two biggest discoveries of the 20th century, so combining them may give wonderful insights, e.g., quantum graviation via quantum error correcting codes?

What is a qubit?

A **qubit** is the smallest unit of quantum information.

In classical information theory a bit is a single 0 or 1 and is the state of some classical (electrical) system.

In quantum information theory a qubit is the state of a quantum system which is represented as vectors in the complex vector space $\mathbb{C}^2$.

I.e., there are two measurable states:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{and} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

What is a qubit?

Think of the qubit as the spin (up/down) of a particle on a fixed axis or as polarization (vert/horiz) of a photon.

The key difference between quantum and classical state is that a particle can be in a **superposition** which mathematically is just a linear combination of the two base states.

E.g.,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Remember α and β are *complex* numbers.

What is a qubit?

So Schrödinger's Cat is just a superposition of two states (alive/dead);

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}|\text{alive}\rangle + \frac{1}{\sqrt{2}}|\text{dead}\rangle$$

What a sec — where did those square roots come from?

What is a qubit?

If a particle is in a superposition state $\alpha|0\rangle + \beta|1\rangle$ then you can never directly access α and β.

The **Born Rule** says that when you measure the state you get either $|0\rangle$ or $|1\rangle$ with probability:

$$P(\text{measured } |0\rangle) = |\alpha|^2$$
$$P(\text{measured } |1\rangle) = |\beta|^2$$

For this to be valid we need $|\alpha|^2 + |\beta|^2 = 1$ so I should have said earlier that qubits are always *unit vectors in* $\mathbb{C}^2$.

Let's see a qubit superposition

Here is one interpretation of the effect of polarizing filters

- $(0°, 0°)$ and $(0°, 0°, 0°)$ — Show that $0°$ *prepares* photons in state $|0°\rangle$ and that they stay in that state.
- $(0°, 90°)$ — Shows that $90°$ filters out *all* the photons in state $|0°\rangle$.
- $(0°, 45°, 90°)$ and $(0°, 45°, 45°, 90°)$ — Show that passing through $45°$ puts the photons in a superposition of $|0°\rangle$ and $|90°\rangle$

Complex systems

We saw the state of a single qubit is a unit vector in $\mathbb{C}^2$. In general the state of a more complex system is a unit vector in an n-dimensional complex vector space (aka Hilbert space).

If your system is a pair of qubits then the Hilbert space for the joint state is $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.

If your system consusts of n qubits then the Hilbert space for the joint state is $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{(2^n)}$.

Complex systems

In a system of two qubits, if Bit-1 is in state

$$|\psi_1\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}$$

and Bit-2 is in state

$$|\psi_2\rangle = \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}$$

then the joint system is in state

$$|\psi_1\rangle|\psi_2\rangle = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix}$$

(Not all joint states are of this form. . . see **entanglement** later!)

What is a quantum computer?

A quantum computer consists of a closed set of n qubits that start in a specifified state (conventionally $|00\ldots0\rangle$), together with a set of steps (called *gates*) which transform them to a final state.

In general all transformations of a closed system are **unitary** operators, i.e., matrices U satisfying $UU^\dagger = U^\dagger U = I$.

E.g.,

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{or} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The art of quantum computing is to build interesting transformations as the matrix product of an "instruction set" of specified "standard" operations.

The quantum NOT gate

Consider the single-qubit operation

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

Remember the state of our qubit is a linear combination of

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{and} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

So

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

and, likewise,

$$X|1\rangle = |0\rangle$$

hence the name NOT.

The quantum NOT gate

So the quantum NOT gate flips classical state. But remember quantum state is

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

so that on a general state, by linearity,

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

The Hadamard gate

The **Hadamard gate**

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

maps

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

So this takes a qubit prepared in standard state $|0\rangle$ and puts it in a superposition of $|0\rangle$ and $|1\rangle$ where the probability of measuring either 0 or 1 is $1/2$.

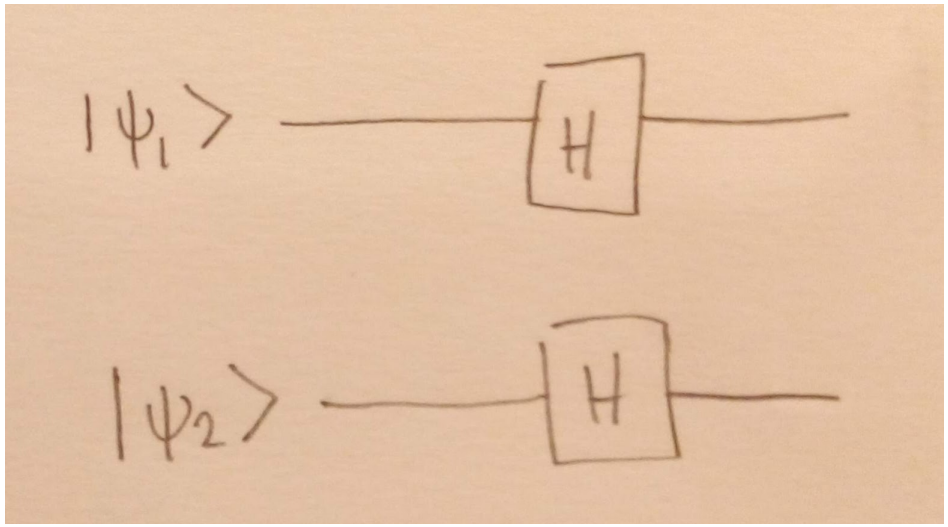
(In other words this is the process that creates a Schrödinger's cat!)

A two-qubit gate

Recall states in a two-qubit system are unit vectors in $\mathbb{C}^4$, and if Bit-1 and Bit-2 are independently $|\psi_1\rangle$ and $|\psi_2\rangle$ then the system is in state $|\psi_1\rangle|\psi_2\rangle$. So we can have a unitary operator defined by acting on Bit-1 and Bit-2 independently by H. I.e.

$$|\psi_1\rangle|\psi_2\rangle \longmapsto |H\psi_1\rangle|H\psi_2\rangle$$

(Not all vectors in $\mathbb{C}^4$ are of the form $|\psi_1\rangle|\psi_2\rangle$, but the ones which are, span $\mathbb{C}^4$, and this is enough.)



Another two-qubit gate

We can use the same ideas to define another two-qubit gate. Let $f : \{0,1\} \to \{0,1\}$ be a fixed function (only 4 possibilities!).

For each $i, j \in \{0,1\}$ define

$$U_f|i\rangle|j\rangle = |i\rangle|f(i)+j\rangle$$

So for example if we had taken $f(0) = 1$ and $f(1) = 0$, then

$$\begin{aligned} U_f|00\rangle &= |01\rangle, \\ U_f|01\rangle &= |00\rangle, \\ U_f|10\rangle &= |10\rangle, \\ U_f|11\rangle &= |11\rangle \end{aligned}$$

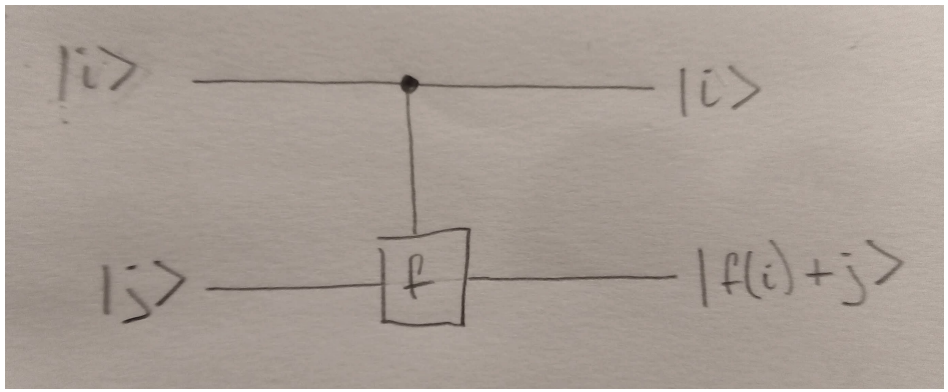
(All this is, is a permutation of the standard basis of $\mathbb{C}^4$.)

Another two-qubit gate

We can use the same ideas to define another two-qubit gate. Let $f : \{0,1\} \to \{0,1\}$ be a fixed function (only 4 possibilities!).

For each $i, j \in \{0,1\}$ define

$$U_f|i\rangle|j\rangle = |i\rangle|f(i)+j\rangle$$



Deutsch's Algorithm – let's compute!

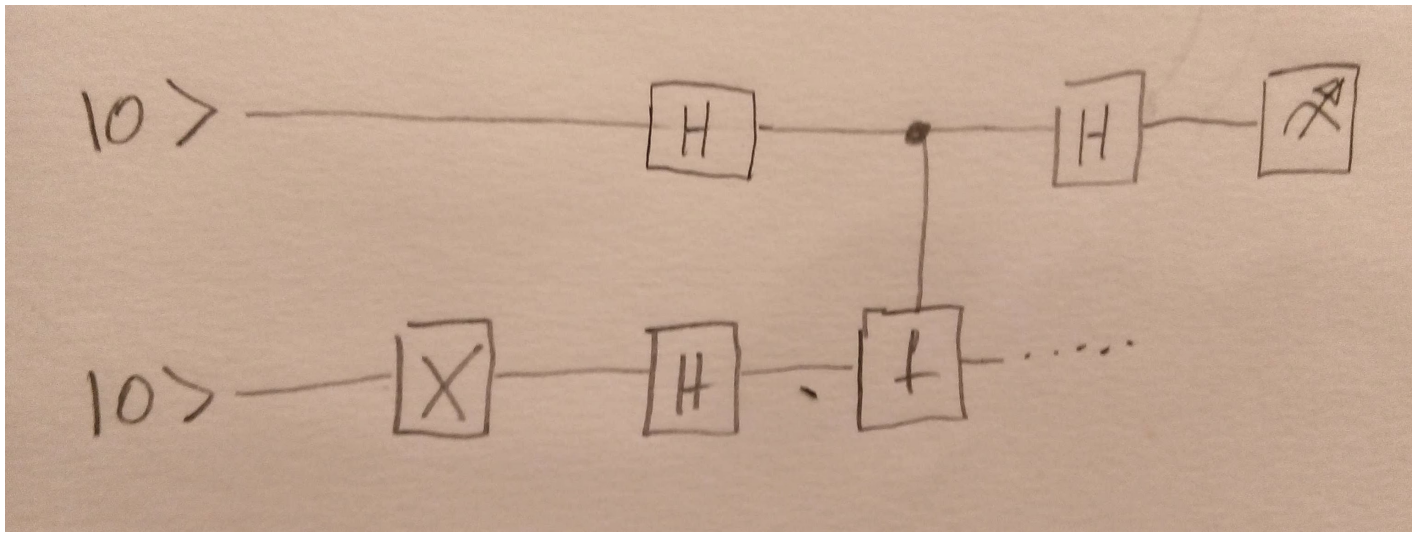
Suppose you have an *oracle* – a black-box function – which in this case is incredibly simple, it's just that funtion

$$f : \{0, 1\} \to \{0, 1\}$$

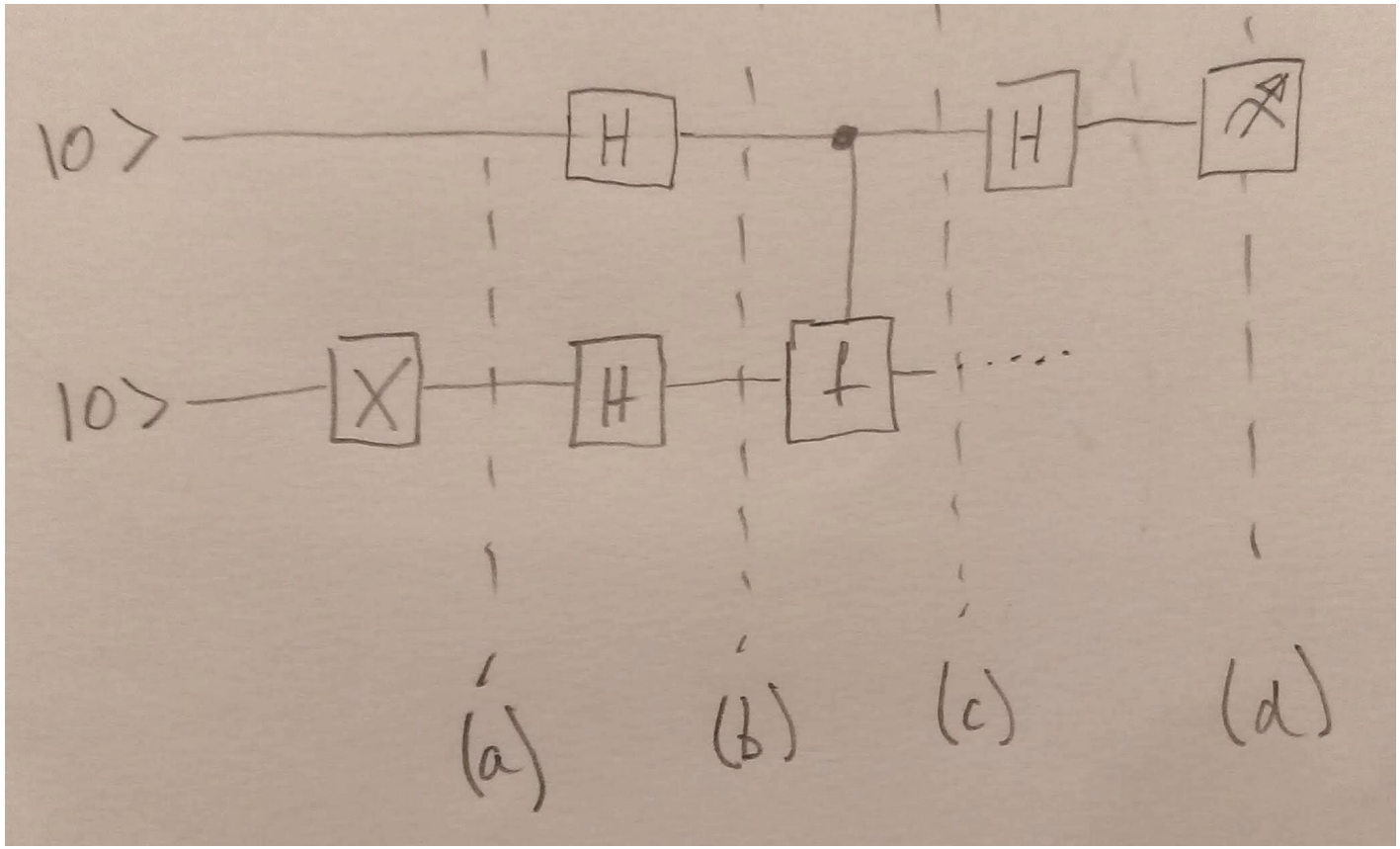
and you want to know, does it always return the same answer or not? (In other words, does $f(0) = f(1)$ or not?)

Question: How many times do you need to evaluate f?

Deutsch's Algorithm – let's compute!



Deutsch's Algorithm – let's compute!



Deutsch's Algorithm – step (a)

The state was

$$|0\rangle|0\rangle$$

and now the state is

$$|0\rangle|1\rangle$$

Deutsch's Algorithm – step (b)

The state was

$$|0\rangle|1\rangle$$

and now the state is

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

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

Deutsch's Algorithm – step (c)

The state was

$$\frac{1}{2}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle(|0\rangle - |1\rangle)$$

and now the state is

$$\frac{1}{2}|0\rangle(|f(0)+0\rangle - |f(0)+1\rangle) + \frac{1}{2}|1\rangle(|f(1)+0\rangle - |f(1)+1\rangle)$$

Deutsch's Algorithm – step (c)

But now for a clever trick:

$$|f(0)+0\rangle - |f(0)+1\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)$$

and likewise

$$|f(1)+0\rangle - |f(1)+1\rangle = (-1)^{f(1)}(|0\rangle - |1\rangle)$$

so that the state at step (c) becomes

$$\frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)$$

and since $(-1)^{f(1)} = (-1)^{f(0)}(-1)^{f(0)+f(1)}$ we get

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)+f(1)}|1\rangle)(|0\rangle - |1\rangle)$$

Deutsch's Algorithm – step (d)

Finally we throw away Bit-2 and apply H to Bit-1. The state of Bit-1 was

$$\frac{1}{\sqrt{2}}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)+f(1)}|1\rangle)$$

Case 1: If $f(0) = f(1)$ then this is $|0\rangle + |1\rangle$ and H maps it to $|0\rangle$, so we measure 0 with 100% probability.

Case 2: If $f(0) \neq f(1)$ then this is $|0\rangle - |1\rangle$ and H maps it to $|1\rangle$, so we measure 1 with 100% probability.

Deutsch-Jozsa Algorithm

Given a function $f : \{0,1\}^n \to \{0,1\}$ which is promised to be either *constant* or *balanced*, determine which is which.

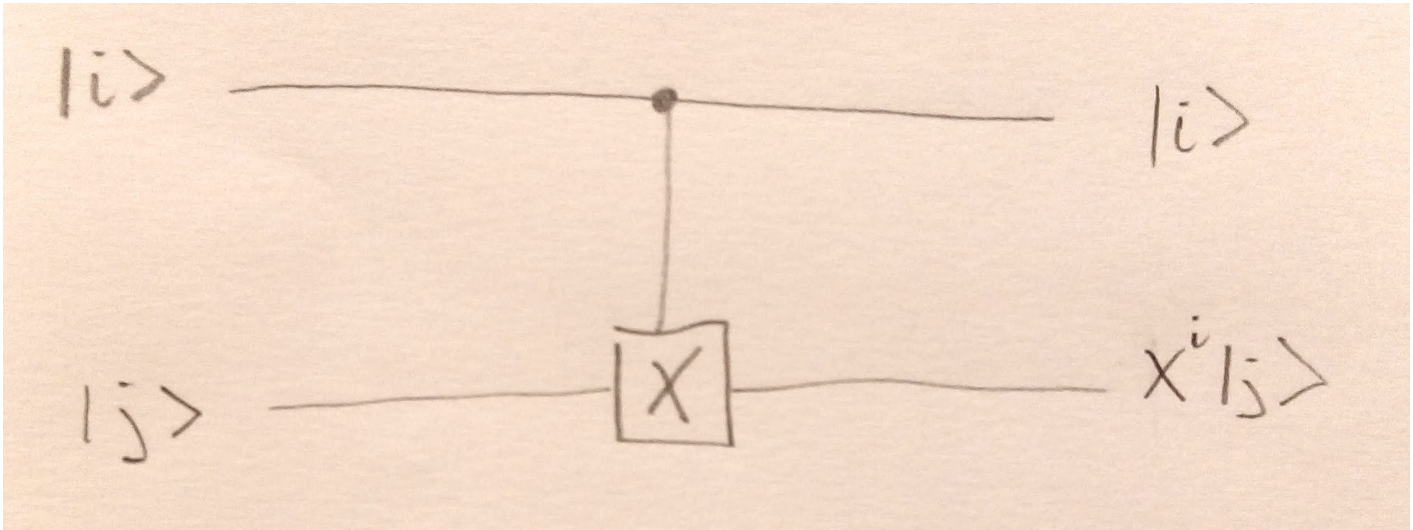
Any **classical** algortihm must make worst-case $2^{n-1} + 1$ evaluations.

The **Deutsch-Jozsa Algorithm** requires a **single** evaluation of f.

Entanglement

Consider the quantum gate on two qubits defined by

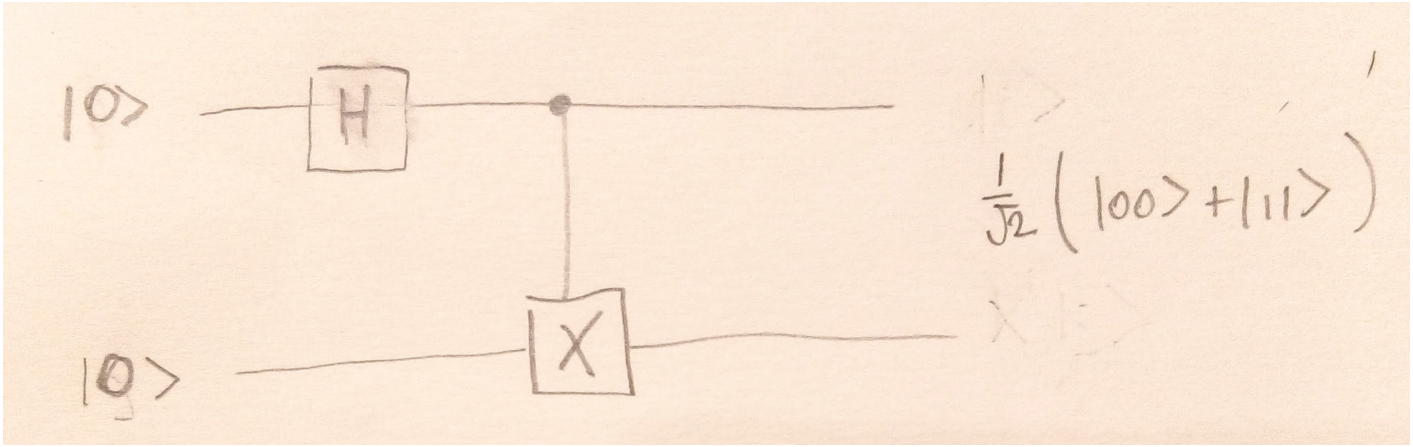
$$U|0\rangle|\psi\rangle = |0\rangle|\psi\rangle \qquad \text{and} \qquad U|1\rangle|\psi\rangle = |1\rangle(X|\psi\rangle)$$



This is called the *controlled-NOT* or CNOT gate.

Entanglement

Using a CNOT gate we can prepare two qubits as an "EPR pair"



Note that the state

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

cannot be written in the form $|\psi_1\rangle|\psi_2\rangle$ and so Bit-1 and Bit-2 are *entangled*.

Entanglement

If

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

then, if we measure Bit-1 there is a 50% chance of getting 0 and 50% chance of getting 1. But if we then measure Bit-2, then we must **always** get the same result as for Bit-1. I.e., the results of measuring Bit-1 and Bit-2 are perfectly correlated.

Quantum teleportation