Sean Carroll, seancarroll@gmail.com

125c, Lecture Fifteen : 5/22/17

We can use the vocabulary of quantum circuits to discuss an important process:

Quantum Teleportation.

Here's the setup: Alice has a qubit, $|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$, but she doesn't know α & β. She wants to send this qubit to her friend Bob, who is some distance away. She can send classical information to Bob, no problem, but she can't send the physical qubit itself. Nor can she just measure the qubit; that projects $|\psi\rangle_A$, destroying the information about α & β. Nor can she clone it! What to do?

Fortunately, Alice & Bob have planned ahead — they share an entangled EPR pair, in a Bell state

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

So the total state they start with is

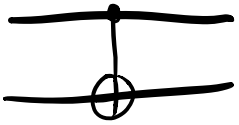
$$|\Psi_0\rangle = |\psi\rangle_A |\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}\left[(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)\right].$$

Some gates we have to work with:

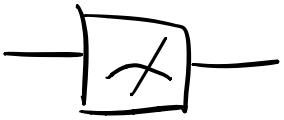
$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ (Hadamard)

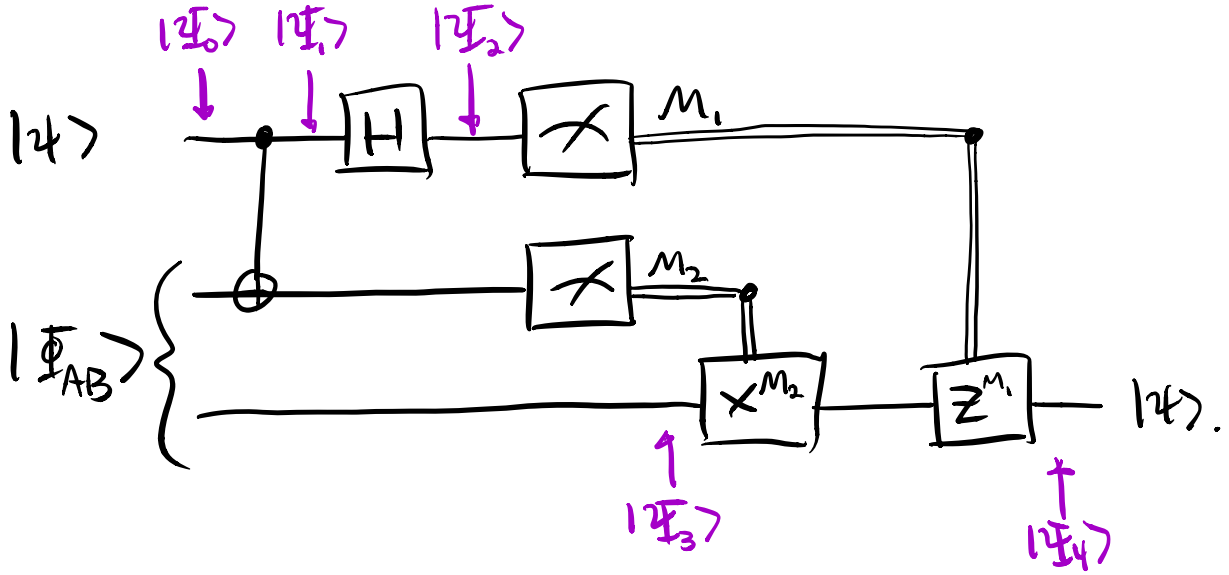


$$= \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$ (CNOT)



$$= \begin{cases} |0\rangle \\ |1\rangle \end{cases}$$ (measurement)

Alice can teleport the information in her qubit to Bob via the following quantum circuit:



Double lines = flow of classical information.

Let's follow what happens. First the state goes through a CNOT, flipping the second qubit when the first is a 1. This gives

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\right].$$

Then the first qubit goes through a Hadamard, yielding

$$|\Psi_2\rangle = \frac{1}{2}\Big[\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle) + \beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)\Big]$$

$$= \frac{1}{2}\Big[\alpha(|000\rangle+|011\rangle+|100\rangle+|111\rangle) + \beta(|010\rangle+|001\rangle-|110\rangle-|101\rangle)\Big].$$

Now Alice measures her two qubits. Post-measurement, she has two bits of classical info (M_1 & M_2), and Bob still has some qubit, $|\Psi_3\rangle$:

M_1 M_2	$\|\Psi_3\rangle$
0 0	$\alpha\|0\rangle + \beta\|1\rangle$
0 1	$\alpha\|1\rangle + \beta\|0\rangle$
1 0	$\alpha\|0\rangle - \beta\|1\rangle$
0 1	$\alpha\|1\rangle - \beta\|0\rangle$

So if:

$M_1 M_2 = 00$: Bob has Alice's original qubit.

$= 01$: Bob can obtain Alice's qubit by operating with $\hat{X}$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

$= 10$: Bob can obtain Alice's qubit by operating with $\hat{Z}$:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$= 11$: Bob can obtain Alice's qubit by operating with $\hat{X}\hat{Z}$.

These possibilities are summarized by $\hat{X}^{M_2} \hat{Z}^{M_1}$, where $M_1, M_2 \in \{0, 1\}$. If Alice sends classical bits M_1, M_2 to Bob, he can manipulate his qubit to put it in Alice's original state $\alpha|0\rangle + \beta|1\rangle$.

Might seem mysterious. The qubit never moved! How did it get from Alice to Bob? Note:

1. The particle (or whatever was representing the qubit) never moved. We simply reconstructed the qubit at Bob.
2. Alice doesn't have her own qubit any more. No cloning.
3. Info wasn't transmitted faster than light — A needed to send classical bits to B.
4. Quantum teleportation is harder than classical. Classically we could just use a 3D fax machine.

But still it seems funny that α & β, which were located @ Alice, somehow moved to Bob. What happened?

Answer: nothing moved. α and β were never "located at Alice." They were always part of the wave function of the universe:

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left[\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)\right].$$

α & β were multiplying Bob's qubit just as much as they were multiplying Alice's. Our circuit simply made them manifest at Bob's location.

Final note: quantum teleportation has been achieved in practice: Bennett et al., PRL 1993.

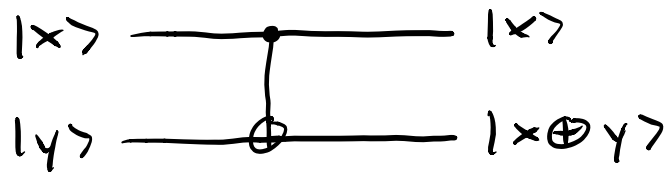
The real power of the quantum-circuit way of thinking becomes evident when we consider algorithms.

Let's give a very simple example:

add two classical bits $x, y \in \{0, 1\}$.

Obviously we'll represent our classical bits as qubits, with $0, 1 \to |0\rangle, |1\rangle$.

You might think we already know how to do that, using CNOT:



But that XOR "$\oplus$" does addition modulo 2. So if $x=1$, $y=1$, we get $1 \oplus 1 = 0$, which is not ordinary addition.

To represent $1+1=2$, we need one more qubit. Consider the Toffoli Gate, a.k.a. CCNOT (Controlled-CNOT).

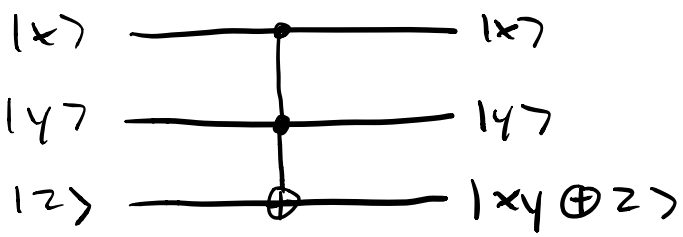
Given 3 qubits, it flips the third iff the first two are both 1.

xyz	CCNOT
000	000
001	001
010	010
011	011
100	100
101	101
110	111
111	110

Matrix:

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

Action:



Constructing a three-bit Toffoli gate out of one- and two-qubit gates is possible, but far from obvious. (Classically it's impossible!) Here's one way.

Define a one-qubit phase gate:

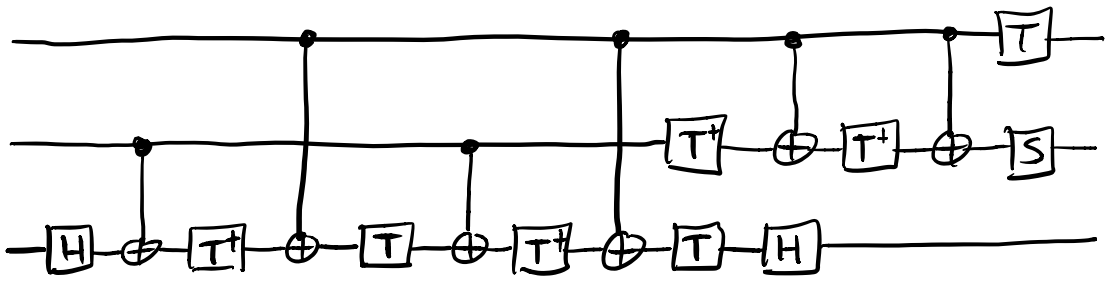
$$-\boxed{P(\phi)}- \;=\; \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

E.g. $\hat{Z} = \hat{P}(\pi)$. We'll use

$$\hat{S} = \hat{P}(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$\hat{T} = \hat{P}(\pi/4) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

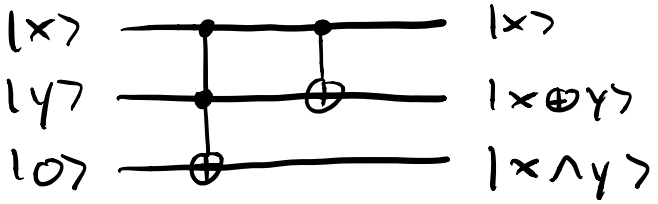
Then Toffoli is



Check for yourself!

Let's just take it for granted.

Then here's a quantum circuit that properly adds two bits (encoded as qubits):



We can read out our answer from the bottom two qubits: the second is the "ones" bit, and the third the "twos" bit, of our binary number.

Admittedly that's a bit silly, we don't need a quantum computer to add numbers.

Quantum computers are intriguing because of the possibility they can do calculations faster than classical ones.

In theoretical computer science, "faster" means "in fewer steps."

Another simple example: Deutsch's Algorithm.

Here's the (somewhat artificial) setup.

We are given a black box that performs an unknown function $f(x)$ mapping one bit to one bit. There are only four such functions, two reversible and two irreversible:

reversible: $\begin{cases} f_1(x) = x \\ f_2(x) = x+1 \end{cases}$ irreversible: $\begin{cases} f_3(x) = 0 \\ f_4(x) = 1. \end{cases}$

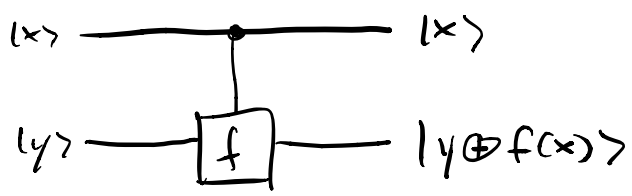
Note $f(x)$ is irreversible iff $f(0) = f(1)$.

Our task is to determine whether the function inside the box is reversible or irreversible, by querying it (putting some input in and seeing what comes out).

Classically, this requires two steps — we have to query both $f(0)$ and $f(1)$ to determine whether $f(x)$ is reversible.

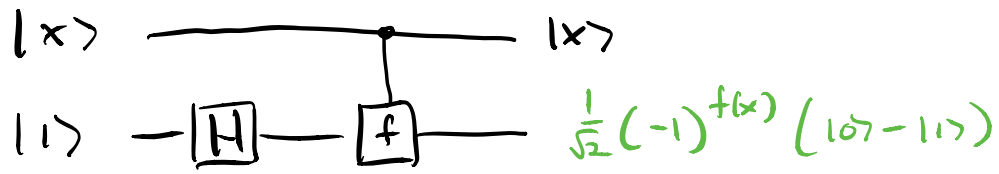
Can QM do better?

First we have to implement $f(x)$ using only reversible operations, so let's imagine a "controlled-f gate":



That is, "flip y if $f(x) = 1$, otherwise leave it alone." Clearly reversible.

Now consider:



The Hadamard sends $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

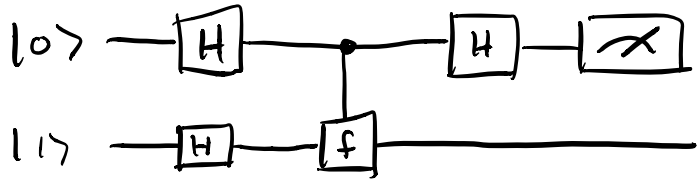
Then, for $|x\rangle \in \{|0\rangle, |1\rangle\}$,

$$\frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) \xrightarrow{C\text{-}f} \begin{cases} \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle), & f(x)=0 \\ \frac{1}{\sqrt{2}}|x\rangle(-|0\rangle + |1\rangle), & f(x)=1. \end{cases}$$

This can be summarized as

$$\frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) \xrightarrow{C\text{-}f} \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle).$$

Deutsch's algorithm is then:



Watch what happens:

$$|01\rangle \longrightarrow \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$\longrightarrow \frac{1}{2}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right](|0\rangle - |1\rangle)$$

$$\longrightarrow \frac{1}{2\sqrt{2}}\left[(-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)\right](|0\rangle - |1\rangle)$$

$$= \frac{1}{2\sqrt{2}}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right] \otimes (|0\rangle - |1\rangle).$$

Thus:

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

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

∴ All we have to do is measure the first register in the $\{|0\rangle, |1\rangle\}$ basis. If the answer is $|0\rangle$, we know $f(0) = f(1)$, and the function $f(x)$ is irreversible; if it's $|1\rangle$, $f(x)$ is reversible.

Notice something funny: we got the answer by measuring the upper register, even though the definition of the C-f gate leaves the upper wire unaffected! How did the information get there? Resolution: the upper wire is unaffected if $|0\rangle$ or $|1\rangle$ goes through. But a superposition is affected — it becomes entangled with the lower qubit.

The main point of this artificial exercise is: our quantum algorithm distinguished between reversible & irreversible functions in just one step (one call of $f(x)$), whereas a classical algorithm would have needed at least two.

Speed up!