Sean Carroll, seancarroll@gmail.com

125c, Lecture Fourteen: 5/17/17

And now for something completely different.

Quantum Information & Computation.

[refs: Preskill's notes, Nielsen & Chuang]

We've already mentioned that it is often convenient to think of quantum evolution directly in terms of unitary operators $\hat{U}$, rather than dragging out the Schrödinger equation every time. We've also noted that, especially if we're content to focus on finite-dim. Hilbert spaces, it's convenient to consider qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as the fundamental thing we act on.

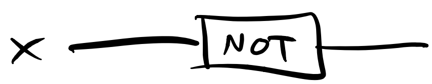
Together, these perspectives suggest that we should consider <u>sequences of unitary operations</u> performed on <u>sets of qubits</u>.

This is exactly the world of quantum information theory. Of course these ideas have direct application to building actual quantum computers, but their usefulness is more general – e.g. there is growing interest in the application of quantum information to black holes and quantum gravity.

Let's recall a bit (ha ha) about <u>classical</u> computation. There what we work with are actual bits $\{0,1\}$.

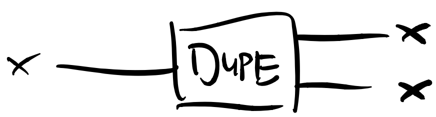
It's convenient to cast our manipulations on bits in terms of circuits, consisting of wires and gates. A wire just carries a bit down the circuit unchanged, while a gate converts a set of input bits into a set of output bits.

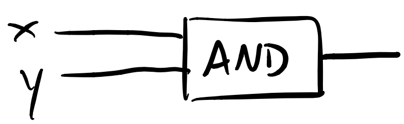
Some famous classical gates:



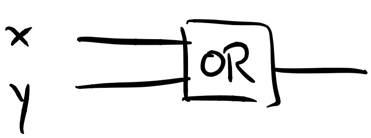
$\neg x = x + 1$.

(Remember arithmetic on bits is carried out mod 2, so $1+1=0$.)





$x \wedge y = x \cdot y$



$x \vee y = x + y - x \cdot y$

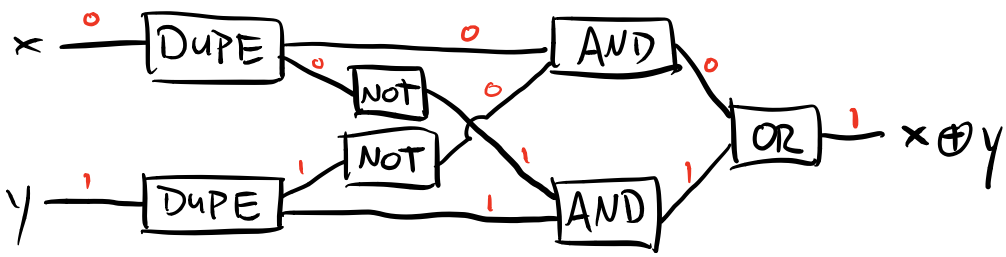
In truth-table form:

x, y	$x \wedge y$	$x \vee y$	$x \oplus y$
0 0	0	0	0
0 1	0	1	1
1 0	0	1	1
1 1	1	1	0

Famous Theorem: this set of gates {NOT, AND, OR, DUPE} is <u>universal</u> — any Boolean function $\{0,1\}^n \to \{0,1\}^m$ is computable by some circuit constructed from them. (Often "DUPE" is taken for granted and left implicit. But in QM such an operation doesn't even exist, as we'll see.)

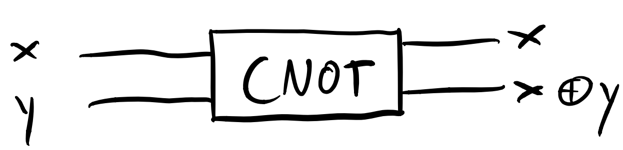
For example $\text{XOR}(x,y) = x \oplus y =$ "x or y but not both" (exclusive OR).

XOR may be implemented by the following circuit:

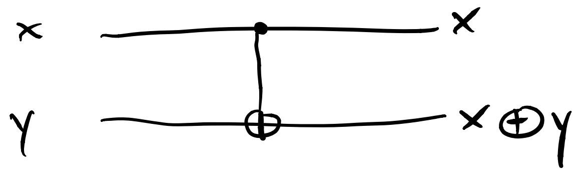


Check with $x, y = 0, 1$.

A gate G is <u>reversible</u> if $\exists$ a gate G^{-1} s.t. $GG^{-1} = \mathbb{1}$. Obviously reversible gates have the same number of inputs as outputs. NOT is reversible, but AND, OR, and XOR are not. The CNOT (controlled-NOT) gate is reversible:

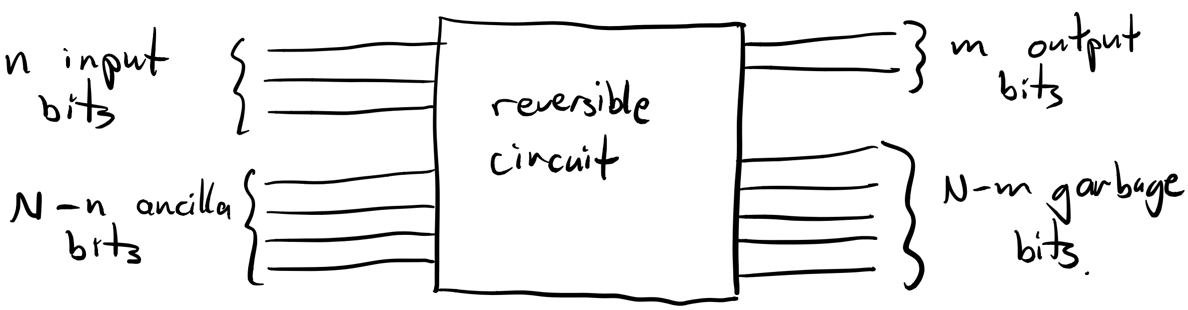


So CNOT says "keep x fixed, flip y if $x=1$, keep y fixed if $x=0$." Often drawn as



x, y	CNOT(x,y)
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

We can perform "irreversible" operations (n bits) → (m bits) by adding extra "ancilla" bits to the input, and "garbage" bits to the output.



Let's generalize to quantum circuits, acting on qubits. Classically, the only deterministic one-bit gates are

$$\left.\begin{array}{l}\bullet \text{ the identity} \\ \bullet \text{ NOT}\end{array}\right\} \text{reversible}$$

$$\left.\begin{array}{l}\bullet\ \{0,1\} \to 0 \\ \bullet\ \{0,1\} \to 1.\end{array}\right\} \text{irreversible.}$$

Obviously there's a lot more flexibility when we act on qubits. We generally stick to <u>unitary</u>, and therefore reversible, quantum gates, though of course we might want to do some measurements at the end of the process.

Obvious examples are <u>Pauli Matrices</u>:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \alpha|0\rangle+\beta|1\rangle \;-\!\boxed{X}\!-\; \beta|0\rangle+\alpha|1\rangle$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \alpha|0\rangle+\beta|1\rangle \;-\!\boxed{Y}\!-\; -i\beta|0\rangle+i\alpha|1\rangle$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \alpha|0\rangle+\beta|1\rangle \;-\!\boxed{Z}\!-\; \alpha|0\rangle-\beta|1\rangle$$

Another useful one is the <u>Hadamard</u> gate:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \alpha|0\rangle+\beta|1\rangle \;-\!\boxed{H}\!-\; \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle+\frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle$$

H rotates $|0\rangle$ to $|+\rangle$, and $|1\rangle$ to $|-\rangle$.

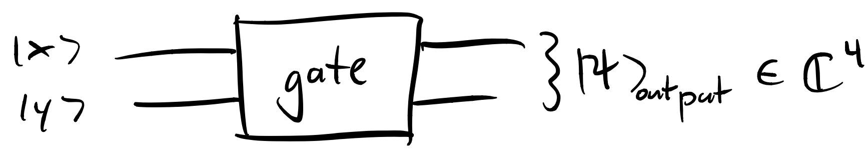
<u>Measurements</u> are denoted by

$$\alpha|0\rangle+\beta|1\rangle \;-\!\boxed{\nearrow}\!-\; \begin{matrix} |0\rangle, \text{ probability } |\alpha|^2 \\ |1\rangle, \text{ probability } |\beta|^2. \end{matrix}$$

We could stick measurements anywhere in the circuit, but it always suffices to put them at the end.

There are of course a number of interesting 2-qubit gates. Here we make use of the linearity of QM.

We denote a 2-qubit gate as

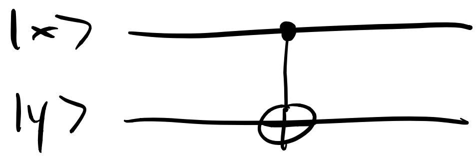


You might think "wait, what if I put an entangled two-qubit state as input?"

Because QM is linear, if we know the action of the gate on a complete basis, we know it for any state. And any 2-qubit state has a basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (and similarly for n-qubit states).

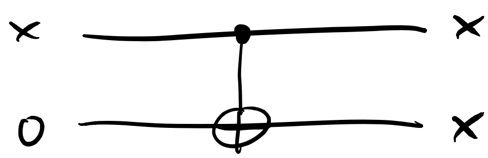
So we generally specify our gates by their actions on unentangled basis qubits.

We've already met the quantum CNOT gate:



$\|xy\rangle$	CNOT(x,y)
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

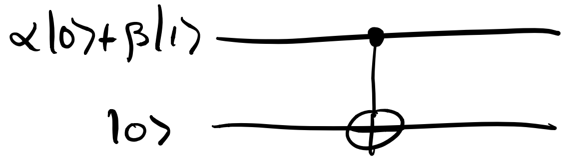
This raises an interesting question. Imagine a classical CNOT, where we fix $y=0$ but leave x arbitrary. Such a gate simply duplicates x:



(classical)

Can we therefore use a quantum CNOT, with $|y\rangle = |0\rangle$, to duplicate a qubit?

No! Because of entanglement.



$\Big\}\ \alpha|00\rangle + \beta|11\rangle.$

Duplication would be

$$(\alpha|0\rangle+\beta|1\rangle)|0\rangle \to (\alpha|0\rangle+\beta|1\rangle)\otimes(\alpha|0\rangle+\beta|1\rangle).$$
$$= \alpha^2|00\rangle + \alpha\beta(|01\rangle+|10\rangle) + \beta^2|11\rangle.$$

But it actually goes to $\alpha|00\rangle+\beta|11\rangle$.

In fact we have the No-Cloning Theorem (Wootters & Zurek 1982, Dieks 1982):

There exists no quantum circuit acting on n qubits that sends

$$|\psi\rangle\otimes(|0\rangle)^{n-1} \to |\psi\rangle\otimes|\psi\rangle\otimes|\Phi_{n-2}\rangle,$$

where $|\psi\rangle$ is an arbitrary qubit and $|\Phi_{n-2}\rangle$ is any "garbage" output state.

<u>Proof</u>: By contradiction. Assume that a cloning circuit exists, implemented by a unitary $\hat{U}$. Then we know

$$\hat{U}(|0\rangle^n) = |0\rangle \otimes |0\rangle \otimes |\Phi(0)\rangle,$$

$$\hat{U}(|1\rangle \otimes |0\rangle^{n-1}) = |1\rangle \otimes |1\rangle \otimes |\Phi(1)\rangle.$$

By linearity, acting on $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gives

$$\hat{U}(|+\rangle \otimes |0\rangle^{n-1}) = \frac{1}{\sqrt{2}}|00\rangle|\Phi(0)\rangle + \frac{1}{\sqrt{2}}|11\rangle|\Phi(1)\rangle.$$

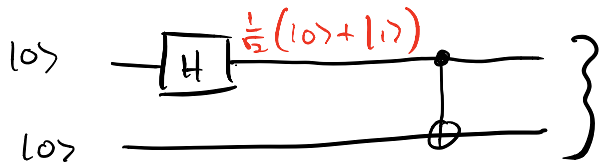
But if it really cloned, it <u>should</u> give

$$\hat{U}(|+\rangle \otimes |0\rangle^{n-1}) \stackrel{?}{=} \frac{1}{2}(|0\rangle+|1\rangle) \otimes (|0\rangle+|1\rangle) \otimes |\Phi(+)\rangle.$$

These are not the same (e.g. there are no $|01\rangle$ terms in the first expression), therefore no such unitary exists.

This is important! E.g. a quantum computer can't use <u>classical</u> error correction, just by duplicating its internal state many times. Need to be more subtle.

We can use a quantum circuit to entangle two qubits. Add a Hadamard to our CNOT:



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

This is one of our Bell states, representing an EPR pair.