6.896 Quantum Complexity Theory September 9, 2008

Lecture 2

Lecturer: Scott Aaronson

Quick Recap

The central object of study in our class is BQP, which stands for "**B**ounded error, **Q**uantum, **P**olynomial time". Informally this complexity class represents problems which are *efficiently* solvable with *high* probability by a quantum computer, a precise definition will be given in later lectures.

For our purposes quantum mechanics is just a generalization of probability theory, the table below describes some of the concepts used in classical probability theory and their equivalent in quantum mechanics.

Probability	Quantum Mechanics
$\mathbb{R}^+$	$\mathbb{C}$
L_1 preserved	L_2 preserved
Stochastic Matrices	Unitary Matrices

The quantum state of a physical system can be described by a vector in Hilbert Space, for which we will use the bra-ket notation. Given a basis, any vector can be represented by a linear combination of the basis elements, therefore in general we express a quantum state as,

$$\alpha_1 |1\rangle + \ldots + \alpha_N |N\rangle$$

Where $|1\rangle, \ldots, |N\rangle$ are the basis vectors and $\alpha_1, \ldots, \alpha_N$ are complex numbers. Mostly we will work with normalized states, which means that $\sum_{i=1}^{N} |\alpha_i|^2 = 1$. When dealing with normalized states $|\alpha_i|^2$ represents the probability that the result of a measurement is $|i\rangle$.

Quantum mechanics can be seen as having only two principles, unitary evolution (multiplying the quantum state by a unitary matrix) and measurement in a standard basis, which results in a collapse of the state to whatever outcome you get. A nice analogy to this is baking a souffle, where if you open the oven to see how it's doing you have collapsed it and have to start over.

Consider the following matrix which represents a 45° counter clock wise rotation in the plane

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

Suppose you are in the state $|0\rangle$ and you apply this operation twice in succession and measure, you would get $|1\rangle$. However if you apply it once, then measure, then apply it again you would get $|0\rangle$ half of the time and $|1\rangle$ half of the time.

This is analog to interference in the double slit experiment.

Why measurement alters the state?

There are three schools of thought that provide different answers to this question,

Niels Bohr (Copenhagen interpretation)

> In essence this interpretation amounts to a sophisticated way of saying not to ask the question. Science relies on the notion of measurements and observations, so in essence asking in quantum mechanics "what is a measurement?" is equivalent to asking the axioms of euclidean geometry "what is a point?".

Hugh Everett (Many worlds interpretation)

> There is only one process in quantum mechanics, unitary evolution. What we perceive as measurements is just unitary evolution applied to the measuring equipment and the observer. Essentially the universe splits every time a measurement is performed, and one copy sees $|0\rangle$ while the other sees $|1\rangle$.

David Bohm (Non-local hidden variables)

> The third answer says that both of the previous answers are unacceptable, so quantum mechanics is somehow incomplete in the sense that there is an additional aspect that we're missing. Non-local hidden variables is one proposal to fill that gap, but there are others.

For our purposes it doesn't matter which of these answers is correct and we are free to pick whatever interpretation is more convenient, since at least for the experiments we can currently conceive it leads to the same outcome.

Why does nature use complex numbers?

One possible explanation is that complex numbers are required if we want our unitary transformations to be continuous. As an example consider the face-flip operation represented by the following matrix:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

This matrix maps the state $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|0\rangle - \beta|1\rangle$. But what is in between these two states? To have a continuos unitary transformation between these two states requires the use of complex numbers.

Why the L_2-norm?

As it turns out only the with L_1-norm and the L_2-norm you can get nontrivial norm-preserving linear transformations.

Entanglement

So far we have considered only a system with a single qubit, now we will start talking about two qubits.

$$\alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle$$

To apply an operation to the first qubit only you can tensor product the transformation with the identity on the second qubit, for example:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

If we measure the qubit the probability of measuring $|0\rangle$ is $|\alpha|^2 + |\beta|^2$. Also, assuming we measured zero, the state of the second qubit collapses to

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

Separable states

An important class of multi-qubit states are those which can be factorized into a sequence of tensored single-qubit states. Such states are called separable, for example:

$$(\alpha |0\rangle + \beta |1\rangle)(\gamma |0\rangle + \delta |1\rangle) = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle$$

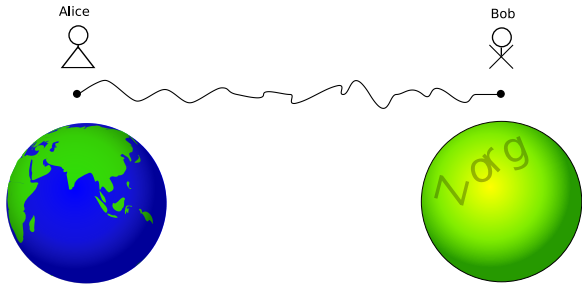
However it is clear that not all states are separable, for example $|00\rangle + |11\rangle$ is not separable. We say such states are entangled.

How is entanglement different from correlation?

EPR paper

In 1935, Einstein, Podolsky and Rosen wrote a famous paper where they brought to widespread attention the tension between quantum mechanics and relativity. One thing that relativity says is that you can't send information faster than light.

However suppose that you have an entangled state like $|00\rangle$ and $|11\rangle$, and suppose one qubit is on Earth and the other is in planet Zorg. If Alice (on earth) measures her qubit and gets a $|0\rangle$, then when Bob (on Zorg) measures his qubit he will also get a $|0\rangle$.



However in this experiment Alice didn't pick what to send. What the EPR paper was trying to ask is if quantum mechanics somehow contradicts relativity. This sets the sate for Bell's theorem.

Bell's inequality

In 1964 Bell played the roll of a quantum complexity theorist. He said, let's compare entanglement against classical correlation as resources to perform some task.

The task is the following, Alice and Bob are given random bits a and b respectively, and they will output bits x and y respectively such that

$$a \oplus b = x \wedge y$$

Even with correlated random bits, the best strategy allows them to win at most 75% of the time, for example if they both pick 0. Bell devised a strategy that allows them to win 85% of the time if they share entangled qubits. The strategy is described below:

Alice: If $x = 0$ then measure and output, else apply the matrix $\begin{bmatrix} \cos\frac{\pi}{8} & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{bmatrix}$ measure and output.

Bob: If $y = 0$ then measure and output, else apply the matrix $\begin{bmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{bmatrix}$ measure and output.

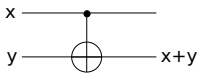
The combined probability of success counting the four possible combinations of a and b is $\cos^2\frac{\pi}{8} \approx 0.85$.

Notice that this doesn't mean that signals are getting transmitted faster than light, after all you need to bring Alice and Bob's outputs together to even tell if they won or not. However this is a communication task that is possible in a classical universe.

1 Quantum Circuits

Quantum circuits are a nice way to visualize operations with qubits, here we define a couple of useful operations and their notation in quantum circuits. The *Controlled Not* operation $|x, y\rangle \to |x, x \otimes y\rangle$ is represented by the following matrix

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

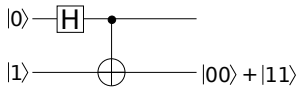


Another popular operation in quantum circuits is the Hadamard operation which intuitively switches between the $|0\rangle$,$|1\rangle$ basis and the $|0\rangle + |1\rangle$,$|0\rangle - |1\rangle$ basis, and is represented by the following matrix

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \qquad \boxed{\text{H}}$$

In a quantum circuit we can apply a sequence of unitary operations or "gates", where each gate can act on the first qubit only (like the Hadamard) or on the second qubit only, or on both qubits together (like the CNOT).

Using the operations described and starting from an unentangled state we create an entangled state with the following circuit,



2 Quantum copying machine

We mentioned before that measuring collapses the state, but what if we could take our quantum state and duplicate it? How would this look like?

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

Therefore we just need to find some unitary transformation to perform the above behavior, however the operation required is nonlinear. This is what its called the No-Cloning Theorem.

6.845 Quantum Complexity Theory
Fall 2010