CS170 Quantum Computation 5/6/04
Spring 2004 Lecture 27

In the next two lectures we will return to a theme that we studied at the very beginning of this course: there we saw that primality testing is easy, while factoring is hard. We now return to factoring, and will show that we can factorize numbers in polynomial time provided we can build computers based on the principles of quantum physics.

But what does physics have to do with computers? Computer science is all about levels of abstraction. When we solve an all pairs shortest path problem, we can do so at a very abstract level as Dijkstra's algorithm. Or we can program it in a high level language such as Lisp or Java. Or compile that into assembly or machine code. At a lower level of abstraction, this we could worry about the architecture of the underlying machine or a gate level description of the machine. But when we are done unwinding all the layers, the shortest path problem is eventually mapped into currents and voltages in a circuit that consists of wires and transistors and resistors. Thus a computer is just a way of mapping a problem onto a physical system, thereby getting nature to solve the problem for us. The genius of computer science lies in the realization that this mapping can be made universal, so that the same physical system can be used to solve a wide variety of problems, by just changing the program.

What are the features of quantum physics that makes it more suitable as the platform to carry out certain computations? Let us start by considering a simple experiment which demonstrates the quantum nature of light.

0.1 Young's double-slit experiment

Let $\psi_1(x) \in \mathscr{C}$ be the amplitude if only slit 1 is open. Then the probability density of measuring a photon at x is $P_1(x) = \left|\psi_1(x)\right|^2$. Let $\psi_2(x)$ be the amplitude if only slit 2 is open. $P_2(x) = \left|\psi_2(x)\right|^2$.

$\psi_{12}(x) = \frac{1}{\sqrt{2}}\psi_1(x) + \frac{1}{\sqrt{2}}\psi_2(x)$ is the amplitude if both slits are open. $P_{12}(x) = \left|\psi_1(x) + \psi_2(x)\right|^2$. The two complex numbers $\psi_1(x)$ and $\psi_2(x)$ can cancel each other out – destructive interference.

But how can a single particle that went through the first slit know that the other slit is open? In quantum mechanics, this question is not well-posed. Particles do not have trajectories, but rather take all paths simultaneously. This is a key to the power of quantum computation.

0.2 Qubits – Naive introduction

The basic entity of quantum information is a qubit (pronounced "cue-bit"), or a quantum bit. Consider the electron in a hydrogen atom. It can be in its ground state (i.e. an s orbital) or in an excited state. If this were a classical system, we could store a bit of information in the state of the electron: ground = 0, excited = 1.

In general, since the electron is a quantum system, it is in a linear superposition of the ground and excited state — it is in the ground state (0) with probability amplitude $\alpha \in \mathscr{C}$ and in the excited state (1) with probability amplitude $\beta \in \mathscr{C}$. It is as though the electron "does not make up its mind" as to which of the 2 classical states it is in. Such a 2-state quantum system is called a qubit, and its state can be written as a unit (column) vector $\binom{\alpha}{\beta} \in \mathscr{C}^2$. In Dirac notation, this may be written as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \alpha, \beta \in \mathscr{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1$$

The Dirac notation has the advantage that the it labels the basis vectors explicitly. This is very convenient because the notation expresses both that the state of the qubit is a vector, and that it is data (0 or 1) to be processed. (The $\{|0\rangle, |1\rangle\}$ basis is called the standard or computational basis.)

This linear superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is part of the private world of the electron. For us to know the electron's state, we must make a measurement. Measuring $|\psi\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis yields $|0\rangle$ with probability $|\alpha|^2$, and $|1\rangle$ with probability $|\beta|^2$.

One important aspect of the measurement process is that it alters the state of the qubit: the effect of the measurement is that the new state is exactly the outcome of the measurement. I.e., if the outcome of the measurement of$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ yields $|0\rangle$, then following the measurement, the qubit is in state $|0\rangle$. This implies that you cannot collect any additional information about α, β by repeating the measurement.

More generally, we may choose any orthogonal basis $v, v^{\perp}$ and measure the qubit in it. To do this, we rewrite our state in that basis: $|\psi\rangle = \alpha'|v\rangle + \beta'|v^{\perp}\rangle$. The outcome is v with probability $|\alpha'|^2$, and $|v^{\perp}\rangle$ with probability $|\beta'|^2$. If the outcome of the measurement on $|\psi\rangle$ yields $|v\rangle$, then as before, the the qubit is then in state $|v\rangle$.

0.2.1 Measurement example I.

Q: We measure $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the $|v\rangle, |v^{\perp}\rangle$ basis, where $|v\rangle = a|0\rangle + b|1\rangle$. What is the probability of measuring $|v\rangle$?

A: First let's do the simpler case $a = b = \frac{1}{\sqrt{2}}$, so $|v\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle$, $|v^{\perp}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle$. See Figure **??**. We express $|\psi\rangle$ in the $|+\rangle, |-\rangle$ basis:

$$\begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ &= \alpha\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) + \beta\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \\ &= \frac{1}{\sqrt{2}}((\alpha+\beta)|+\rangle + (\alpha-\beta)|-\rangle) \quad . \end{aligned}$$

Therefore the probability of measuring $|+\rangle$ is $\left|\frac{1}{\sqrt{2}}(\alpha+\beta)\right|^2 = |\alpha+\beta|^2/2$. The probability of measuring $|-\rangle$ is $|\alpha+\beta|^2/2$.

1 Two qubits:

Now let us examine the case of two qubits. Consider the two electrons in two hydrogen atoms:

Since each electron can be in either of the ground or excited state, classically the two electrons are in one of four states – 00, 01, 10, or 11 – and represent 2 bits of classical information. Quantum mechanically, they are in a superposition of those four states:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad ,$$

where $\sum_{ij} \left|\alpha_{ij}\right|^2 = 1$. Again, this is just Dirac notation for the unit vector in $\mathscr{C}^4$:

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

where $\alpha_{ij} \in \mathscr{C}, \sum \left|\alpha_{ij}\right|^2 = 1$.

Measurement:

If the two electrons (qubits) are in state $|\psi\rangle$ and we measure them, the n the probability that the first qubit is in state i, and the second qubit is in state j is $P(i,j) = \left|\alpha_{ij}\right|^2$. Following the easurement, the state of the two qubits is $|\psi'\rangle = |ij\rangle$. What happens if we measure just the first qubit? What is the probability that the first qubit is 0? In that case, the outcome is the same as if we had measured both qubits: $\Pr\{\text{1st bit } = 0\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. The new state of the two qubit system now consists of those terms in the superposition that are consistent with the outcome of the easurement – but normalized to be a unit vector:

$$|\phi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

.

A more formal way of describing this partial measurement is that the state vector is projected onto the subspace spanned by $|00\rangle$ and $|01\rangle$ with probability equal to the square of the norm of the projection, or onto the orthogonal subspace spanned by $|10\rangle$ and $|11\rangle$ with the remaining probability. In each case, the new state is given by the (normalized) projection onto the respective subspace.

2 Spooky Action at a Distance

Consider a state known as a EPR pair (also called a Bell state)

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

easuring the first bit of $|\Psi^-\rangle$ in the standard basis yields a 0 with probability 1/2, and 1 with probability 1/2. Likewise, easuring the second bit of $|\Psi^-\rangle$ yields the same outcomes with the same probabilities. Measuring one bit of this state yields a perfectly random outcome.

However, determining either bit exactly determines the other.

In 1935, Einstein, Podolsky and Rosen (EPR) wrote a paper ”Can quantum mechanics be complete?”

For example, consider coin-flipping. We can model coin-flipping as a random pro cess giving heads 50% of the time, and tails 50% of the time. This model is perfectly predictive, but incomplete. With a more accurate experimental setu p, we could determine precisely the range of initial parameters for which the co in ends up heads, and the range for which it ends up tails.

For Bell state, when you measure first qubit, the second qubit is determined. However, if two qubits are far apart, then the second qubit must have had a dete rmined state in some time interval before measurement, since the speed of light is finite. Moreover this holds in any basis. This appears analogous to the coin flipping example. EPR therefore suggested that there is a more complete theory where “God does not throw dice.”

What would such a theory look like? Here is the most extravagant framework... When the entangled state is created, the two particles each make up a (very long!) list of all possible experiments that they might be subjected to, and decide how they will behave under each such experiment. When the two particles separate and can no longer communicate, they consult their respective lists to coordinate their actions.

But in 1964, almost three decades later, Bell showed that properties of EPR states were not merely fodder for a philosophical discussion, but had verifiable consequences: local hidden variables are not the answer.

He showed that there are certain measurements that you can make on the two particles such that the maximum correlation you can obtain in any local hidden variable theory is $3/4$, whereas quantum physics predicts that the correlation is close to 0.8. Experiments on EPR states have shown that within experimental errors, the correlation is indeed 0.8 and not $3/4$, thus showing that nature does behave in this wierd quantum manner.

3 n qubits

Now consider a system of n hydrogen atoms (think of $n = 500$). Classically the state of the system is described by 500 bits, and is in one of 2^{500} states. Quantum physics asserts that in general, the state of the system is a linear superposition of all 2^{500} classical states x, each with its amplitude α_x. Thus the state is $\Psi = \sum_x \alpha_x |x\rangle$, where $\sum_x |\alpha_x|^2 = 1$. What makes this remarkable is that even for modest values of n of a few hundred, 2^n is larger than estimates on the number of elementary particles in the Universe. How does nature keep track of all this information. And how does it find time to update this information at every moment of time as the system evolves? Rather than dwell on these philosophical issues, quantum computation proceeds with the viewpoint that if nature is so extravagant at the quantum level, then that is where we should map our computational problems.

The only problem is that when we actually a measure an n-qubit quantum state, we see only an n-bit string: x with probability $|\alpha_x|^2$. Quantum physics claims that nature is very complicated, but when it is measured it pretends to be much simpler than it is. The main challenge in quantum computation lies in accessing the hidden power implicit in the exponentially large superposition that we cannot directly access through measurements.