C/CS/Phys C191 Quantum States, Superposition 8/30/05
Fall 2005 Lecture 1

1 Course Philosophy/Outline

Over the last decade the there have been foundational progress at the interface of quantum physics and computer science. The remarkable power of computing devices based on quantum mechanics is the subject of the emerging area of quantum computation (which incidentally provides an alternative to the exponential Moore's law dash towards fundamental limits in classical computation). This course provides an introduction to this area, the basic ideas of quantum mechanics, the formal model of quantum computers, basic quantum algorithms and more concrete proposals for experimental realization of quantum computers.

Qubits are the building blocks of quantum computation, quantum information and cryptography. They also provide a particularly simple setting in which to introduce the basic concepts of quantum mechanics such as the superposition principle, tensor products, measurements, and the enigmatic Bell's inequalities and Heisenberg uncertainty principle. The first part of this course provides a simple introduction to quantum mechanics for non-physics majors, while providing physics majors an opportunity to deepen their understanding of this important topic.

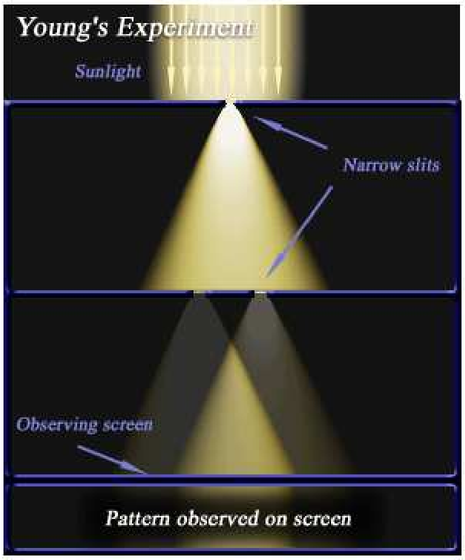
The course will then focus on the enormous computational power latent in quantum mechanics, and how it can be used to design quantum computers and quantum algorithms. We will also discuss schemes for quantum error-correction and for implementing unconditionally secure cryptography based on the principles of quantum mechanics.

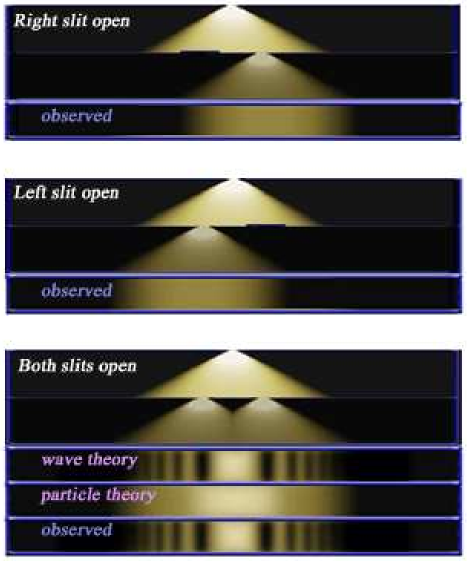
Finally, we will turn our attention to physical realization: we will discuss in detail the spin properties of elementary particles - the vehicle of choice for carrying a qubit. The course will conclude with a survey of schemes for implementing quantum computers in the laboratory.

There are four main properties of quantum systems that are useful in quantum computation, cryptography and Information:

- Interference
- Superposition
- Entanglement
- Measurement

In particular, the detailed study of entanglement is the most important point of departure from more traditional approaches to the subject. For example, quantum computation derives its power from the fact that the description of the state of an n-particle quantum system grows exponentially in n. This enormous information capacity is not easy to access, since any measurement of the system only yields n pieces of classical information. Thus the main challenge in the field of quantum algorithms is to manipulate the exponential amount of information in the quantum state of the system, and then extract some crucial pieces via a final measurement.





Quantum cryptography relies on a fundamental property of quantum measurements: that they inevitably disturb the state of the measured system. Thus if Alice and Bob wish to communicate secretly, they can detect the presence of an eavesdropper Eve by using cleverly chosen quantum states and testing them to check whether they were disturbed during transmission.

1.1 Young's double-slit experiment

Recall Young's double-slit experiment from high school physics, which was used to demonstrate the wave nature of light. The apparatus consists of a source of light, a screen with two very thin identical slits, and a screen to view the (interference) pattern created by transmitted light (see picture on next page). If only one slit is open then intensity of light on the viewing screen is maximum on the straight line path and falls off in either direction. However, if both slits are open, then the intensity oscillates according to the interference pattern predicted by wave theory.

In the quantum version of this experiment, the light source is replaced by a source of single photons. Instead of the intensity of light falling on a point x on the viewing screen, we can only speak about the probability that a detector at point x detects the photon. If only a single slit is open, then plotting this probability of detection as a function of x gives the same curve as the intensity as a function of x in the classical Young experiment. What happens when both slits are open? Could the probabability plot duplicate the interference pattern? Classical intuition strongly suggests that this is impossible. After all, for the photon to be detected at x, either it went through slit 1 and ended up at x or it went through slit 2 and ended up at x. The probability that it is detected at x is just the sum of the probabilities of these two events. However there are points x where the detection probability is large if only one slit is open although it is zero or small in the interference pattern. If the photon actually goes through slit 1, why should it matter whether slit 2 is open or shut. How could the probability that the photon goes through slit 1 and ends up at x be affected by whether or not slit 2 is open.

Nonetheless, the probability of detection when both slits are open does duplicate the interference pattern. How does quantum mechanics explain this? Quantum mechanics explains this as follows (although this might not be very satisfactory as an explanation, it does provide a good formal was of thinking about the phenomenon):

Quantum mechanics introduces the notion of the complex amplitude $\psi_1(x) \in \mathscr{C}$ with which the photon goes through slit 1 and hits point x on the viewing screen. The probability that the photon is actually detected at x is the square of the magnitude of this complex number: $P_1(x) = |\psi_1(x)|^2$. Similarly, let $\psi_2(x)$ be the amplitude if only slit 2 is open. $P_2(x) = |\psi_2(x)|^2$.

Now when both slits are open, the amplitude with which the photon hits point x on the screen is just the sum of the amplitudes over the two ways of getting there: $\psi_{12}(x) = \frac{1}{\sqrt{2}}\psi_1(x) + \frac{1}{\sqrt{2}}\psi_2(x)$. As before the probability that the photon is detected at x is the squared magnitude of this amplitude: $P_{12}(x) = |\psi_1(x) + \psi_2(x)|^2$. The two complex numbers $\psi_1(x)$ and $\psi_2(x)$ can cancel each other out to produce destructive interference, or reinforce each other to produce constructive interference or anything in between.

But in this quantum mechanical explanation, how does a 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.

1.2 Basic Quantum Mechanics

The basic formalism of quantum mechanics is very simple, though understanding and interpreting the results is much more challenging. There are three basic principles, enshrined in the three basic postulates of quantum mechanics:

- The superposition principle: this axiom tells us what the state of a quantum system looks like.
- The measurement principle: this axiom governs how much information about the state we can access.
- Unitary evolution: this axoim governs how the state of the quantum system evolves in time.

1.3 The superposition principle

Consider a system with k distinguishable states. For example, the electron in an atom might be either in its ground state or one of $k-1$ excited states, each of progressively higher energy. As a classical system, we might use the state of this system to store a number between 0 and $k-1$. The superposition principle says that if a quantum system is allowed to be any one of number of different states then it can also be placed in a linear superposition of these states with complex coefficients. Thus the quantum state of the k-state system above is described by a sequence of k complex numbers $\alpha_0, \ldots, \alpha_{k-1} \in \mathscr{C}$. α_j is said to be the (complex) amplitude with which the system is in state j. We will require that the amplitudes are normalized so that $\sum_j |\alpha_j|^2 = 1$. It is natural to write the state of the system as a k dimensional vector:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{k-1} \end{pmatrix}$$

The normalization on the complex amplitudes means that the state of the system is a unit vector in a k dimensional complex vector space — called a Hilbert space.

In quantum mechanics it is customary to use the Dirac's ket notation to write vectors. As we shall see later, this is a particularly useful notation in the context of quantum computation. In the ket notation, the above state is written as:

$$|\psi\rangle = \sum_{j=0}^{k-1} |j\rangle$$

Here $|0\rangle = (10...0)^T$ and $|k-1\rangle = (0...01)^T$. 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 $\{|0\rangle, |1\rangle, \ldots, |k-1\rangle\}$ basis is called the standard or computational basis.

1.4 Measurement Principle

This linear superposition $|\psi\rangle = \sum_{j=0}^{k-1} |j\rangle$ 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 standard basis yields j with probability $|\alpha_j|^2$.

One important aspect of the measurement process is that it alters the state of the quantum system: 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 is j, then following the measurement, the qubit is in state $|j\rangle$. This implies that you cannot collect any additional information about the amplitudes α_j by repeating the measurement.

More generally, a measurement is associated with any orthonormal basis of the k-dimensional Hilbert space (complex vector space). The measurement can be conceptually thought of as follows: suppose the basis vectors of this orthonormal basis are labelled from 0 to $k-1$. The outcome of the measurement is j with probability equal to the square of the length of the projection of the state vector ψ onto the $j-th$ basis vector. Moreover, if the outcome is j, then the new state is the $j-th$ basis vector. Thus measurement may be regarded as a probabilistic rule for projecting the state vector onto one of the vectors of the orthonormal measurement basis.

1.5 Qubits

The basic entity of quantum information is a qubit (pronounced "cue-bit"), or a quantum bit. This corresponds to a 2-state quantum system, 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:

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