KEY POINTS FROM LECTURE 21

No-Cloning Theorem

It is impossible to produce a system with the same quantum mechanical properties as another system, without relying on prior knowledge of that system and without altering the state of that system.

This can be proved quite simply (see Problem Sheet 6 and Solutions) but it makes some sense. If it were possible to create a large ensemble of cloned systems and measurements on individual systems could be done without effecting the whole ensemble, potentially violating the uncertainty principle.

Quantum Teleportation

Quantum teleportation is the transfer of the quantum state of a reference system to a target system (by non-cloning the state of the reference system is altered in the process). Initially this sounds like a hard thing to do; the uncertainty principle limits what you can know about the reference state so how can you transfer all the properties to another system? Entanglement helps as follows.

Alice has a reference state based on a spin-1/2 qbit, Qbit 3: $\psi(3) = A\alpha(3) + B\beta(3)$. She wants to transfer this to a target, Qbit 1, and then send it to Bob. She arranges things such that Qbit 1 is part of an entangled pair with a third qbit, Qbit 2. Ths overall system is then:

$$\psi(1,2,3) = \frac{1}{\sqrt{2}}\left[A\alpha(3) + B\beta(3)\right]\left[\alpha(1)\beta(2) - \beta(1)\alpha(2)\right]$$

This is algebraically identical to:

$$\psi(1,2,3) = -\frac{1}{2}\left[A\alpha(1) + B\beta(1)\right]\psi_1(2,3) + \frac{1}{2}\left[A\alpha(1) - B\beta(1)\right]\psi_2(2,3)$$

$$-\frac{1}{2}\left[A\beta(1) + B\alpha(1)\right]\psi_3(2,3) - \frac{1}{2}\left[A\beta(1) - B\alpha(1)\right]\psi_4(2,3)$$

where the expression written in terms of an entangled wave function of Qbits 1 and 2 has been rewritten in terms of entangled states of Qbits 2 and 3:

$$\psi_1(2,3) = \frac{1}{\sqrt{2}}\left[\alpha(2)\beta(3) - \beta(2)\alpha(3)\right]$$

$$\psi_2(2,3) = \frac{1}{\sqrt{2}}\left[\alpha(2)\beta(3) + \beta(2)\alpha(3)\right]$$

$$\psi_3(2,3) = \frac{1}{\sqrt{2}}\left[\alpha(2)\alpha(3) - \beta(2)\beta(3)\right]$$

$$\psi_4(2,3) = \frac{1}{\sqrt{2}}\left[\alpha(2)\alpha(3) + \beta(2)\beta(3)\right].$$

There four wave functions are known as Bell's States and are the maximally entangled states of two spin-1/2 particles or indeed two particles in any two-level systems.

Alice now sends Qbit 1 to Bob.

She performs a Bell State measurement on Qbits 2 and 3 i.e. a measurement of some observable with an operator whose eigenfunctions are the Bell States. The wave function $\psi(1,2,3)$ then collapses into the appropriate term, out of the four terms with Bell States as factors in the above expression.

For the $N/2$ events where Alice and Bob have the same orientation, on average half the time Eve will do so as well. She steals the information and passes on a correct copy to Bob.

Alice phones Bob and tells him the result of her measurement

If Alice's measurement yields the eigenvalue associated with $\psi_1(2,3)$, $\psi(1,2,3)$ will collapse to either the first term in the expression above. Qbit 1 then has the wave function $\pm\left[A\alpha(1) + B\beta(1)\right]$ which is the same as the initial state of the reference system Qbit 3 (apart from a trivial phase factor)and the object of the exercise has been achieved.

If Alice's measurement yields the eigenvalue associated with either $\psi_2(2,3)$, $\psi(1,2,3)$ will collapse to second term in the expression above. Qbit 1 now has the wave function $-\left[A\alpha(1) - B\beta(1)\right]$. Bob then turns on a magnetic field perpendicular to the quantum axis to induce precession of the spins; the time evolution of Qbit 1 while the field is on is determined by $\pm\left[A\alpha(1)e^{-i\omega t} - B\beta(1)^{i\omega t}\right]$ where $\omega = \frac{eg}{4m}B$. So if Bob leaves the field on for a time such that $\omega t = \pi/2$ the wave function will be $-i\left[A\alpha(1) + B\beta(1)\right]$, which is the same as the initial state of the reference system Qbit 3 (apart from a trivial phase factor) and the object of the exercise has been achieved.

If Alice's measurement yields the eigenvalue associated with the other two remaining Bell States, Bob can still use the magnetic field trick to rotate spins to achieve $\left[A\alpha(1) - B\beta(1)\right]$, possible multiplied by irrelevant phase factors, and achieving the object of the exercise.

Quantum Computing

A classical computer takes in information in the form of a series of classical bits. It performs operations on them according to a set of rules and outputs the resulting information as a modified series of bits.

A quantum computer takes in information in the form of a set of qbits, whose wave functions are often entangled, in a particular quantum state. The computer allows the state of these qbits to evolve for a certain amount of time under specific conditions. The readout is then performed by making a measurement on the resulting state.

In principle all operations done by a classical computer are thought possible by a quantum machine, but to realise this in practice is extremely difficult, requires the development of all sorts of new technology and is not assured.

A NOT gate is a very simple example. NOT gate transforms a 1 into a 0, and a 0 into a 1. In a quantum computer with register formed from a single spin-1/2 qbit, a 0 could represented by α_z and a 1 by β_z. A NOT operation could be fairly simply undertaken by placing the qbit in a magnetic field oriented perpendicular to the z axis. The spin will then Larmour precess about the perpendicular axis and if the field is left on for the correct amount of time α_z will precess into β_z, and β_z will precess into $-\alpha_z$, apart from the presence of some trivial phase factors achieving the NOT operation.

If instead of the spin eigenvectors, the qbit was prepared in an initial state corresponding to a superposition $A\alpha_z + B\beta_z$ the same operation will result in $A\beta_z - B\alpha_z$. In other words, one quantum operation can do both basic classical operations at the same time.

One spin-1/2 qbit has two terms in a superposition. Two entangled qbits have a wave function that in its most general form is:

$$A\alpha(1)\alpha(2) + B\alpha(1)\beta(2) + C\beta(1)\alpha(2) + D\beta(1)\beta(2).$$

So two entangled qbits could undertake four basic operations in one quantum computation. Extending, N qbits coudl do 2^N basic operations simultaneously. This is dramatic; for example, for $N = 300$, 2^{300} is a number (probably) more than the number of atoms in the Universe!

Quantum computing appears to have a significant advantage over classical computers. However, to get the results out you need to make a measurement and the resulting collapse of the wave function means that most of the information gets lost. In the simple NOT case above, you can only get one of the two answers out because the wave function collapses down to one of the two terms in the superposition when you measure the spin direction.

Quantum computing therefore only appears to have a significant advantage in cases where there is a very large and complex calculation to do (if it were performed classically) and where the aim is to produce only a limit number of pieces of information. It has been proved (in principle) that data base searches, or factorising a number into two primes, are more efficient with quantum systems.

There are many ways to think about realising quantum computing: systems of spin-1/2 particles; manipulation of polarisation of entangled photons; microwave-induced flipping of molecular spins... But there are major issues, particularly with isolating the qbits from environmental effects such as stray fields precessing spins when you don't intend to. Work has been done on methods of performing quantum error correction to compensate for this. But it currently remains the case that: entangled states of two qbits are fairly routine; entangled states of a few qbits are really quite difficult; entangled states of many seem impossible...at the moment, but who knows?