

Last Lecture (given as Last Collection -June 2000)

First, I want to thank you for asking me to speak at this time. I may be the only professor asked to give Last Collection who has never been to one. Others would give you advice or tell jokes, I will stick to what I do best and present a Last Lecture about some startling results from the area of my research interest, quantum physics. The Last Lecture today is titled: **Superposition, Entanglement, Computing and Teleportation.**

During the past century, many strange properties of the microworld have been discovered by physicists. My goal today introduce you to amazing quantum effects that will affect you in this century.

At key points in human history, civilization has advanced because people discovered new ways of understanding and using nature. Urban society began when hunter gatherers learned how to farm land and domesticate animals. The control of steam power led to the industrial revolution. The classical digital computer began the information revolution and now quantum computers and quantum teleportation, which rely on quantum aspects of nature that are now totally unexploited by technology, are going to have a dramatic effect on our lives.

The idea of a quantum computer emerged when scientists were pondering the fundamental technological limits of classical computing. They realized that as engineers try to pack ever more logic gates onto silicon chips, they would eventually reach a point where the logic gates are so small that each is made of only a few atoms and they would be quantum systems, which obey very different rules those of the classical world.

At this time, Feynman showed how a quantum system could do computations using a property called **quantum parallelism.**

To understand **quantum parallelism**, we look at Young's double-slit experiment in which he projected a point source of light onto a plate with two narrow, closely spaced slits. As the light passed though the slits and subsequently reached a screen, it produced a pattern of dark/light regions called fringes, which Young said were caused by the destructive and constructive interference of classical light waves.

Although the classical wave theory of light seemed to explain the experiment, we now know that light is particles, called photons, and photons only emulate classical wavelike behavior for intense light sources.

Physicists have now studied the extraordinary experimental results that emerge when we reduce the light intensity so only one photon is passing through the apparatus at any given time. If we record the locations of each individual photon as it arrives at the screen and wait long enough, the same interference pattern as that of an intense source eventually appears. This occurs even though it takes many hours to accumulate the data one photon at a time-very non-wavelike behavior!!

We can try to determine which slit any particular photon actually passes through by doing extra measurements, but this always destroys

the interference pattern. So, if we try to determine how they got to the screen from the source, the photons behave like particles and do not interfere.

There are several ways that physicists have tried to make sense of this experiment.

The traditional explanation was to say that quantum objects like photons can behave like waves or like particles, depending on what an experiment required of them. If we do not try to determine on which path they travel through the apparatus, then they behave like waves and interfere. If we do attempt to determine their path, then they behave like particles and do not interfere. The wave interference argument is invalid, however, for the single photon experiments. There are no other photons to interfere with and they cannot interfere with themselves.

In fact, you end up saying the following: the photon did not go through slit A, the photon did not go through slit B, the photon did not go through both slits simultaneously, and the photon did not go through neither slit.

This exhausts all possibilities according to ordinary logic!!!

The modern explanation is "**superposition**". Superposition is "**none of the above**".

All quantum systems (a photon in this case) exist in multiple states. Classically, we can think of two ways the photon might get to the screen in the experiment. It passed through one slit or it passed through the other slit. QM says that we cannot continue to think of these paths as real since we cannot determine if the paths are actually traveled without ruining the experiment. We can show they pass through a particular slit, but not if we also want to see interference.

QM says that when a single photon passes through the apparatus in an interference experiment, what happens is that the photon passes through as a superposition of passing through each slit separately or as some combination of all the possibilities at the same time. It does not travel along either path. QM says that the photon only has probabilities for being on each path.

Using this scheme, QM is able to predict the probability that a photon will arrive at any particular point on the screen and hence predict the interference pattern. It does so correctly. However, along the way QM really messes around with the way we think about the world; messes with our view of **reality**.

QM says that when we are not measuring its path, the photon does not have a path. QM says that when we are not measuring its path, the photon is only a set of probabilities to have paths. QM says that when we measure its path, then the photon does have a path, namely, the one we found in the measurement. Measurement seems to destroy the superposition and create a definite value or a reality.

The path of the photon, in fact, all of the photon properties are only part of quantum reality when we measure them. In between

measurements, the photon is just a set of quantum probabilities.

Experiments now clearly show that this strange QM view is correct, which means that quantum systems seem to have no objective reality in between measurements.

So when QM says that the photon passes through the apparatus as a superposition of all the possibilities (two in this case), QM means that it seems to be doing all of those things simultaneously as long as we do not check by measuring to see what it is actually doing or as long as you do not measure it and make it do something definite. If you do check, then you destroy the superposition and reduce the system to only one possibility, namely, the one you found in the measurement. This is called **collapse of the superposition**.

The photon is exhibiting a **quantum parallelism** in a superposition because of nonzero probabilities for being on many different paths simultaneously.

You might ask at this point: How can such a theory make any sense? I would counter with the question: What do you mean by make sense? You might argue that it goes against your intuition. I would say that is OK because you have never been a photon and therefore you do not have any intuition about how photons should behave.

QM correctly explain all known experiments in the microworld correctly. It is the correct theory for all technology that relies on the behavior of atoms. The superposition idea is now universally accepted even though it says that the microworld is one of possibilities and probabilities instead of determinism as in the classical world.

We can exploit this idea. Since a photon can simultaneously be on multiple paths in the two-slit apparatus or in many states simultaneously, theory says it is possible to build a computer that computes using all the different states in a superposition simultaneously like an immense parallel processing machine.

One possible difficulty is that you can't look at the results of each computational path separately because it is part of a superposition. Just as in the two-slit experiment, looking destroys the superposition or interference. If you look, then you see only one part of the superposition and get only one result.

Does this say quantum parallelism is an illusion? Does it occur, but give us no way to make use of all of the results? There is a way to take advantage of all of the simultaneous calculations. We must not look at the results directly, but only allow parts of the superposition to interfere in some clever way. This is what happens when we get information from the two-slit interference pattern where interference occurs when we observe the position of photons as they interact with the screen. Likewise, in a quantum computer, interference can be achieved by observing the result of a calculation in the proper way so that we do not get a result from only one part of the superposition but get a sum or interference pattern over all the parts. If we are clever in asking the questions, then we can extract more than one piece of the calculation.

How to do it?

In human relationships, you may not know what your partner is thinking and this can cause all sorts of trouble. It is nothing, however, like the trouble that occurs for QM partners. For a pair of quantum particles, even a brief interaction creates a very strange bond. When involved in this bond and before being measured, both particles in the partnership are, not only, each in a state that is a superposition of possibilities, but also, the two sets of possibilities have a special relationship where they are dramatically correlated. A very strange quantum dance.

When the state of superposition of one is measured and collapsed to a single possibility, the state of superposition of the other is **simultaneously** collapsed to a single possibility correlated with its partner - even if halfway across the universe when the measurement on the partner took place.

In the strange lexicon of quantum physics, the two particles are said to be **entangled**. Entanglement occurs when quantum systems interact. Entanglement means that if you perform any kind of measurement on one of the particles, then it affects the partner even if they are separated by a large distance. This is called **quantum nonlocality**.

Entanglement was at the heart of a philosophical debate between Einstein and Bohr over the nature of reality in the quantum world. Einstein could not cope with the probabilistic or non-deterministic nature of the world of QM.

Einstein disagreed with the view that an electron in an atom has no definite state, but only possible states. That, at best, the theory can predict the probability that the electron is in a state. That the electron might not be in one state, but in a superposition of all states at once. That it is meaningless to try to describe the electron's state until a measurement is made, at which point the measurement destroys the superposition and causes the particle to be in a definite state.

Einstein felt that underlying quantum theory was an objective world in which all particle properties had real pre-existing values and measurements were just finding out what those values were and not creating any reality.

Einstein, Podolsky and Rosen (EPR for short), designed an experiment involving entanglement that was supposed to show that quantum theory gave an incomplete view of reality. They argued that the nonlocal bond of entangled particles was a physical impossibility because it had to act instantaneously everywhere and no known influence could travel faster than the speed of light according to Einstein's own special theory of relativity. Einstein dubbed these quantum influences - **spooky action at a distance**. At this time, an experimental lower bound on the speed of the quantum influence is 10 million times the speed of light.

Bohr, on the other hand, saw entanglement as a quantum fact of life. Entangled particles are essential parts of the same quantum system no matter how far apart they are. Although, we cannot measure any information-carrying signal passing between them, it turns out that

no matter how far apart they are, they cooperate during a measurement and end up with measurement values that are strongly correlated.

Knowing a quantum property of one particle in an entanglement tells you the same property of the other particle without having to measure it.

This nonlocality is best described by saying that quantum theory has a way of getting a feather in my hand in New York to tickle someone in San Francisco even though the feather is always observed to be in New York and the other person is always observed to be in San Francisco.

It was not until 1982 that a real version of the EPR experiment was built. It produced convincing results that supported Bohr's view of quantum reality. Today researchers are building more accurate versions of these EPR-type experiments to probe the boundary between the classical and quantum worlds. In all cases, the QM view of reality agrees with the experimental results. Bell, in fact, proved that any theory that agrees with all of the probabilistic QM predictions cannot be local. **Nonlocality and entanglement is a quantum fact of life.**

To understand how this all relates to the quantum computing revolution, we digress to understand binary numbers, their connection to classical and quantum computers and how superposition and entanglement come into play.

I will use some volunteers from the undefeated women's rugby team to help me demonstrate. Rhiana, Meghan, Alexa and Danielle.

A **bit** is a object that can be either 0 or 1. In a classical computer, it is a memory register whose voltage can be 0 or 5 volts.

1-bit register = 0,1

$$2^1 = 2 \text{ numbers}$$

2-bit register = 00=0,01=1,10=2,or 11=3

$$2^2 = 4 \text{ numbers}$$

3-bit register = 000=0,001=1,010=2,011=3,100=4,101=5, 110=6, or 111=7

$$2^3 = 8 \text{ numbers}$$

an L-bit register can store

$$2^L \text{ numbers}$$

The 10-bit number 1111101000= 2000 =1024+512+256+128+64+16

A **classical** 3-bit memory register can store **only one** of the eight numbers at any one time.

A quantum register composed of one quantum bit or a **Q-bit**, can store at a single moment of time **both** of the numbers 0 and 1 in a quantum superposition of being 0 and being 1. A quantum register composed of two Q-bits can store at a given moment of time **all four** numbers 00,01,10,11 in a quantum superposition being 0,1,2 and 3. A quantum

register composed of three Q-bits can store in a given moment of time **all eight** numbers 000,001,010,011,100, 101,110,111 in a quantum superposition 0,1,2, 3,4,5,6 and 7. All eight numbers are present in the 3 Q-bit quantum register at one time.

Quantum memory registers are in superpositions of all the register possibilities as long as we do not look at them. If we do look at them they become one of the possibilities or one of the numbers by collapse of the superposition.

If we keep adding Q-bits to the register we increase its storage capacity exponentially, four Q-bits can simultaneously store 16 different numbers, five Q-bits can simultaneously store 32 different numbers, etc.

Once the register is prepared in a superposition of different numbers we can perform quantum operations on all of them simultaneously. For example, if the Q-bits are atoms then suitably tuned laser pulses can affect the atomic states and evolve initial superpositions of encoded numbers into different superpositions, carrying out a complex mathematical task along the way.

During the evolution each number in the superposition is affected in a different way and as a final result we generate a massive parallel computation on a many-bit quantum memory register. This means that an L Q-bit quantum computer can, in one computational step, perform the same mathematical operation on 2^L different input numbers encoded in a superposition. To accomplish the same task, a classical computer has to repeat the same computation 2^L times or has to use 2^L different processors working in parallel. This is why computers using quantum parallelism will be so powerful.

At the beginning, however, quantum computers were only an academic curiosity. In order to get a definite result from a quantum computer, it seemed that we had to do a measurement, which always collapses the superposition of possibilities (the results) to only one result. That means, in a given time step, it seemed that both a quantum and a classical computer made the same number of calculations (L). Since, we already know how to build regular computers and do not yet know how to build quantum computers, why bother?

A quantum computer, however, has the ability to generate interference between the different results or states in the superposition.

Thus, to exploit quantum parallelism, one must only ask questions of a quantum computer that can be answered by some kind of interference and not by direct questions that collapse the possibilities to one. By doing a computation on a superposition, then interfering the results to get the answers, a quantum computer can exploit quantum parallelism.

No one, however, knew how to ask such questions. If quantum computers were to have any future, it needed a **killer application** - something very useful that only a quantum computer could do in a reasonable amount of time.

Peter Shor of ATT's Bell Labs, found the first true quantum computer algorithm. He derived a method using quantum computers to solve a

problem in number theory which has powerful real-world applications. Shor created a toolbox of mathematical operations that only work on a quantum computer. He showed how these operations lead to an algorithm that enables a quantum computer to factorize (like $15 = 5 \times 3$) huge numbers extremely rapidly, much faster than possible by conventional computers. Factorization is so important because a common method of encryption (RSA) relies on the extreme difficulty of factorizing very large numbers. Recently, a 129-digit number was factorized by over 1600 classical computers hooked up via the Internet, but it took over eight months! The RSA scheme relies on the fact that no efficient classical factoring algorithm is known and any set of classical computers can be defeated by adding more digits to the codes since factorizing numbers gets exponentially harder the bigger they are.

But then Shor dropped a second bombshell. He showed that a quantum computer would be able to factorize RSA-129 in a few seconds or be able to break **any** so-called "**uncrackable**" secret codes in seconds rather than years.

It does it by trying out very large number of cases simultaneously in a superposition with the calculations on every part proceeding in a massively parallel way. The actual results are obtained by allowing all the components of the final superposition to interfere with each other. Shor's algorithm was designed so that only results leading to a factor interfere constructively, while all the results that were not factors cancel out by destructive interference. The interference pattern produces the required answer!

There are many proposals to build a real quantum computer. As long as there is a way to put the system into a quantum superposition and there is a way to get the Q-bits to interfere, any system can be used as a quantum computer.

One proposal is to use the nanotechnology of **quantum dots**, that is, a single electron trapped inside a cage of atoms. When a single dot is exposed to a pulse of laser light of precisely the right frequency and time duration, its electron is put into an excited energy state. An additional pulse of light of same frequency and time duration puts the electron back into its ground state again. In a quantum computer, the ground state and excited state of the electron are used to represent 0 and 1 so that a single quantum dot can act as a 1 Q-bit memory register.

A quantum dot also behaves like another important device. A pulse of laser light turns a 0 (false) into a 1 (true), or a 1 into a 0, which is the same behavior as a NOT gate.

It turns out, however, and this is most important, that there are operations that can be done with these quantum dot structures or Q-bits that cannot be replicated by classical registers. It is here that we enter the strange world of quantum computing.

Consider the NOT gate again. The requirement is that you shine laser light of the right frequency for precisely the right length of time to cause a Q-bit to flip. What happens if we shine the light for half the prescribed time? According to quantum mechanics, the quantum dot does not flip, but instead goes into a superposition of both the excited and ground states (a superposition of being 0 and being 1).

This function behaves like the **square root** of a NOT gate.

The importance and significance of these square root functions is that they have **no analog** at all in conventional computers. You **cannot** make them in a classical computer.

These old and new logic functions made from groups of quantum dots are all the tools needed to construct a quantum computer.

To build a quantum computer, however, we would need over 100,000 dots on a single chip, which is not possible now. There is also a big difficulty with total computation time. The electrons in quantum dots tend to stay in their excited states for only about a microsecond. Since each burst of laser light lasts around 1 nanosecond, there is only time for about a thousand logical operations before all bits are erased. This puts a severe limit on the length of any quantum calculation.

In addition, physicists have only managed to entangle a maximum of three-to-four quantum systems. To factor a number like 15 would take 20,000 logic gate operations on 20 entangled particles. So practical quantum computation is still a long way off.

Remember, however, these are the early days of quantum computing and physicists are still trying to understand entanglement. There are many examples where once technology gets its foot in the door, advances come very rapidly. So watch out and watch for IPOs!!!

Now let me tell you about a **real working example** of a quantum computer. In this quantum computer, the Q-bits are the spin states of a proton, which exist as a superposition of both 0 and 1 (spin up and spin down) until a measurement is made. Lov Grover of ATT Bell Labs showed how a quantum computer could guess a chosen number in a certain range. The task is similar to the game of high/low-homing-in on a number by asking if the your guess is too high or too low. **Such repeated questioning would be all a classical computer could do.** Grover showed how a quantum computer could figure out the number in one try by packing all the questions into the superposed states of a Q-bit.

Isaac Chuang of IBM's Almaden Research Center and Neil Gershenfeld of MIT's Media Lab, one of my former students—a 1980 Swarthmore graduate, have made a quantum computer that works out one of Grover's algorithms, answering two questions about one of four numbers. This problem is similar to asking which of the numbers 1,2,3 and 4 is odd and greater than 2. Although a simple exercise, they showed that it can be done with a quantum computer in **one step**.

They used the nuclei of a carbon atom and a hydrogen atom in a chloroform molecule as two Q-bits. Both nuclei had spin 0 and spin 1 states, giving four combinations which existed simultaneously, 00,01,11 and 10. Using magnetic fields and radio waves in an NMR apparatus, they manipulated the atom spins, making them evolve in time according to the algorithm's logic. The correct answer to the calculation then came when a measurement of the spin states singled out, via interference, those states containing the correct answer. This work proved that a quantum computer was no longer just a theory!

The major difficulty is creating large enough entanglements. In addition, the entanglements are extremely fragile. Disturbing one member of an entangled pair destroys the superposition. Making a measurement is one way to do this, but random noise is even more insidious leading to **decoherence**, which is the arch enemy of entanglement. In order for a system to be effective, we must be able to do many operations before the quantum superposition decoheres. Decoherence is inescapable and gets worse as the entanglement gets larger. I believe, however, that decoherence can be controlled by a better understanding of how it works. I am very optimistic that we can make large entangled states very robust and quantum computers possible.

Now, the dream of **teleportation** is to be able to travel by disappearing at one location and simply reappearing at some distant location, without ever being anywhere in between. Captain Kirk and his crew do it all the time with the greatest of ease. This form of travel, however, has seemed to be science fiction and not a real possibility. It turns out that in the world of QM, teleportation is not only theoretically possible, it has actually been done.

For our purposes, an object to be teleported is characterized by all of its measurable properties. To make a copy of the object at a distant location, we need to send the measured information so that it can be used to reconstruct the object.

Until recently, physicists had all but ruled out teleportation because particles can exist in superpositions. The difficulty is that to produce an exact duplicate of any one particle, we need to determine all of its properties. But doing so, requires many measurements, each of which collapses the superposition. Since each collapse wrecks the superposition and hence the particle's properties, a second measurement is impossible on the same particle. In fact, QM says it is impossible to exactly measure all the properties of the particle at the same time. The more you learn about one set of characteristics, the less you can say about the others with any real certainty. This is real content of Heisenberg's uncertainty principle.

Although QM says we have this measurement problem if we try to gather information, QM also says that it is possible to transfer the quantum state of one particle onto another particle - the process of quantum teleportation - provided one does not get any information about the state of the particle in the course of this teleportation. This can be done by using entanglement in a clever way.

Experimental teleportation has now been done, at least for photons, over distance of up to 10 kilometers.

It is not Star Trek. No Beam me up, Scotty, no shimmering sparkles as someone materializes in the transporter room on the U.S.S. Enterprise. The experimental group has not sent a colleague to Katmandu or a car to the moon. Yet they did demonstrate that it is possible to transfer the properties of one quantum particle(a photon) to another even if the two are at opposite ends of the galaxy.

The solution was based on the fact that in an entangled state, both particles are part of the same quantum system so that whatever you do

to one messes around with its partner. The experiment used entangled photons to transport a polarization state from one photon to another.

Here is how the experiment works:

The diagram I have given you depicts the experimental setup for quantum teleportation.

At the sending station of the quantum teleporter, Alice encodes a **"messenger"** photon M with a specific state: say 45° polarization. This travels to a beam splitter. Meanwhile, two additional **"entangled"** photons A and B are created. Because of entanglement, each photon is in a superposition of two polarization states and the two photons have a strong correlation - they always have opposite polarizations. If A is measured to have horizontal polarization, then B collapses into the opposite state of vertical polarization. Now entangled photon A arrives at the beam splitter at the same time as message photon M. The beam splitter causes each photon to either go to detector 1 or go to detector 2. In 25% of all cases, the two photons go to different detectors, 1 and 2. Alice, however, cannot tell which photon went to which detector. Alice's inability to distinguish between the two photons causes quantum weirdness to kick in.

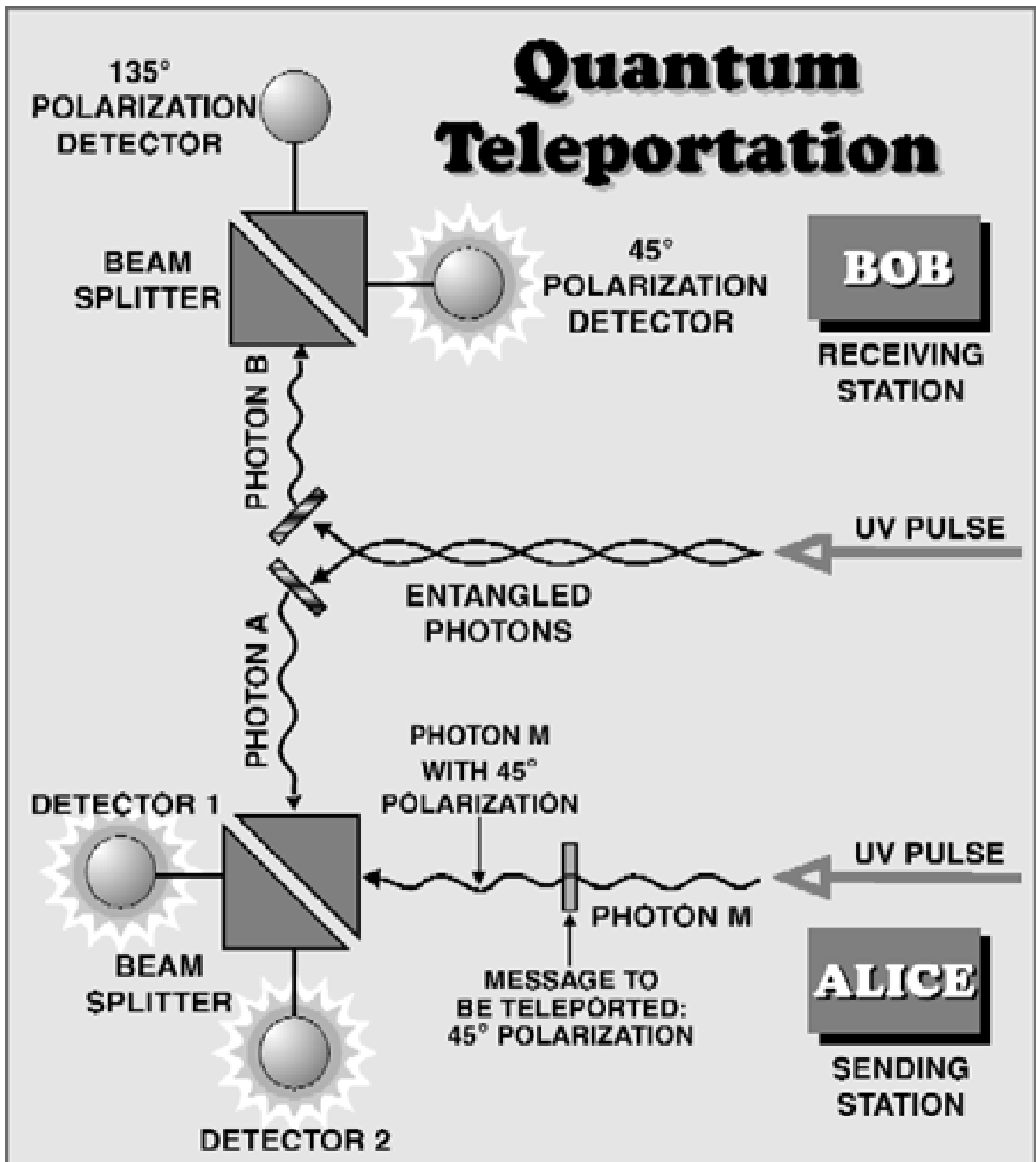
The fact that the two photons A and M are now indistinguishable allows QM to say M becomes entangled with A. The polarization values for photons A and M are now opposite. At that instant, since message photon M must have opposite polarization to photon A, then photon B, which is also entangled with A, must also be opposite to A and now have the same polarization value as M. Therefore, teleportation is successful. The polarization value of photon B when B arrives at Bob, is the value of the message photon M.

During teleportation, particle M loses its identity as it becomes entangled with particle A and the initial state of M is destroyed.

The measurement does not reveal any information about the properties of any of the particles, which is why the entanglements are not collapsed. The teleportation of quantum information from particle M to particle B can happen over arbitrary distances.

After successful teleportation particle M is not available in its original state any more and therefore its twin, particle B, is truly the result of a teleportation. The scheme does not teleport the photon itself, it only transports its properties which are imparted to another, remote photon.

Science fiction coming true!



So here are my final thoughts.

Relativity ensures a degree of separateness and individuality for distant parts of the Universe because of its imposition of a maximum speed of light for information transfer. Quantum entanglement, maintains links between distant regions, and keeps the whole the Universe coherently connected. Randomness and superposition make it possible to tie distant parts of the Universe together more tightly than might otherwise be imagined, while ensuring that cause and effect stay distinct and causality is maintained. Quantum mechanics manages to combine nonlocality and causality so that everything works in harmony.

Do we have any other choice but to use quantum rules? Is quantum mechanics the only theory that can reconcile nonlocality with relativity and causality? Can quantum theory be modified and still be consistent with the experimental world?

If you try to alter the theory very slightly say by adding some extra feature like nonlinearity, then quantum nonlocality immediately becomes malignant. It allows faster-than-light signalling which then leads to the possibility of time travel and all kinds of logical difficulties with causality. It seems that quantum theory as presently known is the only one that is consistent with all evidence. At this time, we know that the universe uses quantum mechanics, but we do not why that must be so as yet.

Many philosophers and physicists believe there is a need for a radical change in the very modes of thought that we use. For instance, after Einstein introduced his theory of relativity we threw out the old Euclidean notions of space and time, and now have more generalized notions, which work even better.

Quantum theory may demand a similar revamping of our concepts of rationality and logic. Boolean logic, which is based on true-false propositions, suffices for a world in which an atom goes either through one slit or the other or for your classical world, but may not suffice in a world of superpositions. Quantum mechanical logic seems to be non-Boolean. Someday we may know why.

Until then, like ancient cave dwellers, we can only stare at the shadows of quanta flickering on the walls of our cave, and wonder what they mean.

Thank you.