1 The Problem of measurement

According to the Copenhagen Interpretation we can only speak meaningfully about the attributes of a quantum system after a measurement has been made. At the point of measurement, the wave function collapses to an eigenstate. But how do we decide the point of measurement? How do we separate system, apparatus, observer? When does collapse occur? We cannot make meaningful statements about a measurement without including the entire experimental context. Until a measurement is made, we have seen that a system persists in a linear superposition of states and its evolution is unitary (a unitary transformation preserves scalar products, which includes, of particular relevance here, probability amplitudes) and governed by the Schrödinger equation, which is linear. Indeterminacy enters when a measurement is made, and the wave function collapses, or in other words is reduced. The reduction of the wave function is referred to by Penrose as the R-process, while unitary evolution is called the U-process. The R-process is irreversible and non-unitary, not governed by the Schrödinger equation. A measurement involves the magnification of quantum events to the classical level.

But where does the boundary lie between the quantum system subjected to measurement and the measuring apparatus? If we assume that the world can be divided into a microscopic quantum system on which measurements are made by a macroscopic measuring apparatus that obeys classical mechanics exactly, no problem arises. But if quantum mechanics is a universal theory then all measuring devices should also be subject to quantum effects. For example, in the case of polarised light incident at 45^o to a polariser, the incoming state is a superposition of two states, one parallel, the other perpendicular to the polariser. The measuring apparatus will thus also have two states, each correlated to one of the two polarisation states of the photon. If the laws of quantum mechanics are applied to the detector, then it too passes into a superposition of states. Von Neumann concluded that the measuring apparatus can only be deemed to have made an act of measurement when it too is subjected to a measurement and collapses into one of its possible states. But the second measuring device requires a third to make it collapse, the third a fourth, and so on, leading to an infinite regression, which is known as a von Neumann chain.

Suppose we have an observable A (e.g. a spin) with eigenvalues λ_n associated with a measured system Q (e.g. an electron) and a measuring device M to measure the value of A and record the result of the measurement. The recorded result must always be one of the eigenvalues of A, λ_n. We will assume that M has only one degree of freedom, the position of a pointer on a scale. A measurement involves an interaction between the quantum systems Q and M. If before the interaction (measurement) Q is in an eigenstate $\mid 1 >$ of A with eigenvalue λ_1, and M is in a state $\mid \phi_0 >$, then the combined system is in a state

$$\mid \psi_b >= \mid 1 > \mid \phi_0 >$$

After the interaction it will be in a state

$$\mid \psi_a >= \mid 1 > \mid \phi_1 >$$

where $\mid \phi_1 >$ is the wave function of M with the pointer in the position corresponding to λ_1.

But if Q is initially in a linear superposition of two states $\mid 1 >$ and $\mid 2 >$ the combined state before interaction will be

$$\mid \psi_b >= (c_1 \mid 1 > + c_2 \mid 2 >) \mid \phi_0 >$$

but after it the state will be

$$\mid \psi_a >= c_1 \mid 1 > \mid \phi_1 > + c_2 \mid 2 > \mid \phi_2 >$$

which is a linear superposition of two states in one of which the pointer is at "λ_1" and the other at "λ_2".

For example, if prior to measurement a spin one half particle is in an eigenstate of S_x which has eigenvector $\frac{1}{\sqrt{2}}(\alpha + \beta)$ the total wave function is

$$\mid \psi_b > \frac{1}{\sqrt{2}}(\alpha + \beta) \mid \phi_0 >$$

and after a measurement of S_z it is

$$\mid \psi_a >= A\alpha \ \mid \phi_\alpha > + B\beta \ \mid \phi_\beta >$$

This last equation implies that the detector after measurement is in a linear superposition of $\mid \phi_\alpha >$ and $\mid \phi_\beta >$. The wave function $\mid \alpha\phi_\alpha + \beta\phi_\beta >$ may be appropriate to describe a microscopic system but not a supposedly macroscopic one like a detector. It would give rise to macroscopic interference effects, which are not observed. In such a state, the detector's pointer, which is supposed to indicate which state Q is in, would fly about, delocalised between two positions, unable to know which way to point! The equation contradicts the idea of collapse of the wave function, which should require, after measurement, the combined systen to be in either $\alpha \ \mid \phi_\alpha >$ or $\beta \ \mid \phi_\beta >$. It hasn't collapsed, and the detector is left in two states at the same time. (This is scarcely surprising since nowhere has any mechanism of collapse been introduced into the theory.) A second measurement would be required to collapse it. But the second device could be considered part of an extended combined system, particle plus first apparatus plus second apparatus, which on measurement would also go into a superposition, not collapsing until in turn a measurement was made by yet another apparatus. And so on, ad infinitum. Where should the line be drawn? Until something acts to collapse the wave function, all macroscopic systems should remain as superpositions of states. But we are not accustomed to seeing,say billiard balls, in superpositions of different states.

However, recent experimental studies with a superconducting quantum interference device (SQUID) have revealed that simple macroscopic systems can be put into a superposition of two states (A "Schrödinger's Cat" state, see next section) and with the advance of nanotechnology quantum behaviour may soon be observed to extend to other systems.

2 Schrödinger's Cat.

Schrödinger illustrated how the problem of measurement could appear at the macroscopic level in a graphic thought experiment involving an unfortunate cat. A cat is penned up in a sealed box, together with the following device; in a Geiger counter there is a small piece of radioactive substance such that in the course of one hour one of the atoms decays, or none of the atoms decays, with equal probability. If a decay occurs, the counter tube discharges and through a relay releases a hammer that shatters a flask of hydrocyanic acid. If after one hour an atom has decayed, the cat will be dead, if not, it will be alive.

According to the rules of quantum mechanics, the cat in the box is supposedly in a superposition of states, live and dead, with a feline wave function

$$|\Psi >= C_l \ |undecayed \ \ atom; live \ \ cat > + C_d \ |decayed \ \ atom; dead \ \ cat > .$$

Until the box is opened, the cat remains in this limbo state of alive-dead, but when it is opened, the cat collapses into either a live state or a dead state with equal probability. But

before that, how can we attach meaning to a live-dead cat? When the observer opens the box, does he or she go into a superposition of

$$| \textit{observer in state } l;\ \textit{undecayed atom};\ \textit{live cat} >$$

plus

$$| \textit{observer in state } d;\ \textit{decayed atom};\ \textit{dead cat} >$$

until another observer comes along and performs a measurement on the first? And how would the cat feel about being in a superposition of alive and dead? Wigner devised an experiment (imaginary, it is to be hoped) in which the cat was replaced by a human (Wigner's friend), definitely a conscious being. What would be going through his mind in such a state ?

Schrödinger did not believe that a cat could be placed in a superposition of live and dead states, that his equation could be applied to a system as large and complex as an animal. Therefore this implied there was some incompleteness in quantum theory and in the Schrödinger equation. Many authorities disagree on this, but Schrödinger remains entitled to his opinion - after all, it was his equation he was talking about.

In traditional quantum theory, a measurement is regarded as the interaction of a microscopic system, which obeys the laws of quantum mechanics, with a macroscopic one, the apparatus, which obeys classical mechanics. It is as if there are two sets of laws, one for the microscopic and another different set for the macroscopic, with no quantitative limiting process that takes one into the other. Ian Percival of Queen Mary, University of London has pointed out that this scheme resembles that of the ancient Greeks who believed in one set of laws for the heavens and another for the earth.

A quantum system cannot be considered in isolation; it interacts with the environment, and when an experiment is carried out, with the apparatus, which must also be regarded as part of this environment. All these parts should be subject to the same laws of physics.

Many physicists never pursue the logic of the quantum theory of measurement to its ultimate extreme. Somewhere along the unending line of detectors it is assumed that one of them somehow "turns into" a classical, deterministic system that gives a macroscopically detectable result. But the details of how and at what stage this occurs are left vague and do not stand up to close scrutiny.

3 Mind and Matter.

Some scientists, notably **Wigner**, have advocated the view that the chain is brought to an end only when a conscious individual is involved and the result of a measurement enters that individual's mind. It is only a conscious mind that brings about the irreversible collapse that characterises a measurement. But, one might ask, does the individual have to be human? Will a cat serve as the final observer? Or an insect, or an amoeba? Would any complex adaptive system do? Who or what was responsible for collapsing wave functions throughout the cosmos before life evolved on this obscure planet? And what is special about a conscious mind, (which is, after all, composed of quantum particles) that prevents it, too, from being put into a superposition of states, (leaving aside the confused mental state which that could induce.) We know far too little about the mind or the brain to begin to answer such questions. And if, as it seems reasonable to assume, conscious minds are sparsely distributed throughout the universe, there must be vast regions of the cosmos where everything remains in a state of pristine, uncollapsed, quantum superposition! Wigner's view seems to suggest that Mind (however that may be defined) has influence over matter, that some *deus ex machina* from outside the sphere of physics intervenes to effect final collapse of the wave function. The microscopic/macroscopic boundary is replaced by the matter/mind interface.

The problem of the nature of Mind has preoccupied philosophers for as long as there have been philosophers. Wigner's solution to the collapse of the wave function recalls Descartes' theory that Mind (or Soul, as he called it) is a type of substance, different from matter, not interacting with it except in the human brain where by exercising volition it can change the direction of motion of the "vital spirits" and thus, indirectly, other parts of the body. This view was later dropped by his followers when found to conflict with momentum conservation.

All rigidly deterministic philosophies are difficult to reconcile with the concept of free will. Thus when quantum mechanics emerged, declaring that nature was indeterminate, it was immediately recognised that this provided a release from the mechanistic viewpoint and could readmit free will, via the uncertainty principle, which, permitting a range of outcomes from any state, makes it possible to conjecture that Mind could play a role in deciding between alternatives presented to the brain.

4 Irreversible Processes and Indelible Records.

So long as a quantum system can be considered isolated, its time evolution is governed by unitary operations and it follows the TDSE. However, if a measurement is made, a non-unitary, irreversible operation ("collapse", or "the R-process") occurs on the system, the results of which cannot be undone. An indelible record has been made. The system, regarded as an ensemble, has gone from a pure state to a mixed state. (In a pure state, particles have a unique state vector, which is in general a superposition of states, while a mixed state is a probability mixture of different eigenstates each with its own state vector; there is no unique wave function.) The collapse of the wave function cannot be described by the TDSE. However, if we include the apparatus and consider the combined system, and assume that after interaction takes place it goes into a superposition of common eigenstates of quantum system + apparatus, unitarity is preserved and a TDSE (though perhaps a very complicated one) will be followed. Since no wave function collapse has taken place, it may not be said that a measurement that created an indelible record has been made. Bohr called the irreversible operation that leaves an indelible record a "process of irreversible amplification". Quantum effects are magnified to the classical level. Wheeler has maintained that a measurement, in order to be regarded as such, entails two stages, the first, the process of irreversible amplification – such as the blackening of a grain of photographic emulsion in a camera by a photon – followed by the act of putting the result of the process to use, thereby establishing meaning by communication of knowledge. The second stage is not always accomplished – for example, if the camera is destroyed immediately after the grain is blackened, the result of the first stage is not put to use and no knowledge is gained. It does not have to be carried out by a conscious being like a physicist; any other complex adaptive system, self-aware or otherwise (the information gathering and utilising system (IGUS) of Gell-Mann and Hartle) will do. It consists of noticing that a particular alternative has occurred and including the observation in a database of some kind.

5 The Path-Integral Approach.

Richard Feynman, developing some original ideas of Dirac, described an alternative perspective to that of Schrödinger, Bohr and Heisenberg. According to this picture, a particle such as an electron, in travelling from point A to Point B, traverses **Every possible path simultaneously.** The probability of the particle arriving at point B starting from point A is given by the squared modulus of an amplitude (or kernel)

$$K(b,a) = \int_a^b e^{\frac{iS(a,b)}{\hbar}} \mathcal{D}x(t)$$

where $S(a, b)$ is the action function and $\mathcal{D}x(t)$ is notation for integration over all possible paths. This includes some that involve trips round the galaxy and beyond.

The probability that the electron arrives at B is built up from the combined ways of getting there. Some of these ways will interfere with each other. The electron is regarded as a particle, there being no associated probability wave, but the calculated probability of arriving at B is identical with that predicted by the wave function approach.

In the classical limit, all paths but one, the classical path, cancel each other out. This path is precisely the one obtained from the classical principle of least action, which leads directly to Newton's laws of motion.

6 Alternative Interpretations and Modern Approaches

Despite the apparent paradoxes and unsatisfactory features of the Copenhagen Interpretation, it virtually reigned supreme for over fifty years. Naturally, during this time there have been dissident voices and attempts have been made to devise alternative interpretations. The hidden variable theories, such as that of Bohm, constitute one class of alternatives and have already been mentioned. A good account of the Bohm-Hiley theory is given in the book by Rae.

An upsurge in interest starting in the early 1980s, was spurred on in part by modern techniques which have enabled experiments to be performed that were previously impossible. We can now look at a single atom, or build up macroscopic systems in a quantum way, and carry out delayed choice experiments.

It is when we come to apply quantum theory to the entire universe – quantum cosmology – that we encounter seemingly insoluble problems with the Copenhagen Interpretation. There is now no possible external measuring device to create an irreversible act of amplification, no possibility of an external observer to collapse the wave function of the universe. The usual lines of reasoning fail completely to give meaning to quantum cosmology. This has led physicists to seek entirely different approaches. Some of these will be discussed in what follows.

6.1 The Many-Universes Interpretation

This view, first put forward by Hugh Everett, proposes that when a measurement is made the universe splits into a number of copies, in each of which one of the possible outcomes is realised. (Clearly, in most cases the number is infinite.) There can be no communication between these different universes. When we measure the spin component of an electron the universe branches into two copies, in one of which the electron has spin up, in the other, spin down. In the cat experiment, two branches appear, in one of which the observer finds a dead cat, in the other, a copy of the observer finds a live one. Both observers believe their universe to be unique.

Proponents of this theory say that after the initial one, no further assumptions are necessary, giving it simplicity; the theory is free from the difficulties of the Copenhagen Interpretation. There is no collapse of the wave function since each alternative universe contains one of the possible outcomes of the measurement.

The idea sounds bizarre and mind-stretching, in postulating an infinity of parallel worlds each of them inhabited by one of an infinite number of copies of each of us. Each time any kind of measurement is made the universe branches again into myriads of further copies of itself.

What constitutes a measurement is not made clear.

Its opponents protest that it introduces "excess metaphysical baggage": to postulate an infinity of universes, only one of which we experience, to explain a technical point like wave function collapse looks like the antithesis of Occam's Razor ("Entities are not to be multiplied without necessity" or "It is vain to do with more what can be done with fewer")

Also, being limited to one universe we could never either confirm or refute the existence of all the others. The many-universes or many-worlds interpretation tends to be favoured by those In the scientific community researching in the field of quantum information Theory. David Deutsch has formulated a modified form of many-universes theory in which there are a pre-existing number of universes, always the same in number. When the world is faced with quantum alternatives, instead of branching and proliferating, they partition themselves into groups, in each of which a different outcome happens. The universes exist in parallel, and change in content and complexity, in accordance with the principle of the increase of entropy following from the second law of thermodynamics. Deutsch has even devised an experimental test to confirm or deny his hypotheses.

6.2 Pure and Mixed States.

A fermion has an intrinsic angular momentum, which we call its spin, whose component along a given axis is $\pm\hbar/2$. It thus carries around with it a preferred direction or orientation. Similarly, a photon carries with it a preferred direction called its polarisation. (A classical electromagnetic wave is composed of oscillating electric and magnetic fields perpendicular to its direction of propagation, and the direction of polarisation is that of the electric field vector.) An ensemble of identical fermions all with spin in the same direction is said to be spin-polarised in that direction. An emsemble of identical photons all with polarisation vector in the same direction is said to be plane polarised in that direction. Thus a beam of electrons all with spin-up in the z-direction is spin-polarised in the positive z-direction, while a beam of photons all with polarisation vector along a horizontal axis is horizontally polarised. In a **PureState** of an ensemble, every member has the same state vector ψ. This may be an eigenstate, but more generally a superposition of states of the form

$$\psi = a\psi_a + b\psi_b$$

In such a state there is the possibility of interference taking place as the probability density is

$$\mid \psi \mid^2 = \mid a \mid^2 \mid \psi_a \mid^2 + \mid b \mid^2 \mid \psi_b \mid^2 + a^* b \psi_a^* \psi_b + b^* a \psi_b^* \psi_a$$

the third and fourth terms being interference terms. Because states of the superposition can interfere, it may be called a **coherent** superposition. Each particle in the ensemble is in the same superposition of states. A **Mixed State** on the other hand is a probability mixture. There is no unique state vector; a fraction of the particles f_1 has state vector ψ_1, a fraction f_2 has state vector ψ_2 and so on. In a mixture of two states for example each particle is in **either** state 1 or state 2, not in a superposition of them. A measurement will yield state 1 with probability f_1, and so on. There is no interference in a mixed state of an ensemble.

Decoherence is the process whereby a pure state is converted into a mixed state. It can be used to explain the transition to the quasi-classical, apparently deterministic, domain that includes everyday experience.

6.3 Decoherence

The state vector of a cat, dead or alive, or any comparable macroscopic system such as a detector in an experiment, is complicated in the extreme, and depends on an enormous number of variables, perhaps 10^{25} or so. The states of a system such as

$$\psi_a = A\alpha\phi_\alpha + B\beta\phi_\beta$$

(where A and B are constants) must be considered as an entanglement of an enormous number of states.

This effect of this is to convert an initial **pure state** which has a wave function and is a superposition, into a probability mixture of states, a **mixed state**, which does not exhibit interference, by decoherence.

Consider an ensemble represented by the wave function $\mid \psi_a >$, and consider an operator $\hat{Q}$ which represents some physical operation on the whole system of particle-plus-detector. In a pure state $\mid \psi_a >$ the expectation value of $\hat{Q}$ will be

$$< \hat{Q} >= \int (A^* \alpha^* \phi_\alpha^* + B^* \beta^* \phi_\beta^*) \hat{Q} (A \alpha \phi_\alpha + B \beta \phi_\beta) d\tau$$

where the integration $d\tau$ is over the vast number of variables required to describe the state of the particle plus measuring apparatus (which may include a cat.)

The expectation value $< \hat{Q} >$ can be written as

$$< \hat{Q} >= \mid A \mid^2 Q_{\alpha\alpha} + \mid B \mid^2 Q_{\beta\beta} + A^* B Q_{\alpha\beta} + A B^* Q_{\beta\alpha}$$

where

$$Q_{\alpha\alpha} = \int \alpha^* \phi_\alpha^* \hat{Q} \alpha \phi_\alpha d\tau$$

etc. The terms $Q_{\alpha\beta}$ and $Q_{\beta\alpha}$ are the interference terms. If they are zero, then the expectation value is

$$< \hat{Q} >= \mid A \mid^2 Q_{\alpha\alpha} + \mid B \mid^2 Q_{\beta\beta}$$

which is the weighted mean of the expectation values of the states $\alpha\phi_\alpha$ and $\beta\phi_\beta$ or the expectation value in a mixed state in which a fraction $\mid A \mid^2$ are in the state $\alpha\phi_\alpha$ and a fraction $\mid B \mid^2$ in the state $\beta\phi_\beta$. This shows that loss of interference makes a pure state indistingishable from a mixed state. This is decoherence. Model studies have shown that under typical conditions under which measurements take place, macroscopic superpositions decohere with a decoherence time, or the time in which interference terms fall to zero, so small that the interference effects can be safely ignored for most practical purposes.

Thus Schrödinger's cat, a macroscopic object, will initially be in a superposition

$$\mid cat >= a \mid alive > + b \mid dead >= \sum_l a_l \mid l > + \sum_d b_l \mid d >$$

There are a vast number of scenarios describing "dead cat" or "live cat", countless billions of ways in which the cat can differ in fine detail or interact with its environment. These states will interfere, but the interference terms between them will sum to zero on average after a characteristic time, the decoherence time. It has been shown that the decoherence time is very short indeed, the cut-off of interference terms being exponential or faster, so if the cat is ever in a superposition of live and dead states, it is only for an unmeasurably short time.

In summary, in the Schrödinger's cat experiment, there is no quantum interference between live and dead cat scenarios. They decohere.

When the box is opened the situation is then no different from the classical one in which the cat, after having suffered a long air journey imprisoned in the box, is found, on opening it, to be alive or dead with different probabilities.

Already an experiment has been carried out by Brune, Hagley, Dreyer, Maître, Maali, Wunderlich, Raimond and Haroche in which decoherence has been detected using Rb atoms in superpositions of states interacting with electromagnetic waves in cavities. The measurement is made under conditions like those of Schrödinger's cat.

Decoherence may deal with the problem of superposition of macroscopic states, but it says nothing about collapse.

In the field of quantum information, which depends on the existence of superpositions of states, decoherence appears as an obstacle that has to be overcome.

6.4 The Ghiradi-Rimini-Weber (GRW) scheme

In the GRW model, the Schrödinger dynamics governing the evolution of the wave function is modified by introducing stochastic and non-linear effects that leave all standard quantum predictions about microsystems practically unaltered. The wave function, as it evolves according to the Schrödinder equation is subjected at random times to spontaneous processes corresponding to localisations in space of the microconstituents of any physical system. It is assumed that a spreading wave packet is suddenly, with very low probability, subject to a "hit" that has the effect of multiplying it by a Gaussian function. The probability that the peak of the Gaussian finds itself at a particular place is proportional to the squared modulus of the wave function at that location. These Gaussian hits occur roughly once every 10^8 years. The chance of it happening to a single particle within a period of one second is 10^{-15}, or in other words negligible. But any such hit would affect the entire state of any macroscopic object or environment interacting with the particle entangled with it. For a cat containing some 10^{27} particles one might expect a hit within 10^{-12} seconds. One of these particles would almost instantaneously receive a Gaussian hit, and as this particle would be entangled with the many other particles making up the cat, the reduction of the particle would drag all the others with it causing the entire cat to find itself in a state of life or death. As in the case of decoherence, linear superpositions are suppressed in extremely short times. The GRW scheme may be criticised on the grounds of its being very ad hoc; it is not based on any known laws of physics. The widths of the Gaussians and the time between hits were chosen purely to obtain reasonable results. The model also involves a small violation of the principle of conservation of energy.

6.5 Gravitationally Induced Reduction.

Standard quantum theory and general relativity do not form an easy partnership. The curved-space notions that Einstein's theory of gravity demands do not fit well into the framework of quantum mechanics. Attempts to produce a unified theory of quantum gravity have so far been unsuccessful. Eventually, a satisfactory theory may evolve out of modified versions of current quantum mechanics and general relativity. Some physicists, like Penrose, believe that the incorporation of the effects of gravity into quantum mechanics could provide an explanation of wave function reduction as a real physical process. Suppose a system evolves by Schrödinger evolution into a linear superposition of two states that occupy significantly different locations in space. The evolved state must then involve a superposition of gravitational fields which according to general relativity, have different space-time geometries. We would thus have two different space-time geometries superposed! According to Penrose, reduction of the wave function could occur if the geometries (space-times) of superposed states became so different from one another that they were unable to coexist. The hypothesis is that superposed, widely different states are unstable towards reduction, with a rate somehow dependent on a measure of the difference between them.

6.6 Concluding Remarks.

Recent studies have gone some way towards resolving or explaining the paradoxes and curiosities of standard quantum mechanics. Plausible alternatives to the Copenhagen Interpretation have been proposed. However, paradoxes do remain. Double Bell-type thought experiments have been devised that, when relativity is included, lead to forbidden causal loops which are hard to explain away. Finally, there is the problem of quantum gravity. General relativity and quantum mechanics still coexist uneasily and a reconciliation in the form of a unified theory is still awaited by physicists, astronomers and cosmologists.

At the same time, experimental techniques are becoming increasingly sophisticated and promise to shine fresh light on interpretations of the theory.

7 Quantum Information: Exploiting "weirdness".

It may come as a surprise to learn that quantum properties such as superposition, coherence, entanglement and the EPR effect are finding practical applications.**Quantum Information** is currently a burgeoning area of research.

The fact that a quantum system may be in a superposition of states and the non-local nature of entangled states can be turned to our advantage in the new fields of quantum computation, quantum cryptography (the sending of unbreakable ciphers) and quantum teleportation.

7.1 Information Theory.

The elementary unit of information theory is the bit (binary digit.) Any system, classical or quantum, with two well-defined states can be used to define bits which can take on two values, usually called 0 and 1. A classical system can reside in either state 0 or state 1, an example being the off and on positions of a switch. But a quantum system can exist in a superposition of states, both 0 and 1 at the same time in different proportions:

$$|\Psi >= c_0|0 > +c_1|1 >$$

In practice, the spin of a fermion, polarisation of a photon, energy levels of an atom, the states of trapped ions, and many other systems could all be used to define quantum bits, or qubits, as they are called.

7.2 Quantum Computers.

A quantum computer is based on the fact that any two-state quantum system can be prepared in a superposition of its two logical states 0 and 1; a qubit can store both 0 and 1 simultaneously in some proportion. The probability of obtaining on measurement the value 0 is $\mid c_0 \mid^2$ and the value 1, $\mid c_1 \mid^2$. A classical register composed of L physical bits can store any one of 2^L binary numbers, whereas a quantum register can store up to 2^L binary numbers at the same time in a superposition. For L=250, say, which could be formed by a string of 250 atoms, this equals 10^{75}, a colossal number. Unfortunately, the laws of quantum mechanics only permit us to see one of them if we measure the resister's contents. Mathematical operations can however be performed simultaneously on all of them, initial superpositions evolving into different superpositions. Thus a massive parallel computation that would require 2^L classical processors in parallel, or a single computation repeated 2^L times, can be performed in a single step. Although a quantum computer can hold all the outcomes of 2^L computations, since quantum mechanics only allows us to see one of them, there is no great gain in bulk information storage. However, it has been demonstrated that quantum computers can offer spectacular gains in the use of time and memory in certain types of algorithm such as searches or factorisation of very large numbers. To find the prime factors of a number containing 100 binary digits classically would take 10^{44} seconds (the age of the universe is 10^{17} seconds). Using quantum computational methods this could be achieved in a few seconds. Research into quantum computers based on, among other physical systems, trapped ions and nuclear magnetic resonance is currently being carried out in several countries. Construction of logical gates has already been demonstrated. One major practical obstacle that needs to be overcome is that of decoherence, the enemy of quantum computing, which destroys the superpositions of states upon which it relies, which need to persist for sufficiently long times.

7.3 Quantum Cryptography.

Cryptography is the art of disguising messages or any kind of information by means of secret codes that are difficult to crack by an outsider. Quantum mechanics at last offers us the means of creating codes that are undecipherable. In quantum cryptography binary information is hidden in a jumbled string of bits that is meaningless to anyone who does not know the key. It has been demonstrated by sending polarised photons through optical fibres tens of kilometres long, and even through free space. The sender (Alice) and the receiver (Bob) generate a secret sequence of binary digits (a key) known only to the two of them, thus providing perfect security. The key may then be added to any message that has been encoded in binary form, and transmiited over a public channel like email to the receiver who subtracts the code and thus reveals the original message.

The way in which the key is generated is the following:

A source of photons is available to Alice, who is in possession of two polarisers, one of which can linearly polarise photons vertically, and the other at 45^0. She assigns binary digit 0 to vertical polarisation, 1 to 45^0 polarisation. Bob has two analysers that can measure photons linearly polarised at -45^0 and horizontally, to which he assigns 0 and 1 respectively. Vertical polarisation is equivalent to an equally weighted superposition of $\pm 45^0$ polarisations, and 45^0 polarisation to a similar superposition of vertical and horizontal. Alice chooses a polariser at random, and sends the photon to Bob, who chooses an analyser at random and records whether or not he detects a signal. If, for example, Alice has sent a Vertical photon and he has chosen the -45^0 analyser, he has a fifty-fifty chance of detecting a photon. If he does detect a signal, it is easy to see by considering all possible combinations, that it is certain that he and Alice have both selected the same binary digit. Bob communicates openly to Alice whether he has (Y) or has not (N) received a photon. Alice and Bob retain only the bits for which a photon was received and use this string as a secret key.

For example, suppose the key is 01101001 and Alice wants to send the message " My password is szarasz.vörösbor", which she expresses as some binary equivalent 10110101. Adding, she gets 11011100, which she sends to Bob. He subtracts 01101001 from 11011100 and obtains 10110101, the original message.

An alternative method makes use of entanglement to generate strings of randomly generated qubits known to two people and no one else. It works in the following way: A supply of entangled photons is available to two Alice and Bob. Of each pair, one photon goes to Alice, the other to Bob. They agree to make a long series of plane polarisation measurements on their photons, half the time distinguishing between two perpendicular directions (x,y) and the other half between directions (X,Y) rotated by 45^0 to (x,y). Before each measurement, the pair of axes is selected at random. Alice and Bob work independently. When the measurements are finished, they openly exchange information about which kind of measurement was made on each photon, so that they learn on which occasions they made the same measurement. They then know that because of the EPRB effect, the results of each common measurement must be the same. But only Alice and Bob know what they are. They are in possession of a secret string of digits that can be used as the basis of a code to send encrypted messages to each other. They can even eliminate the effects of an eavesdropping spy by openly comparing a sample, later to be discarded, of their results to check if they are identical. If a spy, Eve, has been intercepting photons, a discrepancy will occur on roughly 1 in 4 occasions and destroy the exact agreement between Alice and Bob's results in the sample.

7.4 Quantum Teleportation.

Although the possibility of teleporting complex macroscopic bodies like human beings still belongs strictly to the realm of science fiction, simple quantum teleportation has been demon-

strated, also making use of the properties of entangled photon states, the Bell states. These are the four superpositions

$$| \Psi^+ >= \frac{1}{\sqrt{2}}(| 1 >| 0 > + | 0 >| 1 >)$$

$$| \Psi^- >= \frac{1}{\sqrt{2}}(| 1 >| 0 > - | 0 >| 1 >)$$

$$| \phi^+ >= \frac{1}{\sqrt{2}}(| 1 >| 1 > + | 0 >| 0 >)$$

$$| \phi^- >= \frac{1}{\sqrt{2}}(| 1 >| 1 > - | 0 >| 0 >)$$

The Bell states can be created in the laboratory by e.g. non-linear crystals. An experimenter can switch from one Bell state to another by performing an operation on one of the qubits: phase shift (change of sign), bit-flip (e.g. $| 0 >\rightarrow| 1 >$), combined phase shift and bit flip, and the identity operation (do nothing). All four operations can be performed on polarised photons using wave plates (polarisers), mirrors or non-linear crystals.

Alice wants to teleport a teleportee photon A in an unknown quantum state

$$| T >= u | 1 > + v | 0 >$$

where u and v are probability amplitudes satisfying $| u |^2 + | v |^2 = 1$, to Bob. One each of a pair of ancillary entangled photons B and C is sent to Alice and Bob. Alice performs a joint measurement on her ancillary photon and the teleportee photon, and obtains one of the Bell states with probability $\frac{1}{4}$. This measurement collapses Bob's ancillary photon C into a well defined state uniquely related to the state of the teleportee $| T >$. Alice then transmits the result of her measurement to Bob over a public channel and he then knows which of the four unitary operations (phase shift, bit flip, combined phase shift/bit flip, identity operation) to perform on his photon C to switch its state to that of the original photon $| T >$.

For example, suppose the ancillary photons are prepared in the Bell state Ψ^-. The three-photon state of A,B and C is then

$$| \Psi >= \frac{1}{\sqrt{2}}[u | 1\ 1\ 0 > + v | 0\ 1\ 0 > - u | 1\ 0\ 1 > - v | 0\ 0\ 1 >]$$

This can be regrouped in terms of Bell states of photons (A and B) and single-photon states of C:

$$| \Psi >= \frac{1}{2}[| \phi^+ > (u | 0 > - v | 1 >) + | \phi^- > (u | 0 > + v | 1 >)$$
$$- | \Psi^+ > (u | 1 > - v | 0 >) - | \Psi^- > (u | 1 > + v | 0 >)]$$

Suppose Alice, in her Bell state measurement, finds $| \Psi^- >$. C is projected into the state

$u | 1 > + v | 0 >$, which is the same as $| T >$. Alice then tells Bob the result of her measurement and Bob knows he has to do nothing (perform the identity operation) on his photon; it is already an identical copy of the teleportee. Bob's photon may have been projected into the state instantaneously, but Bob doesn't know he has to do nothing until he receives Alice's message via a subluminary signal. Special relativity is not violated. If Alice had found the state $| \Psi^+$, Bob's photon would have been projected into the state $u | 1 > - v | 0 >$ and on receiving Alice's message he would have had to have performed a phase change operation to recover the teleportee. In this process of teleportation the original photon is destroyed (by Alice's Bell state measurement), but an identical copy created elsewhere. It is not necessary to know anything about the state of the original photon.

8 References and Further Reading.

1. P.C.W.Davies and J.R.Brown (editors), "The Ghost in the Atom." (Canto, Camb.Univ. Press, 1986.)
2. J.Bell, "Against 'measurement' ", Physics World, August 1990.
3. R.Peierls, "In defence of 'measurement' ", Physics World, January 1991.
4. K.Gottfried, "Does quantum mechanics carry the seeds of its own destruction?", Physics World, October 1991.
5. "Quantum Information", Physics World, Special Issue, March 1998.
6. R.Hughes and J.Nordholt,"Quantum Cryptography takes to the air", Physics World, May 1999.
7. Tony Leggett, "Quantum theory: weird and wonderful", Physics World, December 1999, 73-77.
8. A.Whitaker, "John Bell and the most profound discovery of science", Physics World, December 1998.
9. R.Penrose, "The Emperor's New Mind", (Vintage,1990.)
10. R.Penrose, "Shadows of the Mind", (Vintage, 1995.)
11. A I M Rae, "Quantum Mechanics", (IoP Publishing, Fourth Edition, 2002.)
12. M. Gell-Mann, "The Quark and the Jaguar", (W.H.Freeman and Co., N.Y. 1995.)
13. J.Gribbin, "Schrödinger's Kittens and the Search for Reality" (Phoenix Paperbacks, 1998.)