GRESHAM COLLEGE

13 MARCH 2018

The Quantum Mathematician

PROFESSOR CHRISTOPHER BUDD, OBE

Quantus: Latin, meaning 'How great'

Introduction

Towards the end of the 19th Century, the world's physicists were feeling confident that they understood the world pretty well. For example, the laws of electricity, magnetism and optics were united by the work of Maxwell. Similarly, the laws of thermodynamics were well understood and Newton's laws of mechanics, now 200 years old, seemed to explain all of motion. It was said by some that all that remained for physicists to do was to find the various constants of nature with higher and higher precision. There were, it was to be admitted a few areas of concern, such as the behaviour of the X-ray tube, the nature of radioactivity and the properties of the world at an atomic level, but it was felt that these would soon be resolved. All of this however was to change completely at the start and early part of the 20th Century, when the whole of physics went through a complete revolution. This was due to discovery of the theory of relativity and, at almost the same time of quantum theory. Both theories relied on deep, and elegant, mathematical ideas to take us well beyond our imagination (and indeed the limitations on our thinking given by 'common sense'). In the case of relativity into the large-scale universe close to the speed of light, and in the case of quantum theory to look into the nature of the very small scale of the universe of the atom and smaller. In their separate ways both theories have transformed our understanding of the world and have led to many new technologies. Indeed, without quantum theory to give us insight into the behaviour of the world at the very small scales of atoms and sub-atomic particles, we would not have modern electronics and hence the modern computer and all of the effects this has on modern society. It is quite possible that further advances in the application of quantum theory to technology will cause even greater revolutionary changes. For this reason, quantum technology has been named 'the ninth of the governments eight great technologies'. Yet despite this, quantum mechanics remains at its heart a deeply mysterious and puzzling theory, which often seems to completely contradict common sense. In this lecture I will attempt to explain some of the main (mathematical) ideas behind quantum theory and how it applies to the small-scale world, and of the technology that has arisen from it. I will then talk about some of the new and very exciting developments of quantum information theory and quantum computing. The latter promises to be every bit as transformative as the discovery of quantum theory itself. However, I do not expect in this lecture to be able to explain all of quantum physics and its applications. Indeed, quantum mechanics still seems to defy a simple explanation, as the following quotes will make clear:

> *Quantum theory has two powerful bodies of fact in its favour, and only one thing against it. First, in its favour are all the marvellous agreements the theory has had with every experimental result to date. Second, and to me almost as important, it is a theory of astonishing and profound mathematical beauty. The one thing that can be said against it is that it makes absolutely no sense.*
>
> **Sir Roger Penrose, OM, FRS**

> *I think I can safely say that nobody understands quantum mechanics.*
>
> **Richard Feynman, Nobel Laureate**

Or indeed

Those who are not shocked when they first come across quantum theory cannot possibly have understood it.
Niels Bohr, Nobel Laureate

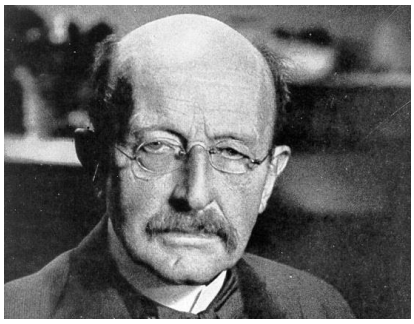
All these quotes lead to a profound issue in the philosophy of mathematics. Is a mathematical formula applied to the real world an approximate description (or solution) of a model the reality it is encompassing, or is reality itself a manifestation of the working out of the formula, and the more elegant the formula the better it represents reality, even if it contradicts common sense? In the quantum universe both perspectives seem to be true, with the latter view often looking the more realistic!

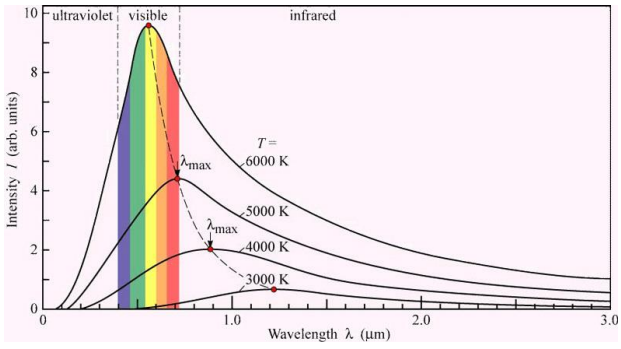
I will include some maths in this presentation, as this is the way that I think about the universe. However, if you prefer a less mathematical treatment I refer you to the excellent popular books [1] and [2], and of course to the best account of all in [3].

A short history of quantum theory: 'old quantum theory'.

Black body radiation

One of the 'small anomalies' faced by classical physics at the end of the 19th century was understanding the nature of the electromagnetic radiation emitted from a black body at different wavelengths. This is an important problem in many fields of physics including studies of climate change. The classical theory of thermodynamics had been developed by the mathematician Lord Kelvin and was being used, to great effect, to develop the internal combustion engine. However, a difficulty with the classical theory of electromagnetic radiation was that it seemed to predict that more and more radiation would be emitted at the short ultra-violet wavelengths, which was far from the case of observations. This phenomenon was carefully investigated by the German physicist Max Plank, often regarded as one of the two key founders of quantum mechanics, the other being Niels Bohr. In 1900 he proposed a resolution to this problem by stating that the energy of the radiation E was proportional to its frequency f so that high frequency radiation such as ultra violet light or X-rays has more energy than visible light or infra red (heat). This placed a restriction on how much energy could be radiated at the high frequencies and resolved the black body problem. Below we see a photograph of Plank and a graph of the intensity of the black body radiation at different frequencies.





Plank's discovery/postulate was that $$E = hf$$

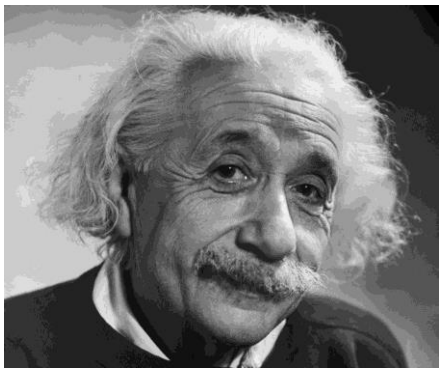
Where h is a small constant, now called *Plank's constant*. Using this, Plank went further to predict that radiation came in discrete amounts which he called *quanta* and that Plank's constant gives a limitation to the size of an individual quantum of energy. Using this idea Plank predicted that the spectral radiance B of the black body radiation (the amount of energy it gives off as radiation of different frequencies) at a temperature T and a frequency f was given by

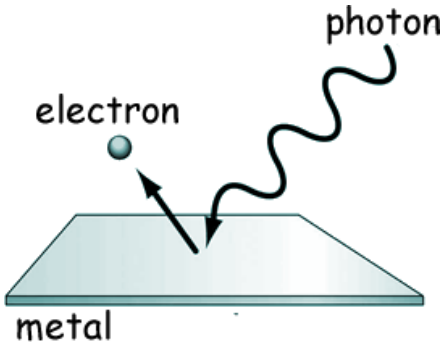
$$B(f,T) = \frac{2hf^3}{c^2}\frac{1}{e^{\frac{hf}{\kappa_B T}} - 1}$$

which agrees perfectly with experiment.

The photoelectric effect

The next major advance in quantum theory came in 1905 and was due to Albert Einstein. This year saw the publication of three quite remarkable papers by Einstein. In particular, he introduced the ideas of special relativity, the kinetic theory of gases, Brownian motion and the photoelectric effect. It was the last paper which won him the Nobel Prize, but to be honest, any of them would have been enough for the award of the prize.





Einstein was studying the photoelectric effect in which a metal is irradiated by light and gives off electrons as a result, by knocking free electrons from its surface. The classical wave theory of light (as described by Maxwell's equations for example) implied that the energy of the light was proportional to its amplitude and thus the energy of the electrons emitted should also be proportional to the amplitude. However, in the photoelectric effect it was found that whilst the *number* of electrons emitted was proportional to the *amplitude* of the light, their individual *energy* was proportional to the *frequency* of the light.

Einstein explained the photoelectric effect by proposing that light came discrete quanta which he called *photons*. Photons behave a little like particles and each has an energy which depends upon its frequency only. The greater the amplitude of the light the more photons it contained (usually a very large number indeed). Each photon, of sufficiently high frequency and thus energy, knocked out an electron with energy proportional to that of the photon. The more photons, the more electrons. Again, there was perfect agreement with experiment.

Light was known (through many experiments, and also Maxwells' theory) to be a wave. Now it seemed to be made up of particles. What was going on?

Models of the Atom

Shortly after this, in 1909, Ernest Rutherford, experimenting in Manchester, shone a beam of Alpha particles at a thin gold foil. He found, much to his surprise, that some of the particles bounced back. The current theory of the atom (proposed for example by J J Thompson at Cambridge) was that the atom was a blob of electric charge with electrons embedded in it. According to that theory the Alpha particles should all have gone straight through. Instead, Rutherford was forced to postulate that the mass of the atom was concentrated in a small, central nucleus, and that the electrons orbited this in a similar manner to planets orbiting the Sun. Whilst very elegant, this theory has a significant problem. A particle in a circular orbit is constantly accelerating towards the centre (see my lecture on *Maths goes into space* for an explanation of this behaviour). According to Maxwell's

theory, an accelerating electrically charged particle such as an electron, gives of radiation, and thus loses energy. As a consequence, the electron in Rutherford's atom would simply spiral into the nucleus.

A first resolution to this apparent paradox was provided shortly afterwards by the great Danish physicist Niels Bohr. Bohr extended the idea of Plank to predict that the orbital electrons could only give up energy in discrete amounts, and that the electron orbits themselves had prescribed energies. The electrons could jump orbits, other to ones of higher energy by absorbing a photon, or to one of a lower energy by releasing a photon. By doing this he could predict the types of radiation emitted by the atom, and his prediction proved remarkably accurate.

Unfortunately, this view of the atom, whilst easy to understand proved to be an overly simplistic description of the behaviour of the small scales.

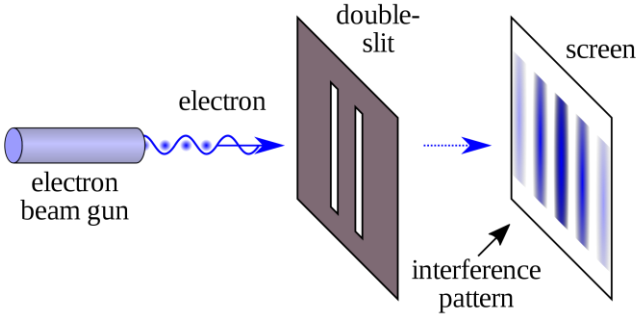
The 'new quantum theory'

It was Bohr himself (pictured below) that led the remarkable advances in quantum theory that followed the end of the Great War. He did this through the foundation of the Institute for Theoretical Physics in 1921 in Copenhagen, which went on to develop the *Copenhagen Interpretation* of quantum mechanics.

Bohr's approach, together with those he recruited for the institute was truly revolutionary and replaced a deterministic interpretation of reality (which is how Newton and Einstein described the world) with one much more based on a probabilistic perspective in which only the probability of a particle having a position and momentum was known. This view was then developed by a group of extraordinarily creative scientists who we now look at. It is notable that scientists are often portrayed as non-creative individuals. This is of course hugely untrue in general and especially untrue in quantum theory. It was only by being prepared to imagine worlds far removed from common sense, that quantum mechanics made the progress that it did.

De Broglie and the wave particle duality

In 1924 the French scientist de Broglie made an extraordinary assertion which flew directly in the face of a common-sense interpretation of physics. Noting that light seemed to have properties of both a particle and a wave, he proposed that all particles could have wave like properties. This included electrons. The reason that this wasn't apparent for large particles, such as those we encounter in real life, is that the more massive the particle is, the shorter its wavelength. A clear demonstration of this was given in 1927 by the famous two-slit experiment. In this experiment an electron is fired towards two slits in a plate. As it passes through the slits it behaves like a wave. Behind the slits a diffraction pattern forms because of this wavelike nature even though the electron behaves like a particle when it hits the screen. The overlapping waves from the two slits cancel each other out in some locations, and reinforce each other in other locations, causing a complex wave like pattern to emerge.



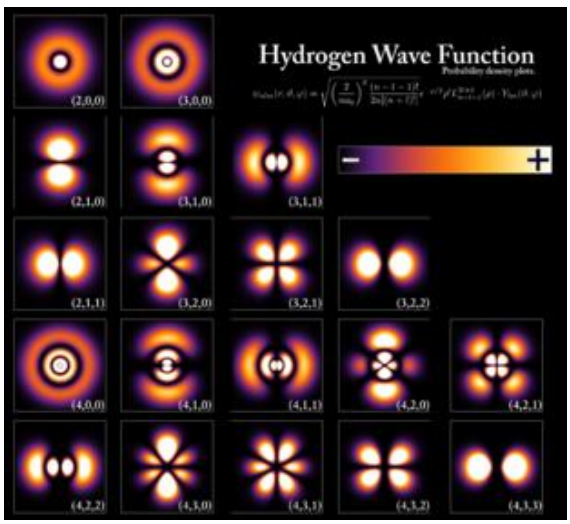
Schrodinger and the wave equation

This view of a wave/particle duality to matter was extended and given a mathematical description by Erwin Schrodinger pictured below, who felt that the particles in the quantum universe (such as the electron) could be described in terms of a wave function $\psi(x,t)$ which represented the *probability* that a particle was in the position x at the time t. In 1926 he derived a wave equation to describe such a wave function.

In modern notation Schrodinger's equation takes the form:

$$i\hbar\frac{\partial}{\partial t}\psi(x,t) = \left[\frac{-\hbar^2}{2\mu}\nabla^2 + V(x,t)\right]\psi(x,t)$$

This is one of the most important mathematical equations of all time! Here i is the square root of -1, and this equation is one of the best applications of this wonderful number. The function V(x,t) is the potential energy of the system. Essentially if you know V(x,t) then you can solve Schrodinger's equation to give the wave function psi(x,t). This then tells you the probability of observing the particle and essentially all you need to know about the system. Simple, or is it? For a simple atom such as Hydrogen this is known so that V = -1/|x| where x is the location of the particle with respect to the centre of the atom. In this case Schrodinger's equation can be solved exactly, to give the wave functions of the orbiting electrons. In Schrodinger's time this was about as much as was possible, and it was enough to show that the predicted wave functions of the electrons orbiting the nucleus agreed with what was observed, including the spectral energies. Indeed, the energies of the wave functions take, as we might expect from the origins of quantum theory, *discrete values*. These values are the eigenvalues of the linear Schrodinger operator. However, in the 1920s it was found hard to make any more progress. Schrodinger's equation was simply too hard to be solved for more complicated systems, such as a molecule. In the 21st Century we can do much better. Fast computers can solve the equation form complex systems, and this allows the chemical properties of a system to be deduced well in advance of it being synthesised. Below we illustrate some of the wave functions for the Hydrogen atom.



Interestingly, Schrodinger himself had a lifestyle which was far removed from the traditional view of a scientist who stays in their laboratory and is dedicated only to science. In contrast Schrodinger had several wives *simultaneously* and famously came up with his famous equation whilst on a passionate holiday with his mistress. Whilst he started his professional career in Austria, he eventually moved to the, then still new, Republic of Ireland in 1940 on the invitation of Eamon de Valera. He became the Director of the School for Theoretical Physics in Dublin and remained there for 17 years before returning to Austria five years before his death.

One of the key features of Schrodinger's equation is that it is *linear*. This means that if psi1(x,t) and psi2(x,t) are two wave functions which satisfy it, then so does the *superposition* psi(x,t) = psi1(x,t) + psi2(x,t) . Loosely speaking this implies that the particle represented by the wave function can simultaneously exist in two states at the same time. This is called the *superposition principle*. The two-slit experiment demonstrates thus. Intuitively, one would not expect the diffraction pattern from firing a single particle at the slits, because the particle should pass through one slit or the other, not a complex overlap of both. Although this is counterintuitive, the prediction is correct and has been verified many times in experiment. The superposition property allows the particle to be in a quantum superposition of two or more quantum states at the same time. This is not completely counter intuitive as a *quantum state* means the *probability* that a system will be at a position *x*, not that the system will actually be at position *x*. It does not imply that the particle itself may be in two classical states at once.

Heisenberg and the uncertainty principle

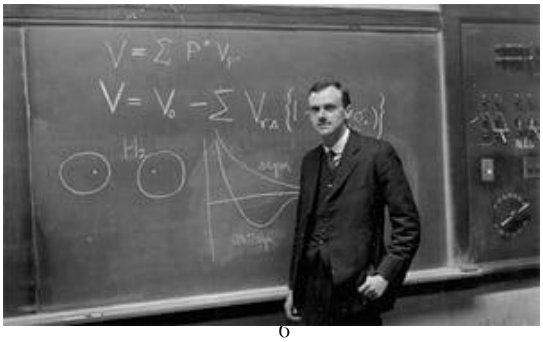
Heisenberg, working in Copenhagen, had an alternative view on quantum mechanics. He developed a mathematical theory for it based upon matrix mechanics in which the observable states for the system were represented by the eigenfunctions of the matrices. In fact, the states only became like particles when they were observed and before then they were just an abstract mathematical quantity about which nothing could be known (if we were not looking). Although this seemed to differ from Schrodinger's perspective they turned out to be two different mathematical ways of looking at the same thing. In 1927 Heisenberg also proposed the uncertainty principle that if Delta x is the error in measuring the position of a particle and delta p is the error in measuring its momentum then

$$\Delta x \, \Delta p \geq \frac{\hbar}{2}$$

This formula places a basic limit on how accurately we can measure things in the universe. Hence the joke. Ask a quantum physicist if a glass is half empty or half full and they will say that *they cannot tell*. The reason why is that if you have precise information of the amount of water in a glass then you can't possibly work out whether it is increasing (half full) or decreasing (half empty).

Dirac and the equation for the electron

Paul Dirac (pictured below) was a British physicist who was born in Bristol and was recently voted the fifth greatest physicist of all time, almost on a par with Newton, Einstein and Maxwell.



As well as being such a brilliant physicist, Dirac was famous for avoiding all social interaction. In 1928 Dirac set about the challenge of finding a unification of quantum theory and special relativity. In particular he wanted to explain the behaviour of a fast-moving electron, which was subject to relativistic effects and obeyed both Maxwell's equations, which are consistent with Einstein's special theory of relativity, and of course the laws of quantum mechanics. Dirac succeeded where the others had failed by introducing a new equation for the electron, an equation which now bears his name. The **Dirac equation** is a relativistic wave equation which describes all electrons and quarks and is consistent with both quantum mechanics and the theory of special relativity. Dirac was (most properly!) motivated to construct his equation based on the principles of mathematical evidence. It resembles Schrodinger's equation, but it describes a massive particle subject to relativistic effect and takes the following form

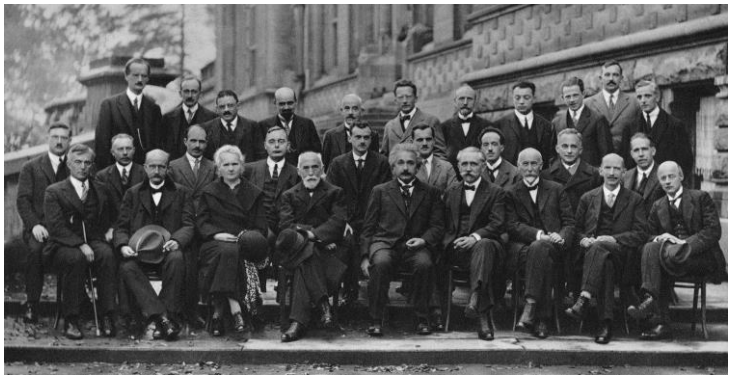
$$\left(\beta mc^2 + c\left(\sum_{n=1}^{3}\alpha_n p_n\right)\right)\psi(z,t) = i\hbar\frac{\partial\psi(z,t)}{\partial t}$$

In this expression p refers to the different components of the momentum of the particle of mass m, and c is the speed of light. The real novelty in this equation is that the wave function psi has four components interpreted as a superposition of a spin-up electron, a spin-down electron, a spin-up positron, and a spin-down positron. The terms alpha and beta are actually 4*4 Hermitian matrices describing the spin of the particle. These obey a set of rules called a Clifford Algebra which were developed as an abstract system in the 19th Century. It is remarkable that such a pure, and to quote Dirac, elegant, system should have such an important use to describe the physical nature of reality.

Dirac's equation accurately predicted the full spectrum of the Hydrogen atom and this was used as a validation for it. However, it went far deeper than that. Indeed, it also implied the existence of a new form of matter, called *antimatter,* so that as well as an electron with positive charge, there was an anti-electron, otherwise identical and with a positive charge. This prediction was experimentally confirmed several years later, and the particle is now called the positron. It also provided a justification for Pauli's theory of spin. Dirac made many other huge contributions to physics. These included showing that Heisenberg's matrix approach to quantum mechanics, and the wave approach of Schrodinger were equivalent. He also wrote The Principles of Quantum Mechanics [4], which became the standard textbook for the field for many years. Furthermore, anyone working in mathematics, physics or engineering will have come across the Dirac Delta function, which was invented by, and named after, Dirac, and is an essential component of signal processing, mechanics, linear systems theory and the study of ordinary and partial differential equations. It is a great pity (and a negative comment on the value that the UK places on science) that Dirac is not more recognised in our country (although he does have a great memorial in Bristol outside the science centre).

The Solvay Conference

The Solvay conference (in Belgium) of 1927 has been described as 'the most intelligent meeting ever' and marked a gathering of many of the greatest minds in physics in the first half of the 20th Century. A picture of the conference is given below. Prizes for spotting Plank, Einstein, Dirac, Bohr, Schrodinger, Heisenberg, de Broglie, and even Marie Curie in the photo, alongside many other distinguished figures.



It was at this conference that the mathematical description of quantum mechanics came to maturity, and the conference marked the end of the second phase of the development of quantum theory. The conference was notable for a heated set of discussions between Einstein and Bohr centred around a number of thought experiments from Einstein that he intended as raising serious objections to quantum physics. Not only was Bohr able to answer these, but some, such as the developing idea of quantum entanglement, have led to profound advances in both the theory and the application of quantum mechanics. I wish that my conferences could be anything like as productive as the Solvay meeting.

Schrodinger's cat

In 1935 Schrodinger described a thought experiment, which has had a profound influence ever since on our thinking about quantum theory and has many applications to quantum technology. In this experiment a cat is in a closed box together with a radioactive material which, when it decays, causes the release of a poison which kills the cat. As the radioactive decay is completely unpredictable, we don't know if at any one time the cat is dead or alive. From a quantum mechanical perspective, it exists as a superposition of alive and dead states. Only when you open the box does it become actually alive or dead. This seems a complete paradox, and indeed it is. At the scale of a cat things are either dead or alive. However, at an atomic scale this is perfectly possible. Things can, and do, exist as a superposition of states, and this fact is hugely important in, for example, quantum computing.

Observable quantum effects such as this superposition do not usually occur in everyday macroscopic objects because their individual atoms are not in a coherent state. Therefore, any quantum effects are basically averaged out by the time we make a measurement of the macroscopic object. But there are examples of quantum effects on a macroscopic scale, including laser beams, superconductors, and liquid helium in a superfluid state.

I leave this section with a remark by Penny in the TV series 'The Big Bang Theory'. A quote which I found very profound and thought provoking

> *We had a cat in a box once. Didn't need to open that box to know that it was dead!*

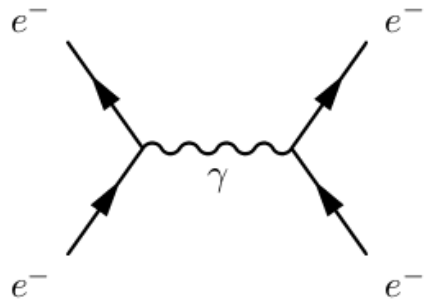
As they say, discuss!

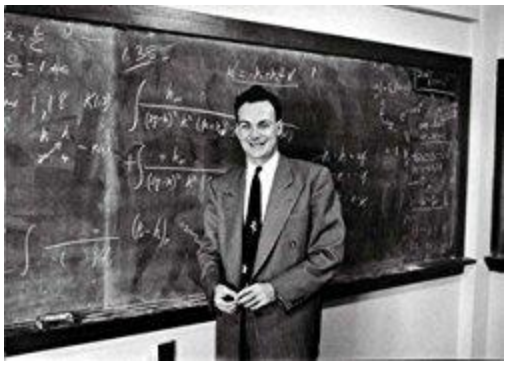
Quantum theory up to date

The Solvay conference marked the end of the beginning of quantum theory and put it on firm mathematical foundation. As a subject it has advanced in leaps and bounds ever since in many different directions. I will describe two of these.

Quantum Field Theory

Quantum Electrodynamics (QED) has been described as the most accurate theory ever devised, and it is an explanation of the way that the electromagnetic force comes about as the result of quantum mechanical driven interactions of matter with light, namely through the exchange of photons. The idea behind this and similar Quantum Field Theories goes back to Dirac. However, their development was hindered by a mathematical problem. In particular the calculations made gave infinite answers. These were overcome by the mathematical process of *renormalisation*. Chief developer of this approach was Richard Feynman who also developed Feynman diagrams (see both below) to summarise the resulting processes. Feynman made many other contributions to quantum theory, including explaining the nature of liquid Helium and (as we shall see) predicting the development of the quantum computer. The predictions of QED (for example on the spin of the electron) have now been verified to over six decimal places of accuracy!





QCD or Quantum Chromo Dynamics, is a similar theory which gives a very complete understanding of the strong nuclear force which binds the atomic nucleus together.

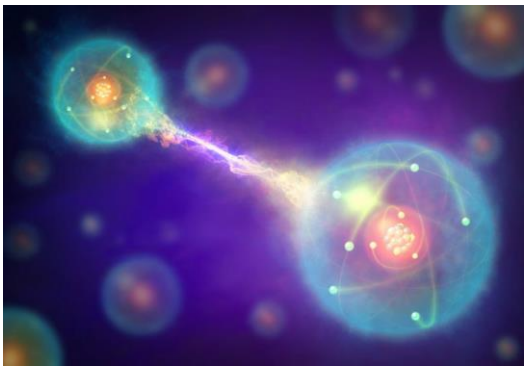
Quantum entanglement

Despite putting quantum mechanics on the map in 1905, Einstein never really came to terms with its later developments. To quote him in a famous remark he said:

Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot but does not really bring us any closer to the secret of the old one. I, at any rate, am convinced that He does not throw dice.

One very strange feature of the quantum universe, with significant implications both in science and technology, is that of quantum entanglement. This was originally proposed by Einstein–Podolsky–Rosen paradox or *EPR* paradox of 1935 as a thought experiment in quantum mechanics with which Albert Einstein and his colleagues Boris Podolsky and Nathan Rosen (*EPR*) claimed to demonstrate that the wave function does not provide a complete description of physical reality. The consequence of this was named by him as 'spooky action'. However, the EPR paradox has since proved to be an important verification of quantum theory and, as we shall see, is finding its way into modern technology. Quantum entanglement is the process by which two separate particles somehow become 'connected' and share a wave function, so that what you do to one instantly affects what you do to the other. Thus, information appears to be travelling faster than the speed of light, which violates both Newtonian mechanics and the theory of relativity. However, in a way this should come as no surprise as we can have experiences just like this. Imagine that you have two boxes which are identical from the outside. At some point a friend of yours places a red ball in one box and a blue ball in the other without telling you which. Your friend then hands you one of the boxes. You take this on a long journey (say to the Moon). When you arrive, you open the box and you see a blue ball. You then instantaneously know that the other box back on Earth contains a red ball. A not unrelated phenomenon connects two quantum particles which are created at the same time and is called a non-local connection, or a quantum entanglement, in which an action on one particle instantaneously affects the other. This is now recognised to be a common quantum phenomenon. The mathematical reason is that, as we have seen, particles really behave like extended waves. If two particles come into contact then their waves become correlated and to a certain extent they behave as though they were one particle, even if they are distantly separated as in the example with the two boxes. If one of these particles is

put into a quantum superposition then the other must be too, and measuring one instantly affects the other. This phenomenon will turn out to be important in cryptography.



Early quantum technology

Quantum theory is a profoundly important way of understanding the nature of the universe around us. In particular it explains the way that molecules and crystals form, and also the way that some elements are unstable through radioactive decay or can give off energy through nuclear fusion. In addition to this, quantum theory has profound technological applications. These are often called the products of the first quantum revolution, to differentiate them from more recent advances. Perhaps the most important of these are semiconductor devices. We are so familiar with these in the form of transistors and micro-chips that we take them for granted and do not realise that they are not a product of classical physics.

Semi conductors

Until the late 1940s all electronic devices used thermionic valves as illustrated below.

These devices performed electronic process such as amplification and oscillation by controlling the flow of electrons in the vacuum between grids in the device. All of this was based on Maxwell's equations which are a classical physical theory. Valves worked very well up to a point, but they had a number of disadvantages. They were large, consumed a lot of power, and had a relatively high failure rate. All of this was exacerbated in devices, such as the early electronic computers, for example the Pilot ACE (illustrated in the last lecture) which used 800 valves. In order to advance electronics, it was essential to find other means of controlling electron flow. The answer to this question came from a study of the way that electricity was conducted in semi-conductor materials such as Silicon and Germanium, and this required the use of Quantum theory. A key part of this was the discovery that unlike metals, and indeed the vacuum inside the valve, there appeared to be two types of charge carrier inside a semiconductor with negative and positive charges. The negative charges were simply electrons, but the positive charges, which behaved very like electrons, were called *holes*. A hole was in fact the absence of an electron in one of the valence bands in the atom, which of course were one of the predictions of quantum theory. Also crucial to the operation of semiconductor devices is the phenomenon of *quantum tunnelling* in which an electron (or a hole) can overcome an energy barrier. This is a factor of having a wave function which gives it

a small, but positive, probability of overcoming this barrier. (Tunnelling is also very important in the processes involved in nuclear fusion, and also in MRI scanners.) Combining the equations for the holes and the electrons leads to the celebrated semi-conductor equations for the negative electrons n and the positive holes p, which allow us to predict the behaviour of semi-conductor devices.

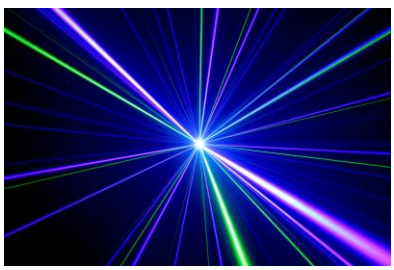
$$\begin{aligned}
\nabla.(\epsilon\nabla V) &= q(n-p-C) \\
\nabla.J_n &= q\left(n_t+R\right) \\
\nabla.J_p &= q\left(-p_t-R\right) \\
J_n &= q\left(D_n\nabla n-\mu_n\ n\ \nabla V\right) \\
J_p &= q\left(-D_p\nabla p-\mu_p\ p\ \nabla V\right)
\end{aligned}$$

The first of these to be invented was the transistor in 1947 by William Shockley at Bell laboratories. (Bell Labs were also responsible for information theory and error correcting codes which I described in two previous lectures.) The transistor, shown below, performed all of the functions of the valve, in particular it could amplify a weak signal, it could act as a switch and it could sustain an electrical oscillation. It was also much smaller, used much less power, and was more reliable than the valve. This led to it being rapidly adopted as the main component in all electronic devices.

A natural development of the transistor was the Silicon chip, which is nothing more than a large number of transistors on the same wafer of Silicon. The invention of the chip led to the modern computer, mobile phone and much of modern technology.

Lasers

Another modern invention, which follows from quantum theory, is the laser. Lasers producing coherent light by making electrons jump orbits. A laser is created when the electrons in atoms in special glasses, crystals, or gases absorb energy from an electrical current and become *excited*. The excited electrons move from a lower-energy orbit to a higher-energy orbit s. When they return to their normal or *ground state*, the electrons emit photons. These photons are all at the same wavelength and are *coherent*, meaning that the corresponding light waves are all in phase. In contrast, ordinary visible light comprises multiple wavelengths, all out of phase, and hence is not coherent. Laser light is different from normal light in other ways as well. First, its light contains only one wavelength. In contrast the particular wavelength of laser light is determined by the amount of energy released when the excited electron drops to a lower orbit. Second, laser light is directional. Whereas a laser generates a very tight beam, a normal domestic produces light that is diffuse. Because laser light is coherent, it stays focused for vast distances. As a demonstration of this for a short distance, witness my laser pointer. For longer distances, a beam of laser light, reflected off a reflector placed by the Apollo astronauts, is constantly used to monitor the distance between the Earth and the Moon. Once described as a 'solution looking for a problem' lasers are used in CD players, DVDs, rangefinders, remote sensing, surgery, microscopy, holograms, welding, barcode readers, printers, special effects and, of course, pointers.

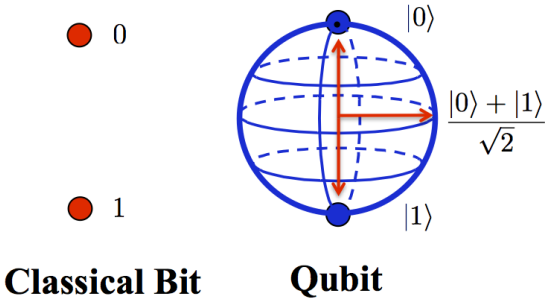


The second quantum revolution: Quantum information, quantum computers and quantum cryptography

We are now into the second generation (called Quantum 2.0) of quantum technology, much of which is based on the thought experiments that Einstein proposed during the Solvay conference.

Quantum information theory

In the earlier lecture on 'Maths is coded in your genes' we saw how the work of the mathematician Shannon in the 1940s led to a revolution in the transmission of information, in which all data was transmitted as bits. This was faster and more reliable than the analogue systems used up to that date, and now all data is transmitted in this way. However, we are now likely to see a second revolution in the way that information is transmitted due to the use of ideas from the theory of *quantum information*. Quantum information theory asks the question of "How is information stored in a state of a quantum system?"



In the classical theory of information developed by Shannon, the basic unit of information is the bit (binary digit) which takes exactly the values of either 1 or 0. In quantum information theory the basic unit or information is the *qubit* which, through the principle of superposition can be in two states at once. So, in principle, N qubits can simultaneously store 2^N amounts of (quantum) information. This is far larger than the one piece of information stored on a classical computer. Qubits can be transported (via quantum teleportation) and an arbitrary qubit *can neither be copied, nor destroyed*. However, Qubits can be changed, by applying linear transformations to them, to alter their state. Quantum information can be moved about, in a quantum channel. This is analogous to the concept of a classical communications channel (which I spoke about in the lecture on How Maths is Coded in your Genes). Quantum messages have a finite size, measured in qubits. As in classical theory quantum channels have a finite channel capacity measured in qubits per second and quantum information can be transmitted using the quantum version of error correcting codes and manipulated in quantum logic gates. Scientists are still working on how to make these gates work but research on them is advancing rapidly. For example, very recently researchers in Oxford [5] are using a trapped-ion technique, to place two charged atoms in a state of quantum entanglement, as described above. The charged atoms then contain qubits of quantum which can be controlled. According to them

We have now produced the highest fidelity and the fastest gate, reaching a point where our gates are in principle good enough for quantum computing. The next step is to think about it in practical terms and work towards scaling up our system to create a viable quantum computer.

So, watch this space.

Black holes and multiverses

A prediction of general relativity is the existence of black holes or singularities in space-time. Using quantum mechanical arguments Hawking showed that these could radiate (through Hawking radiation). However, it was then realised that black holes appeared to violate a precept of quantum mechanics, in that they could destroy the information contained in the matter that fell into them by evaporating. This was considered to be a significant paradox in physics. However, a possible resolution of this paradox is provided by the *many worlds* interpretation

of quantum theory in which rather than the wave function (of the universe) collapsing to a single state to represent one outcome, it branches into a multiverse, with one branch for each outcome. This is in contrast to Heisenberg's view in which we don't know anything about the wave function until it is observed and is very extravagant as it postulates a huge number of possible universes. In this interpretation the idea of information applies to the whole wave function instead of to its individual branches. Perhaps this gives some evidence for a many worlds interpretation of the quantum universe being the right one?

Quantum Computing

The field of quantum computing was initiated by the work of Paul Benioff and Yuri Manin in 1980, Richard Feynman in 1982, and David Deutsch in 1985. It is now predicted that quantum computers could come to dwarf the processing power of today's conventional computers, by harnessing the effects of quantum theory. See [6] for more details. Quantum computers could eventually allow work to be done at a speed almost inconceivable today. As an example of how significant this is, let's consider the fact that most of our money is held in banks. The security of the world's banking system relies on the rather abstract concept of the difficulty of factorising large integers. Whilst it is easy factorise a number such as 143 it is harder to factorise a number such as 262417 and very hard to factorise 97605751. Try doing these yourself. In general, if a number has N digits then the best factorisation algorithms on a conventional computer take a time which is proportional to the exponential of N. If N is large, then this is very large indeed. The reason that this matter is that modern cryptography systems rely on the celebrated RSA algorithm [7] to deliver the key used to encrypt or decrypt a message.

Such systems are used to encode information about your credit card and bank account. The RSA algorithm relies for its security on properties of prime numbers, and in particular to the current fact that it is possible to let everyone know the product N of two of these numbers p and q, whilst keeping the values of p and q secure. If a computer could be made which could factorise N in a much shorter time, say in a time proportional to a power of N (called *polynomial time*) then the security of the RSA algorithm would be fatally compromised. A possible such threat to the security of the banking system is posed by quantum computing, which is in turn reliant on quantum information theory. The property of qubits, that they are the superposition of quantum states allows quantum computers to be exponentially faster than conventional computers because they can perform multiple tasks in parallel (i.e. at the same time).

A quantum computer works by operating on its qubits using quantum gates. The calculation starts with an initial set of qubits and ends with a measurement, collapsing the system of qubits into one of the states where each qubit is zero or one. The outcome can therefore be at most classical bits of information. Quantum algorithms are often probabilistic, in that they provide the correct solution only with a certain known probability. Quantum algorithms have a different computational complexity than classical algorithms. The most famous example of this is *Shor's factoring algorithm* developed in 1994 [8] (which in turn uses the quantum Fourier transform or QFT) for finding the factors of the number N. It is fast because it relies heavily on the ability of a quantum computer to be in many states simultaneously, and to compute the period of a certain function *f,* which is a necessary part

of the algorithm, it evaluates the function at all points simultaneously. As a result of this speed up. Shor's algorithm can factorise a number with N digits in polynomial time, which is far faster than a classical algorithm.

Shor's factoring algorithm

Quantum algorithm [Shor'94]

Given: Numbers N and a.

Task: Find the order r of a modulo N.

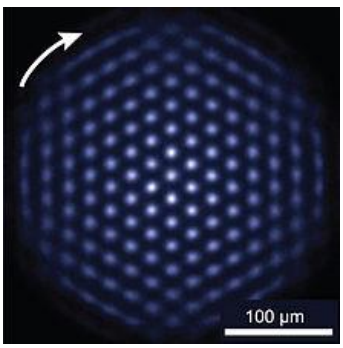
Repeat the following steps few times: (w/o normalizations, $M = 2^m >> N$)

1.	Initialize two quantum registers:	$\|0\rangle \, \|0\rangle$
2.	Equal distribution on first register:	$\sum_{x=0}^{M-1} \|x\rangle \, \|0\rangle$
3.	Compute f in superposition:	$\sum_{x=0}^{M-1} \|x\rangle \, \|a^x \bmod N\rangle$
4.	Measure second register:	$\sum_{k=0}^{M/r-1} \|x_0 + k \cdot r\rangle$
5.	Compute DFT_M on first register:	$\approx \sum_{\ell=0}^{r-1} \omega_M^{\ell \frac{N}{r} x_0} \, \|\ell \frac{N}{r}\rangle$
6.	Measure first register:	Sample a rational number $\frac{p}{q}$ which is very close to $\frac{\ell_0}{r}$.
7.	Classically reconstruct r from $\frac{p}{q}$.	

January 26, 2016 M. Roetteler 60

Another powerful quantum computing algorithm is *Grover's algorithm*. If a full-scale quantum computer is developed, then cryptographic systems such as RSA (which relies on solving the discrete logarithm problem) and especially Triple DES (which is a commonly used symmetric cypher which relies on a complex key and which can be broken using Grover's algorithm) will become much less secure. In 2001, a group at IBM, factored 15 into 3×5, using Shor's algorithm on a quantum computer with 7 qubits. In 2012, the factorisation of 21 was achieved, and in November 2014, adiabatic quantum computation had also factored 56153. So, we are on the way. However other cryptography algorithms, which are based on problems other than the integer factorisation and discrete logarithm, do not (yet) appear to be broken by quantum algorithms.

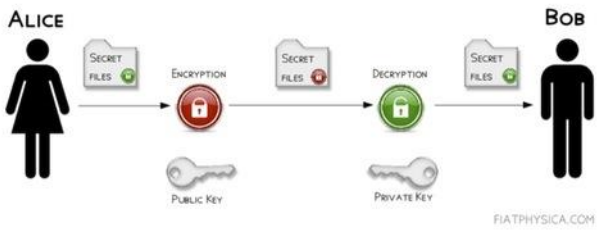
Besides factorisation and computing discrete logarithms, quantum algorithms offering a very significant speedup over the best known classical algorithms, have been found for several important problems. These include the simulation of quantum physical processes from chemistry and solid-state physics, some NP-hard problems such as the travelling salesperson problem, and possibly even to artificial intelligence. Indeed, since chemistry and nanotechnology rely on understanding quantum systems, and such systems are very to simulate in an efficient manner using a classical computer (for example solving the Schrodinger equation is still very difficult for complex systems, and in addition Feynmann showed that it can take exponentially large time to simulate a quantum system due to the effects of superposition). It is thought that the simulation of chemical processes involving quantum mechanics will be one of the most important applications of quantum computing. Below we see the simulation of a quantum lattice.



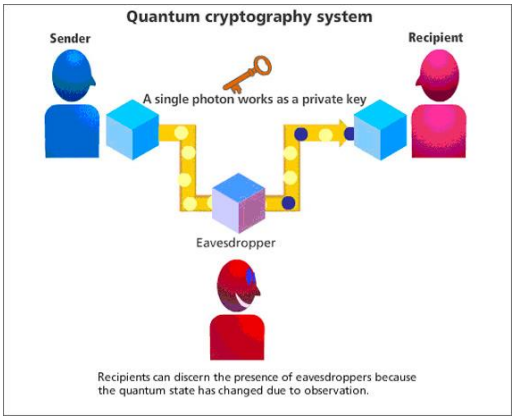
As of today (in 2018), the development of actual quantum computers is still in its infancy (for example we are a long way from factorising the really large numbers used in cryptography), but as we have seen experiments have been carried out in which quantum computational operations were executed on a small number of quantum bits. The problem that all current quantum computers face is the decoherence of the superpositions of the qubits before the algorithm is complete. Practical and theoretical research continues fast, and many national governments and military agencies are funding quantum computing research in additional effort to develop quantum computers for civilian, business, and national security purposes. A small 20-qubit quantum computer exists and is available for experiments via the *IBM-Q quantum experience* project [9]. Exciting times ahead!

Quantum Cryptography

Whilst general quantum computing has yet to be achieved in the large scale, quantum cryptography has to a certain extent already arrived. To understand how this is possible it is necessary to understand how certain types of cryptographic devices operate. A frequently used approach to encrypting a secret message is to transmit a key from the sender (Alice) to the recipient (Bob), so that when Alice sends a message, Bob can use the key to decrypt it. A good example of this is the widely used TripleDes encryption algorithm, or the One Time Pad, beloved of spies. A big problem with doing this however is that of transmitting the key safely and without detection. Key distribution is often done by using the (very hard to crack) RSA algorithm, and it is how the Internet transmits information about your credit card details securely. However, this does not guarantee that someone else (Eve) may be able to intercept the message and somehow find the key (perhaps by using a quantum computer).



In contrast, Quantum Key Distribution (QKD) allows unconditionally secure transmission of classical information. This is unlike classical encryption, which can always be broken in principle, if not in practice. In this procedure, the key is sent through pairs of quantum entangled particles. If Eve tries to learn information about the key by observing one of the particles, then the other will respond instantly and Alice and Bob will immediately notice. Quantum key distribution is secure against quantum computers as its strength does not depend on mathematical complexity, but on physical principles. We may have to rely on it for our security in the future.



Where next

Quantum theory has proved to be a hugely successful way of understanding the world, with enormous applications to modern technology. However, one big mystery still remains (apart, of course, from the obvious mystery that quantum theory doesn't make much sense) and that is how quantum theory relates to the deterministic (classical) General Theory of Relativity, which has proved equally successful in explaining the large-scale universe. Strenuous efforts are being made in this direction and include string theory and loop quantum gravity. However as of today nothing conclusive has been established. But I'm sure, that unlike the scientists at the end of the 19th Century, no one today thinks that there is nothing more to learn in physics.

References

[1] Jim Al-Khalili, *Quantum Mechanics*, (2017), Ladybird Series 117.
[2] Brian Cox and Jeff Forshaw, *The Quantum Universe: Everything that Can Happen Does Happen*, (2012), Penguin.
[3] Richard P. Feynman, Robert B. Leighton, and Matthew Sands, The Feynmann Lectures on Physics, (1964), Addison-Wesley.
[4] Paul A Dirac, *The Principles of Quantum Mechanics*, (1930), Oxford University Press.
[5] http://www.independent.co.uk/life-style/gadgets-and-tech/news/quantum-computing-logic-gates-oxford-university-breakthrough-latest-discovery
[6] John Gribbin, *Computing with Quantum Cats,* (2014), Bantam Press.
[7] Simon Singh, *The Code Book*, (1999), Doubleday.
[8] https://en.wikipedia.org/wiki/Shor%27s_algorithm
[9] IBM-Q project https://www.research.ibm.com/ibm-q/