CHALMERS
UNIVERSITY OF TECHNOLOGY

Quantum technology – popular science description

1 Quantum physics, from theory to ongoing revolution

In the early 1900s observations were made that were not consistent with traditional, classical physics. For example, researchers concluded that hot, black bodies emitted electromagnetic radiation at wavelengths that were not expected, and that atoms could only emit and absorb light of specific frequencies.

In 1900 the physicist Max Planck suggested that light was emitted in small, discrete "packages" – that it was quantised – in order to explain these discrepancies. This marked the start of quantum physics, which describes the world at the atomic level. The brightest physicists of the time, including Niels Bohr and Albert Einstein, led further development. They soon realised that they were on the trail of a paradigm shift, rather than just an adjustment to classical physics. In the 1930s, quantum theory was essentially complete, even though many of its consequences were only understood much later.

Quantum physics has had an enormous impact on society. By exploiting the characteristics of quantum physics in light and materials researchers invented both the laser and the transistor. Such inventions form the basis of information technology as a whole – computers, the internet and much more besides – which to a large extent shape today's society. This was the first quantum revolution.

But even though researchers learnt how to exploit certain quantum characteristics, it was long regarded as impossible to control individual quantum systems such as individual atoms, electrons or light particles (photons). It was only in the 1980s that researchers succeeded in developing methods for measuring and controlling individual atoms and photons, work resulting in the award of the 2012 Nobel Prize in Physics. In parallel with this, other researchers developed electronic components from semi-conductors and superconductors, in which they could manipulate individual electrons.

The control of individual quantum systems has opened the door to a second quantum revolution, offering entirely new possibilities. Today there are goals such as extremely rapid computers, intercept-proof communications and hyper-sensitive measuring methods.

After many years of fundamental research the applications are coming within reach, and researchers as well as policy-makers and business managers are starting to realise that quantum technology has the potential to change our society significantly. Significant investment is now going into quantum technology throughout the world. The EU is launching a decade-long billion-euro investment programme in 2019. There are programmes that are at least as extensive in North America, Asia and Australia. IT companies such as

Google, IBM, Intel and Microsoft are also making significant investments in quantum technology.

2 The central phenomena of quantum technology

Many of the predictions of quantum physics are counter-intuitive. But so far quantum theory has proved to be correct on all points that can be verified. Quantum technology aims to make use of the phenomena of quantum physics to make completely new things possible. The most important phenomena are described below.

2.1 Superposition

In our everyday life things have specific characteristics – for example, they can only be in one place at a given time. But the world of quantum physics is governed by uncertainty and chance. Electrons which spin round atomic nuclei can be both here and there at the same time, and a light particle (photon) can travel along two different paths at the same time. Such composite conditions are called *superpositions.* It is only when a measurement is made that the particle is forced into one of the possible alternatives; chance determines which one. The concept of superposition is general and also applies to other properties such as energy, electric charge and velocity.

Superposition makes it possible to store and process vast quantities of information; read more in section 3.1 Quantum computers.

2.2 Entanglement

Entanglement is a superposition that extends between two or more particles. Interestingly enough the entangled state of the particles remains even when they are separated by a large distance.

Example: Light particles, photons, can be polarised either horizontally or vertically. We place two photons in an entangled condition, which is a superposition of a state in which both photons are horizontally polarised and one in which both are vertically polarised. The polarisation of the photons is therefore indeterminate, but they always have the same polarisation. Then we send one photon off to the moon. When we measure the polarisation of the second photon here on earth, we randomly get a horizontal or vertical result. And the photon on the moon immediately takes on the same polarisation, even though it is so far away and has no communication channel to earth. Einstein was extremely sceptical and called this “spooky action at a distance”, but experiments have shown that it is correct.

Entangled states can be used to send completely intercept-proof messages.

2.3 Squeezed states

One of the cornerstones of quantum physics is Heisenberg’s uncertainty principle. This states that there is a limit to the precision with which the position and velocity of an object can be known at the same time. The same applies to other interlinked variables such as frequency and time.

The uncertainty is normally split equally between the two variables. But by manipulating the quantum system you can ensure that the uncertainty mainly affects one variable. This is called a *squeezed state.* In such a state, it is possible to measure the second variable with extremely high precision, which can be used to design highly sensitive measuring instruments.

2.4 Decoherence

States of superposition (see section 2.1) are very sensitive to disturbances. Disturbances cause the superposition to diminish and finally collapse – and the quantum characteristics then disappear. This process is called *decoherence* and is one of the greatest challenges to be faced in quantum technology. There is an inherent contradiction between isolating the system from its surroundings to avoid decoherence and the need to be able to manipulate the system.

The larger the system, the greater the problems with decoherence. But significant progress has been made in the past 20 years and systems with dozens of qubits (defined in 3.1 Quantum computers) can now be controlled well.

3 The four areas of quantum technology

Quantum technology is based on the ability to precisely control individual quantum systems in order to make use of the phenomena described above. There are applications in secure communications, highly sensitive measurement methods and in creating computing power that far exceeds today's supercomputers.

Quantum technology is often divided into four areas: quantum computing, quantum simulation, quantum communication and quantum sensing. The last two are very close to commercialisation and products have already started to appear.

3.1 Quantum computing

In today's computers the smallest data carrier is the bit, which can have only the value 0 or 1. But the quantum equivalent, known as a quantum bit or qubit, can have both the value 0 and 1 at the same time as a result of superposition. Two qubits can have four values at the same time – 00, 01, 10 and 11 – and each additional qubit doubles the number of possible states. This means that a quantum computer with 300 qubits would be able to represent more values than there are particles in the entire universe. And it only takes 50-60 qubits to exceed the computing power in today's supercomputers.

The first ideas involving the use of quantum systems for calculations came in the 1980s, but at the outset they were not considered to have any practical significance. There was both a lack of usable algorithms (quantum computers cannot be programmed in the same way as normal computers) and nobody knew how to correct the errors that would inevitably arise in a quantum computer.

The situation changed drastically in 1994 when Peter Shor published a quantum algorithm which rapidly finds the prime number factors that make up a given large number, which is the key to cracking today's encryption codes (see 3.3 Quantum communications). A year later he showed how a special error correction code can deal with the errors that occur in a quantum computer. This sparked an interest in building a quantum computer among researchers around the world. A quantum computer with many qubits is the ultimate goal in quantum technology according to many.

The most promising technologies for building a quantum computer are ion traps and superconducting circuits. In an ion trap, qubits are made up of floating ions which are held in place by electric and magnetic fields, and are manipulated by laser light. The ion trap record is currently 14 fully controlled qubits.

Superconducting qubits consist of electric circuits without any electrical resistance (= superconducting), where the energy switches between being electric and magnetic. The circuits can be manipulated by microwaves. Since the circuits are placed on a microchip, it is relatively straightforward to scale up to a large number of qubits. The short decoherence time (see section 2.4) has been a major limitation, but following diligent development work it has been possible to increase it dramatically in the past 20 years. IT companies such as Google, IBM and Intel have launched research projects into superconducting quantum computers. In autumn 2017 IBM launched the largest processor so far with 16 qubits, and Google has announced that it is working on a 49-qubit processor.

An important but difficult element is to implement codes that limit the effect of the errors that inevitably occur, just as they do in all computers. One option is to allow each logical qubit to be represented by several physical qubits which are read out four at a time to check whether an error has occurred. Another option is also to code the quantum information in microwaves.

A quantum computer can also be used to solve problems involving a large number of different possibilities, such as optimisation problems in machine learning and artificial intelligence. It is also suited to calculating the characteristics of large molecules – for example, for developing new pharmaceutical products or materials.

3.2 Quantum simulation

A quantum simulator is a specially designed quantum computer constructed to simulate a certain process. It can therefore only solve a limited number of problems. If you want to solve other problems, you need to build a new quantum simulator, designed to solve those specific problems.

A number of fairly simple examples of quantum simulation have already been demonstrated, but have not yet surpassed classical computers. Rapid progress is, however, being made and researchers are preparing to scale up to the level required to demonstrate what is known as quantum supremacy, which means solving a problem that is beyond the reach of even the most powerful classical computer. Usable applications for quantum simulation are expected within five years.

3.3 Quantum communication

Our internet-based society with internet banks, digital medical records, web-based commerce etc, is based on the secure transmission of information. Today encryption is used, which is based on problems which are presumed to be difficult to calculate such as finding the prime number factors which have created a specific very large number.

But when the quantum computer makes its appearance, cracking today's encryption will be child's play. However, quantum technology also offers a solution – the secure transmission of encryption keys via quantum communication. This is the only known solution which can guarantee that an outsider cannot read the encrypted message.

The encryption key is the code that the recipient needs in order to decode the encrypted message. The sender uses individual photons to send the encryption key to the recipient. Since it is not possible to measure a photon without it being affected, you can be sure of detecting whether an outsider has tried to steal the encryption key.

Nowadays there are commercial systems which can transfer quantum encryption keys via an unbroken optical fibre over a distance of approximately 100 kilometres, but at a fairly low speed.

In order to guarantee the security of the next generation of communications systems, a global quantum network must be developed, which can rapidly and securely transmit encryption keys between many different points. The quantum phenomenon of entanglement (see section 2.2) play a key role when it comes to strengthening and transmitting quantum signals in a large network.

3.4 Quantum sensing

Human knowledge of the world and our technological progress is limited by what we can measure and how precisely we can do so. Researchers are now in the process of learning to use individual particles such as photons and electrons as sensors in measurements of forces, gravitation, electric fields etc. Measurement capability is thus pushed far beyond what had previously been possible. For example, researchers have demonstrated measuring techniques which can measure forces as weak as the gravitational force between two people on either side of the American continent.

Heisenberg's uncertainty principle (see section 2.3) limits how precisely measurements can be made. In most cases the uncertainty is so incredibly small that it can be disregarded. But on a very small scale, such as when measuring a single electron, the limitations of the uncertainty principle are significant. Quantum technology provides tools for enhancing the precision in those quantities we want to measure by shifting the uncertainty to another variable (known as a squeezed state, see section 2.3). It also provides the opportunity to create specially designed quantum states for specific measurement tasks that make the measurement insensitive to the strongest sources of noise.

The development of quantum sensors will lead to more powerful instruments for measuring electric and magnetic fields both in our environment and inside our bodies. We can also expect to have instruments which can measure local variations in gravitation to find minerals, water or embedded pipelines and advanced warning systems for earthquakes and volcanic eruptions.