Appendix 1: An Introduction to Quantum Technology

A1.1 Definition of Quantum Technology

Quantum physics was developed in the early 20th century. Some of its elements, such as quantised energy levels and the properties of light deriving from its dual wave/particle nature, are key to well established areas of existing technology. These technologies are retrospectively being called 'Quantum 1.0' and include electronics and photonics. Electronics relies on the energy band structure of semiconductors, which is a quantum phenomenon, and electrons are the fundamental quantum of electricity. Similarly, photonics is the technology based on the photon, the fundamental quantum of light, and includes all aspects of lasers and their applications.

The principal concepts of quantum physics are that:

- Matter and energy (e.g., light) simultaneously have the characteristics of waves and particles, ***wave-particle duality***.
- The energy states of a physical system (e.g., electrons in atoms) can take discrete, ***quantised***, values.

Until that state is measured the system can be simultaneously in different states, ***superposition***; and particles can be ***entangled*** so that the observed property of one particle determines the state of the entangled partner.

Quantum 2.0 exploits superposition and entanglement to enable entirely new capabilities. For example, *superposition* potentially provides orders-of-magnitude increases in computing speed, albeit with substantial practical problems yet to be resolved; *entanglement* is the basis of new encryption techniques which represent the best candidate to address the potentially critical threat to data and communications security posed by quantum computing (see Section A1.2). Superposition and entanglement also enable other techniques, such as sensing by atom interferometry (see Section A2.4) with applications including navigation and geoscience.

How quantum superposition enables increased computing speed:

1. In conventional computing, **data to be processed comprise digital 'bits'**, '1's and '0's, physically represented as energy states in electronic circuits. Therefore, if two bits can be processed in parallel, then the computation proceeds twice as fast; and if there are *N* bits, then *N* times as fast.
2. But **in quantum technology computing, the data exist as *qubits*** (for example as individual atoms or ions). Because these qubits exhibit superposition, they each can be regarded as being simultaneously in different states. So, for example, each of two superposed qubits can be simultaneously in the '0' or '1' state; and hence two qubits can represent four possible states: 0,0; 0,1; 1,0; 1,1. Therefore, each additional qubit doubles the number of possible states; and so with *N* qubits, there are 2^N possible states, compared with only N in the conventional computing case.

The principal areas of application of 'quantum 2.0' technologies currently envisaged are in computing, communications, and sensing and imaging. Sensing includes the specific and significant area of clocks and timing. Precise timing, currently provided by atomic clocks and distributed by the satellite global positioning system, is critical to the operation of the world's communications system, with particular importance in financial transactions; it is also fundamental to navigation. Quantum technology would potentially remove the vulnerable dependence on satellite navigation systems for distribution of time standards.

A1.2 Computing

The key potential benefit of quantum computing derives from *superposition* to potentially achieve very substantial improvements in computing speed, where the data to be processed are stored as *qubits* (see page 1). The key technical challenge is that the qubits are fragile (they exist, for example, as individual ionised atoms or energy spin-states of atoms). The energy states of the qubits, and hence the information that they contain, are corrupted by their interaction with the environment so that errors accumulate, thus potentially limiting performance or requiring large numbers of additional qubits to correct the errors. Keeping qubits stable currently generally requires extremely low temperatures (less than 1 Kelvin) and near-perfect vibration isolation, posing major engineering challenges.

Research into several different technology platforms continues, with no primary candidate yet identified.

Quantum computers require quite different kinds of programming from conventional ones; they need new operating systems and they are not yet suited to universal problem solving. However, they potentially have special abilities in data science, modelling, and planning, offering significant opportunities in (for example), finance, logistics, and discovery of new drugs and materials, and in the energy and communications infrastructure. Quantum computers are particularly well suited to some specific algorithms, of which perhaps currently the most important are *Shor's algorithm* for encryption and *Grover's algorithm* for digital searching, described in the text box.

The technology also potentially poses threats and challenges, for example in risks to currently used data encryption techniques or ethical considerations in the development of new artificial intelligence applications.

Quantum computing represents the largest single area of quantum technology activity. Companies and government initiatives include:

- The first quantum computer was announced by D-Wave in Canada in 2015, although it has been debated whether it used quantum principles.
- The UK launched its National Quantum Technology Programme in 2013 with around £1bn funding (see above), and the USA launched its $1.2bn National Quantum Initiative in 2018.
- UK quantum computing start-up OQC has built a complete unit including the control system, the hardware and the software. It is the only quantum computer commercially available in the UK.
- Google's 'Sycamore' quantum circuit in 2019 was the first to demonstrate 'quantum advantage' compared to a conventional device.
- Honeywell's collaboration with Cambridge Quantum Computing has culminated in Honeywell acquiring the Cambridge company.
- IBM have made devices from their Quantum Computing Division available to nearly 200,000 clients worldwide via Cloud-based systems, with machines also installed at a German Fraunhofer Institute and at the University of Tokyo.
- A University of Maryland start-up, IonQ, were the first publicly traded purely quantum computing company, raising $83M for their systems based on quantum-entangled ions with laser input and output.

Examples of algorithms suited to quantum computing:

1. *Shor's algorithm* (for factorising integers): almost all current encryption techniques, used (for example) for making on-line payments or securing data, rely on prime factors of very large numbers that could not practically be computed with current technology but would be within the capabilities of quantum computing. Hence quantum computing could pose a major threat to the security of communications and data.
2. *Grover's algorithm*: is used to implement unstructured searches, which is key to e.g. logistical planning and data science more generally.

- There are many Chinese start-ups too.
- In addition to hardware, software development is also essential. As an example, Riverlane (a Cambridge-based company) are a commercial supplier of quantum technology software, for example supplying the UK National Quantum Computing Centre.

The primary technology platform remains unclear and a key decision yet to be made is whether preferred systems will operate at room temperature (e.g. based on trapped ions) or whether they will be cryogenic. The most important practical problem to be tackled is environmental noise and its effect on the qubits:

- IBM and Google use superconducting systems (i.e., at very low temperatures).
- Honeywell use trapped ions.
- Microsoft use electron quasi-particles (collaborating with Delft University of Technology and the Niels Bohr Institute in Copenhagen).
- Orcal Computing (Oxford) and PsiQuantum (California) use photonic technology.
- Other companies using photonics are Quix Quantum (Netherlands). Quantum Brilliance is a German-Australian company exploring room temperature diamond quantum computing,

The applications being pursued by the commercial companies are primarily in the finance sector, oil and gas, automotive, medical and healthcare, and aerospace:

- IBM users include Exxon Mobile, Daimler, JP Morgan Chase and the Cleveland Clinic (for pathogen research);
- Honeywell: cyber security; drug discovery; material science; finance; natural language processing; artificial intelligence;
- IonQ: a cloud-based system, working with the VW group, to optimise assembly lines and for future applications such as optimising traffic routing;
- QCWare (California): finance (in collaboration with Goldman Sachs), and primarily for conducting 'Monte Carlo' simulations (a form of statistical modelling), for which the error-prone nature of quantum computing is less serious; and
- IBM recognise potential opportunities e.g. in simulating properties of chemical systems, perhaps for drug discovery.

Quantum computing software developers in the UK such as Cambridge Quantum and Riverlane have also partnered with end-users in finance, oil and gas, pharmaceuticals and materials in applications involving computational chemistry and simulation.

A1.3 Communications

The primary application of quantum technology is in achieving data security. The current technique used to transmit data securely is known as *public key cryptography*. The 'key' comprises a string of random numbers. However, conventional techniques do not generate numbers that are perfectly random, thereby posing a security risk. Quantum technology is able to generate truly random numbers, and commercial products for that purpose are emerging.

Public key cryptography can, in principle, be broken by quantum computing techniques. Quantum technology provides an alternative technique not susceptible to that threat, by transmitting the means to decrypt the data using *entangled photons* to form a *quantum key*. If an attacker detects a photon that is part of the quantum key, then it will alter the state of the photon with which it is entangled, thus revealing the attack. The technique is called *quantum key distribution (QKD)*. Even when QKD is used, there remain security risks through side-channel attacks, for example by using high intensity laser pulses.

A1.4 Sensing and Imaging

Quantum clocks

Sensing includes the specific and significant area of clocks and timing. The world's time standards are all defined relative to atomic resonance frequencies using 'atomic clocks', which are an example of 'Quantum 1.0'. Timekeeping with the accuracy of atomic clocks is essential in communications technology, for example for timing financial transactions. It is also a fundamental requirement in navigation. The technology of conventional atomic clocks is suitable for e.g. standards laboratories, but would not be suitable to make smaller, more applicable or portable clocks. Consequently, 'world time' is distributed by radio signals, normally from the world's global positioning system (GPS), with consequent security and reliability risks.

'Quantum 2.0' could in principle provide more practical atomic clocks suitable for widespread use and reduce dependence e.g. on GPS.

The current candidate technique employs atoms cooled and loaded into an 'optical lattice', the *optical lattice clock*, where the cooling is achieved using laser techniques.

Atom interferometers

Interferometry is a very well-established technique in optics for making precise measurements by exploiting the wave nature of light, often by using lasers (see the text box). Quantum physics shows that atoms also have wave-like properties, and so it is possible to build an interferometer using beams of atoms rather than beams of light.

Atom interferometry replaces beams of light with clouds of supercooled atoms, driven into a quantum superposition of two states using laser techniques, analogous to the two beams in an optical interferometer. The 'beams' are then recombined, again using laser techniques, to reveal the interference. Therefore, any physical phenomenon that affects how long it takes an atom to travel between the point of division and recombination, and has a differential effect between the two 'beams', will be revealed by the interference with great sensitivity.

Atom interferometry has been successfully demonstrated for example to measure the local gravitational field, acceleration, and electric and magnetic fields. It has been applied in navigation (without the need for GPS), geoscience and geo-engineering measurements, and (with magnetic field sensing) for optimising battery manufacture. Quantum technology magnetic field sensing also has potential for medical applications, for example for brain activity imaging.

How does interferometry work?

As an example, consider a laser beam divided to follow two different paths and then brought back together so that the light waves exactly overlap. If the two paths have just the same length, then the 'crests' of the waves of one path overlap the 'crests' of the second path, and similarly for the 'troughs': the interference is constructive, and a strong optical signal is produced. But if one of the paths is lengthened by exactly half a wavelength then the interference becomes destructive (the 'crests' of one path overlap the 'troughs' of the other) and in this perfect case the optical signal disappears completely. Measurements can therefore readily be made on the nanometre scale of the wavelength of light.

Imaging

Quantum imaging techniques are those in which images are formed by making measurements on individual photons. The techniques are analogous to radar range-finding, in which the distance to a target is found by measuring how long it takes a pulse of energy to travel from the transmitter to be scattered from the target and then back to the receiver.

Quantum imaging is based on producing and detecting single photons and timing their travel to the target and back. By making time-of-flight measurements on a large number of individual photons and with image-processing calculations, it is possible to build-up an image of the target even if the photons have been scattered on their way to and from the target. It is therefore feasible to image through turbid media and 'to see round corners'.

scottish science advisory council

Produced for Scottish Science Advisory Council by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
(June 2022)

scottishscience@gov.scot