CENTRE FOR JOINT WARFARE STUDIES

SYNODOS PAPER

QUANTUM COMPUTING AND LIKELY DEFENCE APPLICATIONS

SYNODOS PAPER | VOL - XI NO 13 / DEC 2017

Quantum Theory

Quantum theory is the theoretical basis of modern physics that explains the nature and behavior of matter and energy on the atomic and subatomic level is sometimes referred to as quantum physics and quantum mechanics. Quantum mechanics (QM) is the body of scientific laws that describe the strange behavior of photons, electrons and other particles that make up the universe. QM is defined as a theory of matter that is based on the concept of the possession of wave properties by elementary particles, that affords a mathematical interpretation of the structure and interactions of matter on the basis of these properties, and that incorporates within it quantum theory and the uncertainty principle, called also wave mechanics.[1]

[1]https://www.merriam-webster.com/dictionary/quantum%20mechanics.

Quantum mechanics is critically important for understanding how individual atoms combine covalently to form molecules. The application of quantum mechanics to chemistry is known as quantum chemistry. Relativistic quantum mechanics can, in principle, mathematically describe most of chemistry. QM also tells us how electromagnetic waves work. It is also called quantum physics or quantum theory. Max Planck, in 1901, accurately described the radiation by assuming that electromagnetic radiation was emitted in discrete packets or quanta. Planck's quantum hypothesis is a pioneering work, heralding advent of a new era of modern physics and quantum theory. In the words of Scott Aaronson[2] , "Quantum mechanics

[2]Scott Aaronson, "Quantum Computing since Democritus", Cambridge University Press, ISBN 978-0-521-19956-8 Paperback

is a beautiful generalisation of the laws of probability: a generalisation based on the two-norm rather than the one-norm, and on complex numbers rather than nonnegative real numbers. It can be studied completely separately from its applications to physics (and indeed, doing so provides a good starting point for learning the physical applications later). This generalised probability theory leads naturally to a new model of computation–the quantum computing model–that challenges ideas about computation once considered a priori, and that theoretical computer scientists might have been driven to invent for their own purposes, even if there were no relation to physics. In short, while quantum mechanics was invented a century ago to solve technical problems in physics, today it can be fruitfully explained from an extremely different perspective: as part of the history of ideas, in math, logic, computation, and philosophy, about the limits of the knowable."

The world is currently experiencing a second quantum revolution. In the first quantum revolution, the fundamental laws of the microscopic realm were discovered and quantum science was formulated. In the following years, ground-breaking technologies such as the transistor and the laser were developed. These inventions can only be understood and developed with the help of quantum mechanics. In the second quantum revolution, technologies are being developed that explicitly address individual quantum states and make use of the strange quantum properties, such as superposition and entanglement, commonly referred to as quantum technologies (QT). A number of start-up companies were founded over the last decades which offer QT to highly specialised markets. Quantum cryptography is among the most advanced QT with highly specialised small and medium-sized enterprises already selling their products to governments, banks and other customers with highest security requirements. Large global companies such as Google, IBM, Intel, Microsoft and Toshiba have recently started to invest heavily in QT. Governments are also starting large funding programmes in the field. Besides quantum computation, quantum communication is particularly high on the agenda of many countries, especially in China, who plans to invest massively and has recently launched a satellite with quantum communication devices.

Quantum Computing

Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.[3] The development of actual commercial quantum computers is still in its infancy, but experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits. Both practical and theoretical research continues, and many national governments and military agencies are funding

[3]Gershenfeld, Neil; Chuang, Isaac L. (June 1998). "Quantum Computing with Molecules", Scientific American.

quantum computing research in addition to developing quantum computers for national security, business, environmental and cryptanalysis purposes. Large-scale quantum computers would theoretically be able to solve certain problems much more quickly than any classical computers that use even the best currently known algorithms. A classical computer could in principle simulate a quantum algorithm, as quantum computation does not violate the Church–Turing thesis. On the other hand, quantum computers may be able to efficiently solve problems which are not practically feasible on classical computers.

A classical computer has a memory made up of bits, where each bit is represented by either a one or a zero. A quantum computer maintains a sequence of qubits. A single qubit can represent a one, a zero, or any quantum superposition of those two qubit states. Quantum algorithms are often probabilistic, in that they provide the correct solution only with a certain known probability. A quantum computer with a given number of qubits is fundamentally different from a classical computer composed of the same number of classical bits. For example, representing the state of an n-qubit system on a classical computer requires the storage of 2n complex coefficients, while to characterize the state of a classical n-bit system it is sufficient to provide the values of the n bits, that is, only n numbers. Although this fact may seem to indicate that qubits can hold exponentially more information than their classical counterparts, but qubits are only in a probabilistic superposition of all of their states. More details on the sequences of operations used for various quantum algorithms such as study of Shor's algorithm, Grover's algorithm, Deutsch–Jozsa algorithm, amplitude amplification, quantum Fourier transform, quantum gate, quantum adiabatic algorithm and quantum error correction is useful for understanding quantum computing. Since chemistry and nanotechnology rely on understanding quantum systems, and such systems are impossible to simulate in an efficient manner classically, quantum simulation is likely to be one of the most important applications of quantum computing. Quantum simulation could also be used to simulate the behavior of atoms and particles at unusual conditions such as the reactions inside a collider.

The ideal expected number for a universal quantum computer is 50 qubits. At this level scientists will surpass the functionality of the fastest supercomputers today. Classical computers are extraordinarily powerful and will continue to advance and underpin everything in business and society. But there are many problems that will never be penetrated by a classical computer. To create knowledge from much greater depths of complexity, quantum computers will be needed. Therefore, International Conference on Quantum Science and Applications (ICQSA-2016 conference) also focused on recent modern theoretical and experimental developments of quantum science in multi-disciplinary aspects of areas of mathematics, physics, statistics, chemistry, biology, computer science, electronics,

informatics, medicine and education.

Nuclear Magnetic Resonance (NMR) Quantum Computing. Nuclear Magnetic Resonance quantum computing is one of the several proposed approaches for constructing a quantum computer that uses the spin states of nuclei within molecules as qubits. NMR differs from other implementations of quantum computers in that it uses an ensemble of systems, in this case molecules, rather than a single pure state. Initially the approach was to use the spin properties of atoms of particular molecules in a liquid sample as qubits - this is known as liquid state NMR (LSNMR). This approach has since been superseded by solid state NMR (SSNMR) as a means of quantum computation.

Global Developments

IBM recently announced that the company is set to build the first universal quantum computer for science and business. The new division called IBM Q has been set up to make such computers and sell them commercially.[4] For the end user, initial quantum computers will be accessed via the cloud. More countries, including Russia, China, the US, and Europe are striving to develop their own Quantum Computers, with the US and China leading the research in this field.

Russia. Two leading Russian quantum computing research institutes, the Russian Quantum Center and the MISiS National University of Science & Technology, announced recently the creation of a joint project known as Quantum Center, for creating quantum computers. Last year, the Russian state atomic energy corporation Rosatom, the Foundation for Advanced Studies and the Ministry of Education and Science has also signed a joint three-year project on the development of a quantum computer. Rosatom's nuclear weapons research institute at the All-Russia Research Institutes of Automatics (VNIIA) has been designated to take the lead in organising the project.[5]

USA. It is believed that investments for the development of quantum computers by companies such as Microsoft, Intel, IBM, D-Wave and Google make the US the leader in this field. In December 2015 NASA publicly displayed the world's first fully operational $15-million quantum computer made by the Canadian company D-Wave at the Quantum Artificial Intelligence Laboratory at its Ames Research Center in California's Moffett Field. The device was purchased in 2013 via a partnership with Google and Universities Space Research Association. The presence and use of quantum effects in the D-Wave quantum processing unit is more widely accepted. In August 2016, scientists at the University of Maryland successfully built the first reprogrammable quantum computer. In March 2017, IBM announced an industry-

[4]IBM's Quantum Computers to Open 'New Realm of Computational Power', https://sputniknews.com/science/201703071051354761-ibm-quantum-computer/

[5]https://sputniknews.com/military/201705111053523495-quantum-computing-military-applications-analysis/

first initiative to build commercially available universal quantum computing systems called IBM Q. The company also released a new API (Application Program Interface) for the IBM Quantum Experience that enables developers and programmers to begin building interfaces between its existing five qubit cloud-based quantum computer and classical computers, without needing a deep background in quantum physics. Recently, IBM announced the successful testing of its most powerful universal quantum computing processors.

Europe. Europe is focusing on the creation of its own quantum computer over the next ten years, investing the equivalent of about a billion dollars into its Quantum Technologies Flagship Program. European Commission has announced an ambitious flagship programme to start in 2018. The flagship will be structured along four mission-driven application domains[6] :

- Communication, to guarantee secure data transmission and long-term security for the information society by using quantum resources for communication protocols.
- Computation, to solve problems beyond the reach of current or conceivable classical processors by using programmable quantum machines.
- Simulation, to understand and solve important problems, e.g. chemical processes, the development of new materials, as well as fundamental physical theories, by mapping them onto controlled quantum systems in an analogue or digital way.
- Sensing and meteorology, to achieve unprecedented sensitivity, accuracy and resolution in measurement and diagnostics by coherently manipulating quantum objects.

European Quantum Communication Research Agenda[7] flagship will centre mainly on quantum cryptography and quantum networking. In flagship terms, this domain is simply called quantum communication. Its main applications are in probably secure communication, long-term secure storage, cloud computing and other cryptography-related tasks, as well as, in the future, secure quantum communication networks distributing quantum resources like entanglement and connecting remote devices and systems.

China. China is already launching unhackable experimental satellites with quantum-based communication systems, building quantum radars, hundreds of kilometers worth of quantum communication

[6]Max F Riede, Daniele Binosi, Rob Thew and Tommaso Calarco, 'The European quantum technologies flagship programme', Quantum Science and Technology, Volume 2, Number 3 , 23 June 2017.

[7]Max F Riede, Daniele Binosi, Rob Thew and Tommaso Calarco, 'The European quantum technologies flagship programme', Quantum Science and Technology, Volume 2, Number 3, 23 June 2017.

lines, and creating the world's fastest supercomputers. China's quantum satellite - nicknamed Micius after a 5th century BC Chinese scientist - blasted off from the Jiuquan satellite launch centre in China's northwest Gansu province on August 16, 2016.

Developments in India

Indian Institute of Science is deeply involved in the Quantum Computing research activities. The areas covered by the Institute are[8]:

- NMR (Nuclear Magnetic Resonance) implementation of quantum algorithms
- Implementation of superconducting qubits
- Implementation of quantum dots and nanostructures
- Implementation of ion trap qubits
- Quantum algorithms
- Quantum entanglement in many body systems
- Large scale computation with integer, polynomial and power series
- Foundational aspects of quantum computation

While the Physics departments at the Indian Institute of Science, Bangalore, and the Harish Chandra Research Institute, Allahabad, have only forayed into the theoretical aspects of quantum computing, DST (Department of Science and Technology) is actually planning to fund a quantum computing project in a big way.[9]

Likely Defence Applications

The first applications for a universal quantum computer are likely to be for drug and materials discovery, financial services and supply chain. Purely theoretical computation capabilities aside, the development of Quantum Computers is of great importance for the defence forces. Most major countries have already commenced projects for this purpose.

First and most obvious military application for a modern, fully functional quantum computer is the capability to engage in near-instantaneous hacking into encrypted military servers, and those controlling the national infrastructure systems of the probable adversaries.[10] In early 2014, based on documents provided by former NSA contractor Edward Snowden, it was reported that the US National Security Agency (NSA) is running a $79.7 million research programme titled "Penetrating Hard Targets" to develop a quantum computer capable of breaking vulnerable encryption.[11]

---

[8]Centre for Quantum Information and Quantum Computation, Indian Institute of Science, Bangalore 560012, http://chep.iisc.ac.in/CQIQC.html

[9]Jacob Koshy, India joins quantum computing race, The Hindu, 21 September 2017.

[10]Quantum Computing Arms Race Takes Shape as China, US, Russia Vie for Supremacy,https://sputniknews.com/military/201705111053523495-quantum-computing-military-applications-analysis/#comments.

[11]"NSA seeks to build quantum computer that could crack most types of encryption", Washington Post, 2 January, 2014

The speed of data computation and processing which quantum systems will also significantly improve the work of unmanned and autonomous military vehicles, to which the conduct of military operations will be increasingly entrusted in the foreseeable future.

Quantum communication is already used today for niche applications, but as the technology develops, its use will spread and it has the potential to become an integrated, standard component of global communication networks. To reach this goal, a significant amount of software and hardware development would be needed.[12]

Quantum Computing for Aerospace[13]. Researchers at the University of Southern California (USC) Lockheed Martin Quantum Computing Center (QCC) recently made a major breakthrough in fielding future possibilities for quantum computers. In July 2017, QCC researchers upgraded their existing 512-qubit D-Wave Two system (D-Wave 2X processor) to 1,098 qubits, making it the new leader in qubit capacity.

The new processor will be used to study how and whether quantum effects can speed up the solution of tough optimisation, machine learning and sampling problems. Machine learning algorithms are widely used in artificial intelligence tasks. Engineers within the aerospace industry and many other industries expect the processing power of quantum computers to be able to greatly improve computer modeling and simulation. The main focus of the research currently is to aid in helping solve a problem that exists within avionics and all computing software development: the problem of Verification and Validation (V&V). One of the important problems that exists in aviation and really all software development in general, is making sure the software system being developed is what you intended it to be. The verification and validation of software is a complex problem to solve, its very time consuming and expensive as well; quantum computing has the potential to expedite this process.

Aircraft system software is safety critical, and is among the most heavily regulated and certified software to develop and integrate across all major technological industries. Companies such as Lockheed Martin, put a great deal of effort into ensuring that aircraft system software is correct. The F-35's eight million lines of code is an example of this. Quantum-computing technology could give software developers the ability to achieve capabilities, such as rapidly debugging millions of lines of software code and resolving complex aerospace computational problems.

Aviation software applications that are designed to aid in the routing and scheduling of aircraft, and doing so in the most cost effective way, calculating how

[12]Max F Riede, Daniele Binosi, Rob Thew and Tommaso Calarco, 'The European quantum technologies flagship programme', Quantum Science and Technology, Volume 2, Number 3 , 23 June 2017.

[13]Woodrow Bellamy III, Quantum Computing for Aerospace, What are the Possibilities? http://www.aviationtoday.com/2016/08/15/quantum-computing-for-aerospace-what-are-the-possibilities/

much fuel is required for a commercial aircraft to arrive at an airport or even at a waypoint through its flight plan, these are the types of problems that quantum computing can aid. The USC-Lockheed Martin QCC hosts one of two D-Wave systems that currently operate outside of D-Wave's headquarters. The other system is owned by Google and hosted at NASA's Ames Research Center. A third is being installed at Los Alamos National Laboratory, according to QCC.

Airbus Industries has also shown an interest in quantum computing technology, mainly in using the concept to speed up aircraft research. In 2015, Airbus Defence and Space established a quantum computing unit at its Newport, UK plant. One particular application the company is exploring the use of quantum computing for is digital modeling and simulation. While it currently takes engineers years to model the process of air flowing over a wing, a quantum computer could take just a few weeks to model every single atom of air flowing over a wing at all angles and speeds.

Optimisation is one of the primary uses of quantum computing, for example using computer applications to assess the optimal amount of fuel and the optimal speed at which to operate a commercial aircraft. Presently, it could be a decade or more before quantum processors could be used inside of Flight Management Computers (FMC).

Quantum computers will also be used at various stages of the design of new weapons, new materials, and even in the development of new strategies for warfare.

Air Cmde Trilok Chand (Retd)
Senior Fellow CENJOWS

Centre for Joint Warfare Studies
Kashmir House, Rajaji Marg, New Delhi-110 001
Tel. Nos : 011-23792446, 23006535, 23006538/9, Fax : 011-23792444
Website : https://cenjows.gov.in, e-mail : cenjows@yahoo.com