3-2019

Quantum computing is here to stay

Manoj THULASIDAS
Singapore Management University, manojt@smu.edu.sg

QUANTUM COMPUTING IS HERE TO STAY

MANOJ THULASIDAS

ASSOCIATE PROFESSOR OF INFORMATION SYSTEMS (EDUCATION)
SCHOOL OF INFORMATION SYSTEMS
SINGAPORE MANAGEMENT UNIVERSITY

"DON'T HOLD YOUR BREATH FOR QUANTUM COMPUTERS TO CHANGE THE WORLD QUITE YET."

QUANTUM COMPUTING is emerging from university laboratories and entering the industry arena at a painfully slow pace. The measured and deliberate progress is understandable given its complexity and promise. The stakes are high, because quantum computing presents the tantalising prospect of solving problems previously considered completely insoluble.

The impetus behind quantum computing is being driven, not just by academic institutions, but by a growing body of commercial and military interests. Google, for example, is investing in the next generation of quantum computing, as is NASA. Both are using machines made by D-Wave, a Canadian company. According to Google, these wonder machines perform certain tasks 100 million times faster than their conventional counterparts.

Some scientists still remain sceptical whether quantum computing can ever solve major problems that ‘classical’ devices cannot. Besides, D-Wave machines cost around $10 million dollars each – a serious barrier to entry for those who would like to exploit this emerging sector.

Companies and institutions around the world, however, are betting that quantum computing will revolutionise a range of industries, including transport, space exploration, medicine and even politics.

Google has used a quantum computer to design software that can distinguish cars from landmarks , assisting driverless cars. Other such machines are expected to be able to perform similar miracles. For instance, analysis of the vast amount of data collected by telescopes can help locate Earth-like planets. Analysis of traffic patterns in the air and on the ground could help prevent bottlenecks. New computational models could help determine how diseases develop. Political campaigners will be able to analyse vast amounts of marketing information to exploit individual voter preferences – faster than they already do. The possibilities are endless.

The advent of quantum computers has a flipside. It will present a major challenge to cybersecurity. All methods currently used to encrypt credit card details and other classified information would instantly become transparent. RSA cryptography – a method used widely to keep our data safe – relies on the fact that the kind of computers that we have today find it difficult and time-consuming to factor large numbers. However, quantum computers are likely to be able to overcome this hurdle by using the maths of number theory to turn the factoring problem into one of recognising periodic patterns within certain mathematical functions.

Why is it that quantum computing can address these different problems where conventional computing falters? It boils down to the fundamental aspect of how information is represented in a computer. In a classical computer, it is represented using bits, which can exist in one of two states: 0 or 1. On the other hand, quantum computers, built on the principles of quantum physics, take advantage of the ability of subatomic particles to exist in more than one state at the same time. Known as ‘superposition,’ this uniquely quantum mechanical aspect gives them bits that can have an infinite number of states (quantum bits or ‘qubits’) with which to make calculations.

People have tended to focus on the number of qubits needed for a universal quantum computer, often overlooking other essential parts of the puzzle. Quantum computers operate on principles completely different from those of existing computers. In addition to qubits, the control electronics and microwave pulses needed to manipulate qubits are radically different from conventional machines. Quantum computers have digital electronics that error-correct because these devices are very fragile. Additionally, even the programs, the algorithms written for the quantum devices, are entirely different from conventional digital programming.

With so many variables of such complexity at play, it is easy to see why some researchers think it could take another 20 years before the first ‘universal’ quantum computer appears in the market. In the meantime, physicists are building more specialised devices, known as quantum simulators, which are designed specifically to model quantum systems, but can’t carry out other types of algorithms.

Don’t hold your breath for quantum computers to change the world quite yet. However, given the pace of progress and industry interest, do be prepared for the day when they burst into everyday life and change everything. It may be closer than you think.