The weird world of quantum computers

Author: Barry Dwolatzky

The magician gazed out at his audience. “It’s a cold night,” he said. “Does anyone have a pair of gloves I can borrow?”

There was some shuffling in seats and nudging of neighbours. A middle-aged man in the front row stood up and waved a pair of black leather gloves. “Here you are,” he said. “I hope I get them back!”

The magician smiled as he walked to the edge of the stage and took the gloves. “Oh, you’ll get them back,” he said. “They might just have changed a little!” he said mysteriously.

The trick went like this. The magician laid the black leather gloves on a table. A camera positioned overhead projected an image of the gloves onto a huge screen behind the magician. There was a left glove and a right glove. A matching pair. There were also two identical boxes on the table. He lifted the lid of one box and popped the left glove into it. He replaced the lid. He then opened the other box, put the right glove into it and closed that lid. He then shuffled the boxes.

“Does anyone know for certain which box holds the left glove?” he asked. Nobody in the audience responded. He lifted one of the boxes. “I know for **certain** that this box contains the left glove,” he said. He pointed at the other box. “I also know for **certain** that that box contains the left glove!”.

“What nonsense is this?” thought everyone in the audience.

He then asked his assistant to carry one of the boxes to a table in the foyer outside the auditorium. A camera projected its image on the screen. The magician opened the box in front of him to reveal the right glove. The assistant opened the box in the foyer to reveal the left glove. The magician raised his wand and tapped the right glove. It turned into a left glove. The audience gasped when they saw that at the **exact** same time the left glove in the foyer became a right glove.

Obviously, this happened! After all they were, and always will be a pair of gloves. One right and one left. Changing one means that the other must change. Not so obvious?

This hypothetical magic trick demonstrates two of the weird principles of quantum mechanics. The first is called “superposition”. Before either box was opened there was an equal probability of 100% that each box contained the left glove. Similarly, there was a 100% probability that each box contained the right glove. We say that each box contains **both possible states.** Only when the box is opened does it take on one or other of its possible states.
The second principle is called “entanglement”. Since the gloves are a matched pair changing one from left to right will **instantaneously** change the other from right to left. This will happen even if they are thousands or millions of kilometres apart.

While demonstrating this with gloves would require magic, these quantum phenomena are simply the way things work in the world of sub-atomic particles.

In the early 1980s the physicist Richard Feynman and others suggested ways that quantum mechanics principles could be used to devise computational algorithms. In 1994 Peter Shor suggested a quantum computing algorithm that could factor large integers far quicker than conventional computers can. Factoring integers lies at the heart of encryption algorithms used in most cyber security applications. Shor’s quantum algorithm makes it easy to crack even the strongest encryption. Nobody worried much, however, because at that time quantum computing was hypothetical.

It was the domain of theoretical physicists and mathematicians. And then in 2000 a group of scientists demonstrated an actual working quantum computer. Would all the world's encryption systems now become useless? Many experts started taking note of this new technology.

While conventional computers are based on “bits”, which are devices that can be in either one of two states i.e., “on” or “off”, or “0” or “1”, quantum computers are based on “qubits”, which are devices that can be in both of two states, i.e., “on” **and** “off”, or “0” **and** “1”. Qubits can also be “entangled” in the same way as a pair of gloves. The power of a quantum computer is measured by the number of qubits it has. The number of states it can deal with, in other words the complexity of the problem it can solve, is 2 to the power of the number of qubits. Adding a single qubit doubles the number of states.

In January 2019 IBM launched the world's first commercial quantum computer, the IBM Q, which had 20 qubits. By September 2020 they had released a 65-qubit machine and have plans to grow this to over 1000 qubits by 2023.

Applications for quantum computing are those in which many possible outcomes need to be explored. Such applications include modelling, optimisation and some forms of artificial intelligence. These are mostly things that can be done with conventional computers, but quantum computing will find solutions in a tiny fraction of the time. One of many possible applications could be the development of new drugs or chemical compounds by building detailed models of large and complex molecules. Quantum computers will never replace conventional computers. Your bank, for example, will not run its transaction system on a quantum computer and your cell phone would never have a quantum chip as its brain. The data centre of the future might however have a quantum computer as part of its available hardware ready to solve some part of some problems.

What about Shor's algorithm and using practical quantum computers to crack cyber encryption? The good news is that even with a 1000 qubit machine this will be impossible. For practical reasons we would need millions of qubits to break real-world cyber security algorithms. Quantum computing is still in its infancy but there is no doubt that one day it will be a key technology in the approaching 4th Industrial Revolution.