Explained | What is ‘quantum supremacy’?

What have researchers at Google achieved? How are quantum computers different from regular personal computers? How will it impact the technology world?

Updated – December 18, 2022 01:30 am IST

JACOB KOSHY

The story so far: Tech websites and theoretical computer-science outlets were aflame earlier this week after a story in the U.K.-based *Financial Times* said Google had claimed to have achieved ‘quantum supremacy’. In a line, it means that researchers at Google had solved a really difficult problem in seconds with the help of quantum computers which a supercomputer could not. The research paper is yet to be formally vetted by peers in the field and became public after having appeared briefly on the National Aeronautics and Space Administration (NASA) website — apparently some of its researchers were involved in the project. It is likely to reappear soon in a complete form.

What are quantum computers?

Quantum computers work differently from the classical computers we work on today. Exploiting the principles of quantum mechanics, they can easily tackle computational problems that may be tough for the classical computer as the size of the numbers and number of inputs involved grows bigger. Quantum computers do not look like desktops or laptops that we associate the word ‘computer’ with. Instead (and there are only a handful of them) they resemble the air-conditioned server rooms of many offices or the stacks of central processing units from desktops of yore that are connected by ungainly tangled wires and heaped in freezing rooms. Conventional computers process information in ‘bits’ or 1s and 0s, following classical physics under which our computers can process a ‘1’ or a ‘0’ at a time. The world’s most powerful super computer today can juggle 148,000 trillion operations in a second and requires about 9000 IBM CPUs connected in a particular combination to achieve this feat. Quantum computers compute in ‘qubits’ (or quantum bits). They exploit the properties of quantum mechanics, the science that governs how matter behaves on the atomic scale. In this scheme of things, processors can be a 1 and a 0 simultaneously, a state called quantum superposition. While this accelerates the speed of computation, a machine with less than a 100 qubits can solve problems with a lot of data that are even theoretically beyond the capabilities of the most powerful supercomputers. Because of quantum superposition, a quantum computer — if it works to plan — can mimic several classical computers working in parallel. The ideas

governing quantum computers have been around since the 1990s but actual machines have been around since 2011, most notably built by Canadian company D-Wave Systems.

How will it help us?

The speed and capability of classical supercomputers are limited by energy requirements. Along with these they also need more physical space. Looking for really useful information by processing huge amounts of data quickly is a real-world problem and one that can be tackled faster by quantum computers. For example, if we have a database of a million social media profiles and had to look for a particular individual, a classical computer would have to scan each one of those profiles which would amount to a million steps. In 1996, Lov K. Grover from Bell Labs discovered that a quantum computer would be able to do the same task with one thousand steps instead of a million. That translates into reduced processors and reduced energy.

ALSO READ

Also Read: What quantum computing means for your bank accounts and smartphones

In theory, a quantum computer can solve this problem rapidly because it can attack complex problems that are beyond the scope of a classical computer. The basic advantage is speed as it is able to simulate several classical computers working in parallel. Several encryption systems used in banking and security applications are premised on computers being unable to handle mathematical problems that are computationally demanding beyond a limit. Quantum computers, in theory, can surpass those limits.

What has Google achieved?

Quantum supremacy refers to quantum computers being able to solve a problem that a classical computer cannot. In the research paper, Google used a 53-qubit processor to generate a sequence of millions of numbers. Though these numbers appeared randomly generated, they conform to an algorithm generated by Google. A classical supercomputer checked some of these values and they were correct. Google’s quantum computer, named Sycamore, claimed ‘supremacy’ because it reportedly did the task in 200 seconds that would have apparently taken a supercomputer 10,000 years to complete.

Is this an important achievement?

Impressive as this may sound, experts caution that this does not imply that the quantum computer can solve every challenging problem thrown at it. The number-generating task was the equivalent of having a Ferrari and a truck compete in a race and, on the car’s predictable victory, declare that the Ferrari could do everything that a truck did. While IBM and a few other private establishments also have quantum computer prototypes, a common ailment is that they have their own unique propensity to errors and are not as amenable to executing real world problems as super computers.

Then again, nothing yet rules out the creation of new mathematical methods or techniques that would allow classical computers to execute the same task faster. Some experts even question the term ‘quantum supremacy’ coined by theoretical physicist John Preskill of the California Institute of Technology, United States. However, the Google feat shows that quantum computers are capable of a real world task. It gives confidence to private entrepreneurs and even academics to invest time and money to improving them and customise them to real world problems. In terms of the number of qubits, D-Wave Systems says it is ready to commercially launch a 5000-qubit system by 2020. It already has a 1000-qubit system at NASA. D-Wave claims that car maker Volkswagen used its quantum computers to figure out how best to control a fleet of taxis in Beijing relying on data from 10,000 cars, but the research paper describing this experiment does not quite explain how the proposed solution is better than algorithms that are currently used to optimise traffic flow.

What will it mean for online banking?

A question critics raise is how the use of quantum computing and its ability to break encryption codes will impact online banking. Breaking banking grade encryption is far away. Scott Aaronson, a theoretical computer scientist who has written on Google’s feat, opines that current encryption standards would require a quantum computer to have “several

thousand logical qubits” working in tandem perfectly. It requires millions of qubits of the kind that powers Sycamore to make ‘logical qubits’ and the 53 at Sycamore’s disposal does not quite cut the ice. However, there are other approaches to designing quantum computers and with it there may be cleverer ways to solve problems using them. Moreover, if technological breakthroughs were to pose a real threat to banking or financial operations, it is likely that banks will harness quantum computers themselves.

Is India working on quantum computing?

There are no quantum computers in India yet. In 2018, the Department of Science & Technology unveiled a programme called Quantum-Enabled Science & Technology (QuEST) and committed to investing ₹80 crore over the next three years to accelerate research. The ostensible plan is to have a quantum computer built in India within the next decade. Phase-1 of the problem involves hiring research experts and establishing teams with the know-how to physically build such systems.

Published – September 29, 2019 12:02 am IST