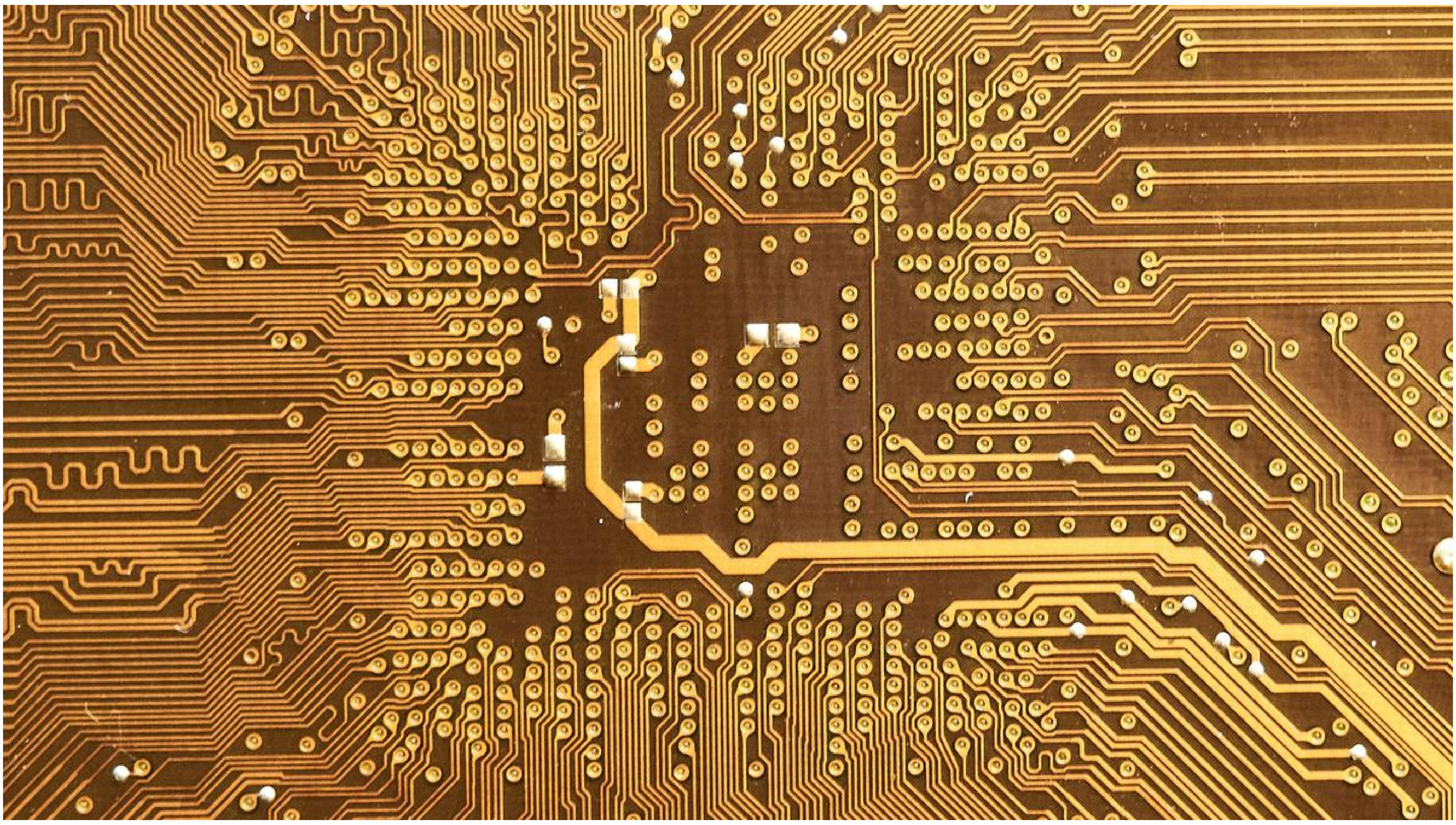
How can a quantum computer prove that it is superior?

A Google researcher has shown that one class of mathematical problems can be solved only by quantum computers, not classical computers.

Updated – September 21, 2023 07:26 pm IST

TEJASRI GURURAJ



A close-up view of a printed circuit board. | Photo Credit: manueljota/Unsplash

Quantum computing is becoming more popular – both as a field of study and in the public imagination. The technology promises more speed and more efficient problem-solving abilities, challenging the boundaries set by classical, conventional computing.

The hype has led to inflated expectations. But whether or not it can meet them, the raison d'être of a quantum computer is taken to be synonymous with the ability to solve some problems much faster than a classical computer can. This achievement, called *quantum supremacy*, will establish quantum computers as superior machines.

Scientists have been exploring both experimental and theoretical ways to prove quantum supremacy.

Ramis Movassagh, a researcher at Google Quantum AI, recently had a study published in the journal *Nature Physics*. Here, he has reportedly demonstrated in theory that simulating random quantum circuits and determining their output will be extremely difficult for classical computers. In other words, if a quantum computer solves this problem, it can achieve quantum supremacy.

But why do such problems exist?

Facing the quantum challenge

Quantum computers use quantum bits, or qubits, whereas classical computers use binary bits (0 and 1). Qubits are fundamentally different from classical bits as they can have the value 0 or 1, as a classical bit can, or a value that's a combination of 0 and 1, called a *superposition*.

Superposition states allow qubits to carry more information. This capacity for parallelism gives quantum computers their archetypal advantage over classical computers, allowing them to perform a disproportionately greater number of operations.

Qubits also exhibit entanglement, meaning that two qubits can be intrinsically linked regardless of their physical separation. This property allows quantum computers to tackle complex problems that may be out of reach of classical devices.

All this said, the real breakthrough in quantum computing is scalability. In classical computers, the processing power grows linearly with the number of bits. Add 50 bits and the processing power will increase by 50 units. So the more operations you want to perform, the more bits you add.

Quantum computers defy this linearity, however. When you add more qubits to a quantum computer, its computational power for certain tasks grows exponentially as 2^n, where n is the number of qubits. For example, whereas a one-qubit quantum computer can perform $2^1 = 2$ computations, a two-qubit quantum computer can perform $2^2 = 4$ computations, and so forth.

#P-hard problems

Quantum circuits are at the heart of quantum computing. These circuits consist of qubits and quantum gates, analogous to the logic gates of classical computers. For example, an AND gate in a classical setup has output 1 if both its inputs are

0 or 1 – i.e. (0,0) or (1,1). Similarly, a quantum circuit can have qubits and quantum gates wired to combine input values in a certain way.

In such a circuit, a quantum gate could manipulate the qubits to perform specific functions, leading to an output. These outputs can be combined to solve complex mathematical problems.

Classical computers struggle with #P-hard problems – a set of problems that includes estimating the probability that random quantum circuits will yield a certain output.

#P-hard problems are a subset of #P problems, which are all counting problems. To understand what this means, let's consider another set of problems called NP problems. These are decision-making problems, meaning that the output is always either 'yes' or 'no'.

A famous example of an NP problem is the travelling salesman problem. Given a set of cities, is there a route passing through all of them and returning to the first one, without visiting any city twice, whose total distance is less than a certain value? As the number of cities increases, the problem becomes vastly more difficult to solve.

To turn this NP problem into a #P problem, we must count all the different possible routes that are shorter than the specified limit. #P problems are *at least as hard* as NP problems because they require not just a 'yes' or 'no' answer but the number of possible solutions. That is, when the answer is 'no', the count will be zero; but when the answer is 'yes', the count will have to be computed.

If a problem is #P-hard, then it is so challenging that if you can efficiently solve it, you can also efficiently solve every other problem in the #P class by making certain types of transformations.

Taking the Cayley path

To prove that there is a class of problems that can be solved by quantum computers but not by classical computers, Dr. Movassagh used a mathematical construct called the Cayley path.

The Cayley path is like a bridge that helps the travelling salesman move smoothly between two different situations in the study – like one random route and one significantly complicated route. With quantum computers, one situation would be the worst-case scenario, like imagining the most challenging quantum circuit possible. The other would be the average case, a quantum circuit that has been randomly selected from the set of all possible circuits.

This 'bridge' allows us to reframe the most challenging quantum circuit in terms of the average circuit – like seeing how tough it might be to handle the worst traffic jam compared to your regular commute.

Dr. Movassagh showed that estimating the output probability of a random quantum circuit is a #P-hard problem, and has all the characteristics of a problem in this computational complexity class – including overwhelming the ability of a classical computer to solve it.

His paper is also notable because of its error-quantifiable nature. That is, the work dispenses with approximations, and allows independent researchers to explicitly quantify the robustness of his findings.

Quantum complexity theory

As such, Dr. Mossavagh's paper shows that there exists a problem that presents a computational barrier to classical computers but not to quantum computers (assuming a quantum computer can crack a #P-hard problem).

The establishment of quantum supremacy will have a positive impact on several fields: cryptography is expected to be a particularly famous beneficiary, at least once the requisite advances in hardware and materials science have been achieved.

Dr. Movassagh's paper is also an advance in quantum complexity theory. The sets NP, #P, #P-hard, etc. were defined keeping the computational abilities of classical computers in mind. Quantum complexity theory is concerned with limits of complexity defined by quantum computers.

The theory also challenges the extended Church-Turing thesis, which is the idea that classical computers can efficiently simulate any physical process. Dr. Movassagh hopes to continue his work to investigate the hardness of additional quantum tasks and someday disprove the thesis.

Tejasri Gururaj is a freelance science writer and journalist.

Published – September 21, 2023 10:30 am IST