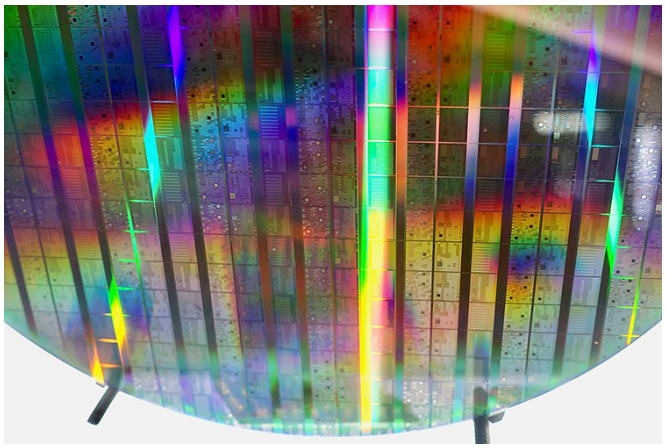
Computer theorists show path to verifying that quantum beats classical

30 October 2018, by Sarah Yang



Close up of an Intel computing wafer. Credit: Steve Jurvetson

As multiple research groups around the world race to build a scalable quantum computer, questions remain about how the achievement of quantum supremacy will be verified.

Quantum supremacy is the term that describes a quantum computer's ability to solve a computational task that would be prohibitively difficult for any classical algorithm. It is considered a critical milestone in quantum computing, but because the very nature of quantum activity defies traditional corroboration, there have been parallel efforts to find a way to prove that quantum supremacy has been achieved.

Researchers at the University of California, Berkeley, have just weighed in by giving a leading practical proposal known as random circuit sampling (RCS) a qualified seal of approval with the weight of complexity theoretic evidence behind it. Random circuit sampling is the technique Google has put forward to prove whether or not it has achieved quantum supremacy with a 72-qubit computer chip called Bristlecone, unveiled earlier this year.

The UC Berkeley computer theorists published their proof of RCS as a verification method in a paper published Monday, Oct. 29, in the journal *Nature Physics*.

"The need for strong evidence for quantum supremacy is under-appreciated, but it's important to pin this down," said study principal investigator Umesh Vazirani, Roger A. Strauch Professor of Electrical Engineering and Computer Science at UC Berkeley. "Besides being a milestone on the way to useful quantum computers, quantum supremacy is a new kind of physics experiment to test quantum mechanics in a new regime. The basic question that must be answered for any such experiment is how confident can we be that the observed behavior is truly quantum and could not have been replicated by classical means. That is what our results address."

The other investigators on this paper are Adam Bouland and Bill Fefferman, both postdoctoral research fellows, and Chinmay Nirkhe, a Ph.D. student, all in Vazirani's theoretical computing research group.

Investment in quantum is heating up

The paper comes amid accelerated activity in government, academia and industry in quantum informational science. Congress is considering the National Quantum Initiative Act, and last month, the U.S. Department of Energy and the National Science Foundation announced nearly $250 million in grants to support research in quantum science and technologies.

At the same time, the Lawrence Berkeley National Laboratory and UC Berkeley announced the formation of Berkeley Quantum, a partnership designed to accelerate and expand innovation in quantum information science.

The stakes are high as international competition in quantum research heats up and the need for increasingly complex computations grows. With true quantum computing, problems that are impractical for even the fastest supercomputers to date could be relatively efficient to solve. It would be a game-changer in cryptography, simulations of molecular and chemical interactions and machine learning.

Quantum computers are not confined by the traditional 0s and 1s of a traditional computer's bits. Instead, quantum bits, or qubits, can encode 0s, 1s and any quantum superposition of the two to create multiple states simultaneously.

When Google unveiled Bristlecone, it said the empirical proof of its quantum supremacy would come through random circuit sampling, a technique in which the device would use random settings to behave like a random quantum circuit. To be convincing, there would also need to be strong evidence that there is no classical algorithm running on a classical computer that could simulate a random quantum circuit, at least in a reasonable amount of time.

Detecting quantum accents

Vazirani's team referred to an analogy between the output of the random quantum circuit and a string of random syllables in English: even if the syllables don't form coherent sentences or words, they will still possess an English "accent" and will be recognizably different from Greek or Sanskrit.

They showed that producing a random output with a "quantum accent" is indeed hard for a classical computer through a technical complexity theoretic construct called "worst-to-average-case reduction."

The next step was to verify that a quantum device was actually speaking with a quantum accent. This relies on the Goldilocks principle—a 50-qubit machine is large enough to be powerful, but small enough to be simulated by a classical supercomputer. If it's possible to verify that a 50-qubit machine speaks with a quantum accent, then that would provide strong evidence that a 100-qubit machine, which would be prohibitively hard to simulate classically, would do so, as well.

But even if a classical supercomputer were programmed to speak with a quantum accent, would it be able to recognize a native speaker? The only way to verify the output of the speaker is by a statistical test, said the Berkeley researchers. Google researchers are proposing to measure the degree of matching by a metric called "cross-entropy difference." A cross-entropy score of 1 would be an ideal match.

The alleged quantum device may be regarded as behaving like an ideal quantum circuit with random noise added. Fefferman and Bouland say the cross-entropy score will certify the authenticity of the quantum accent provided the noise always adds entropy to the output. This is not always the case – for example if the noise process preferentially erases 0s over 1s, it can actually reduce the entropy.

"If Google's random circuits are generated by a process that allows such erasures, then the cross-entropy would not be a valid measure of quantum supremacy," said Bouland. "That's partly why it will be very important for Google to pin down how its device deviates from a real random quantum circuit."

These results are an echo of work that Vazirani did in 1993 with his student Ethan Bernstein, opening the door to quantum algorithms by presenting speedups by quantum computers violating a foundational principle of computer science called the Extended Church-Turing thesis.

Peter Shor of Bell Labs took their work one step further by showing that a very important practical problem, integer factorization, could be exponentially sped up by a quantum computer.

"This sequence provides a template for the race to build working quantum computers," said Vazirani. "Quantum supremacy is an experimental violation of the Extended Church-Turing thesis. Once that is achieved, the next challenge will be to design quantum computers that can solve practically useful problems."

More information: Adam Bouland et al. On the complexity and verification of quantum random circuit sampling, *Nature Physics* (2018). DOI: 10.1038/s41567-018-0318-2

Provided by University of California - Berkeley