Google scientists set the computing world abuzz in October 2019 by announcing its quantum computer had solved a problem in just 200 s that a classical computer would take years—10 000 by Google's estimation—to solve [1]. The achievement, since disputed by scientists at the International Business Machines Corporation (IBM) and downplayed by many experts in the field as too esoteric, signaled proof to Google investigators that quantum computers can achieve "quantum supremacy" and overwhelmingly outperform even the world’s most powerful classical computers on certain tasks. In the future, more robust, powerful versions of quantum computers like Google's, which exploit the properties of matter at subatomic scales to significantly improve processing power, could revolutionize computing, encrypting data, and investigating some of the most mysterious aspects of nature.

"This is certainly an important result, showing at last that a quantum computer can do a specific task in an absolute shorter time than a classical computer," said Daniel Lidar, professor of engineering at the University of Southern California (USC) in Los Angeles, director of the USC Center for Quantum Information Science and Technology, and co-director of the USC-Lockheed Martin Quantum Computing Center. “While the problem Google solved was very specific and not considered particularly useful, I wouldn’t be surprised to see a practically useful quantum computer appear in the next ten years. Quantum simulation, whereby a quantum computer simulates another quantum system or models thereof, appears particularly close and promising.”

While ten years may seem a long way off, the origins of quantum computing date back to 1981, the same year IBM released its first personal computer. In a lecture that year, physicist Richard Feynman made the case that quantum-mechanical phenomena, such as chemical reactions and the flow of electrons through semiconductors, are best simulated with machines based on quantum-mechanical rules [2]. Such computers would harness entanglement, a phenomenon unique to quantum systems whereby two (or more) particles seem to operate in a coordinated manner, even when separated by vast distances. These mysterious links make quantum systems challenging to simulate on classical computers. The expectation is that quantum computers will prove more ideally suited to tackle complex problems like designing better pharmaceuticals and more efficient solar cells.

Also, compared to ordinary computers, quantum computers have the potential to do calculations much, much faster. Standard computers store data and perform computations using bits that are either one or zero. A quantum computer, on the other hand, uses qubits, which can be one and zero at the same time, at least until they are measured, at which time their states become known. Therefore, the total number of states doubles with each added qubit. One qubit is two possible states, two is four possible states, three is eight, and so forth. By the time you get to 100 qubits (hypothetical ones that behave perfectly), every atom on planet Earth would be needed to store the bits describing the state of a quantum computer [3].

Google built its quantum computer by stringing together qubits made of loops of superconducting metal shielded from the noisy non-quantum world in a chamber kept at temperatures just above absolute zero (Fig. 1). Google’s recent breakthrough experiment...
tested whether its quantum computing device, a 54-qubit array named Sycamore (Fig. 2), could correctly verify the results from the quantum version of a random number generator. Sycamore sampled the random quantum circuit one million times in just 200 s. When the team simulated the same quantum circuit on classical computers, it found that even the most powerful in the world, IBM’s Summit supercomputer, would require approximately 10 000 years to perform the same task [1]. “Aside from the blazing speed, another clear win for Google comes in terms of energy consumption,” said Lidar, noting that Sycamore used just a few kilowatts to perform its calculation, while megawatts are required to run Summit.

Some experts in the field have likened Google’s achievement to the Wright brothers’ first plane flight in 1903—conceptual proof of an idea whose practical application is still years away. Other researchers dismissed the milestone because the calculation was so specific it is unlikely to ever be applied to more general computing applications. In addition, rival scientists at IBM published a blog post arguing that the quantum computation could theoretically be run on its Summit supercomputer in less than two and a half days [4].

Though quantum computing is still in its infancy, money has been pouring into the field. Because quantum computing is expected to be particularly adept at factoring large numbers—a critical aspect of many modern data encryption schemes—governments around the world consider it a national security priority. China ($400 million USD) [5], the United States ($1.2 billion USD) [5], and the European Union ($1.1 billion USD) [6] are all spending big. In addition, several competing stalwarts are doing their own quantum research, including Alibaba, Baidu, Google, Hewlett-Packard, Huawei, IBM, and Tencent [7]. Startups are also looking to make a foothold in the industry, with private investors pouring $450 million USD into dozens of companies in 2017 and 2018 [7].

But before quantum computing power can be harnessed to solve practical problems, there is a major obstacle to overcome: Qubits are extremely error prone. Noise in the environment, including mechanical vibrations, temperature variations, or stray electromagnetic fields, weakens the coordination between qubits. This could degrade the machines’ reliability. One potential solution is to add error-correction routines to the system. However, at least five error-correcting qubits are required for every qubit involved in computation [8]. The additional qubits would run up both cost and complexity. Google’s biggest quantum computer has 72 qubits, but between the problems with noise, other sources of inefficiency, and the challenge of combining qubits in a way that they can solve a wide variety of problems, it has been estimated that around one million qubits will be needed for a general-purpose quantum computer [9].

To get around the finicky nature of qubits, some research groups are taking a different approach to the hardware. Microsoft is attempting to use an obscure mathematical theory called topology to create a novel type of qubit that is much more robust than those used in current systems [10]. Startup firm IonQ (College Park, MD, USA) is experimenting with using lasers to read out the quantum state of ytterbium ions trapped in magnetic fields [7]. Another startup, PsiQuantum (Palo Alto, CA, USA), is attempting to make qubits from photons of light guided through tracks laid out in silicon chips [7]. One benefit of this method is that the qubits could be generated in existing semiconductor manufacturing plants. The firm thinks it can build a million-qubit computer in about eight years [7].

Given the expected fragility of individual qubits, Sycamore appears to be a fairly robust system, said Lidar. “More so than solving the random number problem, I was impressed with the extremely high level of calibration and control in Sycamore’s qubits, and the relatively low level of decoherence and noise,” he said. In general, though, the remaining technical hurdles that will need to be overcome concern many experts. In a December 2018 report, the US National Academies of Sciences, Engineering, and Medicine warned that if a practical use for quantum computers fails to emerge soon, investment could dry up [11]. “Nobody wants to miss the boat, but I think at some point there will be very hard re-examination of where the technology stands and what the challenges are,” said Subhash Kak, a professor of engineering at Oklahoma State University in Stillwater, OK, USA, who has published extensively on quantum mechanics and cryptography. Kak thinks no number of error-correcting qubits can solve the noise-related problems. “Personally, I believe that they will never be built for commercial scale,” he said. “Therefore, all that is happening is a massive investment in basic science, which is not necessarily a bad thing.”

Lidar, however, is more optimistic. “Since the mid-nineties, quantum computing has transitioned from essentially a theoretical activity to a rapidly growing hardware-based industry with tens of thousands of active researchers around the world supported by substantial funding,” he said. “For its part, Google has demonstrated a path to a system that is scalable to perhaps a couple hundred qubits without too much more additional engineering innovation. And, at that point, simulating models of quantum systems becomes really interesting.”

Fig. 2. Google’s Sycamore processor has 54 qubits—the fundamental unit for storing and processing data in a quantum computer—arranged in a two-dimensional grid where each qubit is connected to four other qubits. This architecture provides the chip with sufficient connectivity for the qubit states to interact quickly throughout the entire processor, enabling it to significantly outperform even the most powerful classical computer, albeit for a very specific—and not particularly useful—task. Credit: Erik Lucero/Google (CC BY-ND 4.0).

References


