Google announces a new breakthrough for quantum computing

Bryan Dyne
26 October 2019

Researchers at Google AI Quantum have announced a successful experiment in which for the first time a quantum computer has performed a task that ordinary computers based on integrated circuits are incapable of doing in a reasonable amount of time. This technical milestone paves the way for far-reaching advances in physics, chemistry, astronomy, materials science, machine learning and a host of other fields.

The results were produced using Google's quantum computer, dubbed Sycamore. It is the product of a collaboration between 75 scientists led by Frank Arute at Google, NASA, Oak Ridge National Laboratory and more than a dozen other facilities in Germany and the United States. They compared how fast their machine and the world's most powerful supercomputer, Summit, could produce a random number from a specially designed circuit one million times.

The experiment was then repeated multiple times on increasingly complex algorithms until they could show that while a quantum computer generated a result, a classical computer could not. During their final experiment, Sycamore produced its one million random numbers in 200 seconds. Summit was estimated to need 10,000 years to perform the same calculations.

This exponential increase in computing speed is the first documented instance of so-called quantum supremacy. The term was popularized by John Preskill in 2011 to describe the set of problems that are shown to be intractable for even the best modern computers but that should be relatively straightforward for the quantum computers being developed, thus providing a measure to determine if a given quantum computer had in fact surpassed the computational ability of conventional electronics.

Quantum supremacy also defines certain engineering milestones. While quantum computers have always held the promise of being able to do exponentially more processes per second than conventional machines, they have proven exponentially more difficult to build and maintain. It was not at all clear that quantum computers would in practice ever surpass supercomputers. Nonetheless, Google's research indicates that there is at least one case where quantum computers are supreme, and suggests that there are many others.

The end goal, however, is not just to produce random numbers. An off-the-shelf laptop can produce a million random numbers in seconds if the algorithms used to produce them are not purposefully made complicated, as were the test cases for Sycamore and Summit. Rather, quantum computers have in theory the capability of solving in minutes problems that even the best supercomputers would likely not solve in the lifespan of our solar system. Two of these include simulating the motion of atomic and subatomic particles and factoring integers of several hundred digits.

To solve them, one must go beyond familiar binary models of computation which are used in today's personal computers, tablets and phones. These devices store and process information in their memory using distinct physical states, usually some sort of switch being turned off or on, and the data they contain is often described as a sequence of the symbols 0 and 1. One unit of information, a bit, consists of either a 0 or 1 and the number of bits, usually discussed as bytes (where one byte equals eight bits), is the measure of the size of a computer's memory.

This method of storing and retrieving information takes a small but finite amount of time, an amount which is not noticeable for a single calculation yet can grow large very quickly. High-end modern laptops can perform tens of billions of operations per second while the Summit supercomputer is capable of 148 million billion operations per second. And yet, while Summit could multiply two 300-digit numbers almost instantaneously, it would take the supercomputer—using its most advanced algorithms—billions of years to factor the product. A quantum computer is hypothesized to be able to perform the same operation in minutes.

The original rationale for quantum computers was not to factor large numbers, a key part in certain types of encryption, but to directly simulate rather than approximate quantum mechanics. This field of physics, the study of the motion of matter at its smallest scales, is inherently probabilistic. The position and momentum of a particle are not, as in our everyday life, described as a pair of numbers but as two sets of well-defined probabilities. In the early 1980s, Soviet mathematician Yuri Manin and American physicists Paul Benioff and Richard Feynman realized that if a machine could be devised to perform operations using this property of matter, it would be able to calculate the motion of matter exactly as it occurs in nature.

Instead of switches, Manin, Benioff and Feynman proposed to store information in a fundamental particle such as a photon, the basic unit of light. The value of the “qubit” is stored within the inherent rotation of the photon, which is either positive or negative. The difference between a bit and a qubit, and this is key, is that a qubit initially has both the positive and negative values. Only when the photon interacts with some external particle or wave will it fall into a single state, and it will do so following the probabilistic laws of quantum mechanics. This is known as “state superposition.”

In addition to superposition, quantum computing also takes advantage of a second property of fundamental particles known as “entanglement.” It is possible to take two (or more) particles and force them to interact in such a way that even though separated, each particle acts as part of the same system. What results from this is the ability to act on a single entangled particle, which instantaneously acts on all others within the entangled system.

The combination of state superposition and entanglement is what make quantum computers so much more powerful than classical computers. A computer with 266 bits can store or process 266 pieces of information at a time. A quantum computer with 266 qubits can store or process 2^266 (10^80, a one followed by eighty zeros) pieces of information at a time, a number equivalent to the number of atoms in the observable universe.

Yet qubits are incredibly difficult to operate on. The particles that are storing information react with their surroundings, either nearby matter or the so-called vacuum of spacetime, which is not “nothing” but in fact a constant creation and annihilation of particles. This can cause unknown but definite interactions—called quantum decoherence—with one particle which translates to each other particle with which it is entangled, forcing researchers to reset the entire system. Each particle serving as a qubit must be isolated as much as possible from these unwanted connections, typically by physically isolating them and cooling their surroundings to temperatures close absolute zero.

While it is impossible to suppress all quantum decoherence, for that would involve stopping the motion of matter, an impossibility, a great deal of research from groups around the world has gone into eliminating most of the extraneous motion. This effort is what has allowed Arute’s team to successfully align and operate Sycamore, which consists of 53 working qubits, outperforming the world’s most powerful supercomputer, which consists of many trillions of bits.

This technology is expected to herald advances in a variety of fields. Quantum computers, when they are more capable of surpassing supercomputers in all problems, not just one, will be able to more quickly and accurately find exoplanets, determine the properties of new materials, study the outcome of chemical reactions, and produce more advanced forms of artificial intelligence. They are at the same time a striking confirmation of humanity’s ability to understand and master nature.

Quantum computers under capitalism, however, have the capacity for reinforcing oppression. Standard encryption schemes will be broken in minutes or seconds, giving nations or corporations the ability to spy on their rivals and the working class, as well as infiltrate, control and destroy the electronic systems of whole countries. Employees at their workplace can be tracked with even greater efficiency and forced to work longer and harder. Immigrants can be hunted down with facial recognition and other forms of tracking with increased ease. And the algorithms used by Google, Facebook and other tech companies in conjunction with the US military and intelligence agencies will have an unparalleled ability to censor the internet, particularly left-wing, anti-capitalist and socialist publications.

While Google’s Sycamore quantum computer is nowhere near capable of such feats, the social and political consequences of a private company or a capitalist government having control of such a machine must be understood. At the same time, this must galvanize struggle against capitalism and for the establishment of a society where such vast and fundamental advances can be changed from tools of violence and repression to instruments for securing a prosperous and fulfilling life for all people.