Quantum Computing Is Coming, Bit by Qubit

nytimes.com/2019/10/21/science/quantum-computer-physics-qubits.html

By Dennis Overbye

October 21, 2019

YORKTOWN HEIGHTS, N.Y. — A bolt from the maybe-future struck the technology community in late September. A paper by Google computer scientists appeared on a NASA website, claiming that an innovative new machine called a quantum computer had demonstrated "quantum supremacy."

According to the paper, the device, in three minutes, had performed a highly technical and specialized computation that would have taken a regular computer 10,000 years to work out. The achievement, if real, could presage a revolution in how we think, compute, guard our data and interrogate the most subtle aspects of nature.

In an email, John Preskill, a physicist at the California Institute of Technology who coined the term "quantum supremacy," said the Google work was potentially "a truly impressive achievement in experimental physics."

But then the paper disappeared, leaving tech enthusiasts grasping at air.

At the time, Google declined to comment, but many experts suspect that an official announcement, with all the bells and whistles of publicity and proper peer review, is imminent.

And so quantum computing, one of the jazziest and most mysterious concepts in modern science, struggles to come of age.

It's been a century since scientists discovered that, on the most intimate scales, nature operates according to principles that boggle our poor ape brains. Randomness and uncertainty rule, causes are not guaranteed to be linked to effects, and an electron or other subatomic entity can be everywhere or nowhere, a wave or a particle, until someone measures it.

Most of modern technology, from transistors and lasers to the gadgets in our pockets, runs on this quantum weirdness.

Lately technophiles, politicians and journalists have been worrying out loud that China is pulling ahead in the effort to harness said weirdness for industry and power, better spying and better computing. Last year Congress passed, and President Trump signed, the National Quantum Initiative Act, a plan to spend $1.2 billion to boost research into quantum technology and especially quantum computers.

By exploiting the properties of quantum weirdness, these computers could do gazillions of calculations simultaneously, enough to break currently unbreakable codes and to solve hitherto unsolvable mathematical puzzles. Google, IBM, Microsoft and other companies are now designing and building starter versions and even putting them online, where almost anyone can learn to put the quantum realm to work.

Harnessing uncertainty

Ordinary computers store data and perform computations as a series of bits that are either 1 or 0. By contrast, a quantum computer uses qubits, which can be 1 and 0 at the same time, at least until they are measured, at which point their states become defined.

Eight bits make a byte; the active working memory of a typical smartphone might employ something like 2 gigabytes, or two times 8 billion bits. That's a lot of information, but it pales in comparison to the information capacity of only a few dozen qubits.

Because each qubit represents two states at once, the total number of states doubles with each added qubit. One qubit is two possible numbers, two is four possible numbers, three is eight and so forth. It starts slow but gets huge fast.

"Imagine you had 100 perfect qubits," said Dario Gil, the head of IBM's research lab in Yorktown Heights, N.Y., in a recent interview. "You would need to devote every atom of

planet Earth to store bits to describe that state of that quantum computer. By the time you had 280 perfect qubits, you would need every atom in the universe to store all the zeros and ones."

How this is accomplished is an engineer's dream and nightmare. On a recent rainy day, Dr. Gil offered a tour of IBM's quantum operation. The trip started with an actual quantum computer, its innards exposed, on display in the lobby of the Thomas J. Watson Research Center. It looked a bit like a small, inverted Christmas tree: 3 feet high and a foot wide, a series of gold-colored platforms hanging one from another and adorned with chips, wires, mysterious capsules and gleaming, curled silver tubes.

Each quantum computation starts and ends with a string of ones and zeros — classical bits — at the top of this assembly. Those bits are then converted into pulses of microwaves and sent down through wires and pipes to a series of 50 small superconducting devices called "transmons" — the qubits — dangling at the bottom.

The microwave pulses transform the qubits, putting them into a state of uncertainty between one and zero. Subsequent microwave pulses manipulate them, adding or subtracting them from one another or putting pairs of them into a spooky condition called entanglement, in which what happens to one qubit affects measurements of the other.

At the end, the qubits interfere with one another, like waves on an ocean, producing an output string of ones and zeros that is the answer, Dr. Gil said.

All of this happens in a fraction of a second, which is as long as you can keep nature from peeking at the qubits and spoiling things. Moreover, in practice, the qubits must be sheltered from the noisy non-quantum world, so the process transpires inside a dilution refrigerator — a big Thermos bottle — where the temperature of the chips at the bottom is kept at just above absolute zero, colder than outer space.

At the other end of a long curving corridor, sitting alone in its own room, was the real, working thing. Called IBM Q System One, it was encased in a 9-foot-wide cube of black glass and accessible only through 700-pound doors a half-inch thick, the better to seal in the cold and seal out the universe of noise and interference. "Q" is for quantum. Designed by an architectural firm to be as modern, intimidating and opaque as the future itself, this machine is the most beautiful computer its users will probably never see.

While System One went online in January 2019, a set of starter computers called IBM Q Experience has been available online for the last three years; anyone can log on and write and run programs on them. To date, Dr. Gil said, some 130,000 people have used it, running 17 million experiments and publishing some 200 papers. And there were more quantum

devices, behind other doors, operated by scientists trying to learn how to speak nature's exotic subatomic language. "I'm convinced there are more quantum computers working here than the rest of the world combined, in this building," Dr. Gil said.

Quantum supremacy, maybe

Mathematicians are still debating what might be accomplished with all this quantum power when it finally grows up. Ordinary computers are good for solving "easy" problems — questions that can be answered in a reasonable amount of time, like navigating the rings of Saturn or predicting the path of a hurricane.

Then there are "hard" problems, whose solutions are difficult to find but, once identified, are easy to verify. Among them is the factoring of large numbers. Many modern encryption schemes, like the widely used RSA cryptographic algorithm, rely on the inability to factor such numbers in a reasonable amount of time.

In 1994 Peter Shor, then at Bell Labs and now at M.I.T., devised an algorithm that a quantum computer (a still-hypothetical device at the time) could use to factor big numbers and thus break most cybersecurity codes now in common use.

In 2012 Dr. Preskill, the Caltech physicist, invented the term "quantum supremacy" to describe the potential of quantum computers to drastically outperform classical ones.

That is what a Google team has been trying to do with a quantum computer called Sycamore. The calculation they are tackling is highly specialized and technical, designed mostly to show that quantum supremacy is possible.

Success would be an inflection point in the march of human knowledge, a baby step toward a radically different future, like the first Wright Brothers flight. But it's only one step on a long road.

"We need to be very careful about setting expectations," said Bob Sutor, vice president of Q strategy and ecosystem at IBM, which is competing with Google for a different kind of quantum supremacy. "It's easy to overhype this stuff."

Indeed, in a demonstration of just how hazy the quantum future is, and how hotly contested is its ownership, a quartet of scientists from IBM, led by data scientist Edwin Pednault,on Monday challenged Google's claim that the calculation would take 10,000 years on a regular computer. In a paper published on the physics website arXiv, and in a blog entry posted to IBM's research website, they estimated that the task could be accomplished in just two and a half days.

“Because the original meaning of the term ‘quantum supremacy,’ as proposed by John Preskill in 2012, was to describe the point where quantum computers can do things that classical computers can’t, this threshold has not been met,” they wrote in the blog post.

They went on to invite aspiring young scientists who wanted to do quantum computing to log on to one of IBM’s machines: “Go ahead and run your first program on a real quantum computer today.”

Google did not respond to a request for comment.

In conversation, Dr. Gil maintained that the term “quantum supremacy” was misleading and rhetorical overkill: “The reality is, the future of computing will be a hybrid between classical computer of bits, A.I. systems and quantum computing coming together.”

He and his colleagues would rather that we not judge quantum computers by qubits at all. They prefer a new metric, “quantum volume,” which takes into account both the numbers of qubits and the amount of error correction.

Quantum volume is doubling every year, according to IBM, but nobody can say how far this doubling must go before things get interesting.

The ultimate goal of quantum supremacy would be to use qubits to crack encryption codes. But that will take a while. Google’s Sycamore computer has all of 53 qubits to its name, as does a new IBM computer, installed online at the company’s Quantum Computation Center in Poughkeepsie, N.Y. System One, IBM’s black cube from tomorrow, only has 20 qubits.

In contrast, many hundreds of qubits or more may be required to store just one of the huge numbers used in current cryptographic codes. And each of those qubits will need to be protected by many hundreds more, to protect against errors introduced by outside noise and interference.

All told, it could take millions of qubits to break a code using Dr. Shor’s algorithm; patience is required. In the meantime, Dr. Preskill said, “it will be fun to play with them and learn what they can do.”