The Era of Quantum Computing Is Here. Outlook: Cloudy

Quantum computers should soon be able to beat classical computers at certain basic tasks. But before they’re truly powerful, researchers have to overcome a number of fundamental roadblocks.

By Philip Ball

Quantum computers have to deal with the problem of noise, which can quickly derail any calculation.

After decades of heavy slog with no promise of success, quantum computing is suddenly buzzing with almost feverish excitement and activity. Nearly two years ago, IBM made a quantum computer available to the world: the 5-quantum-bit (qubit) resource they now call (a little awkwardly) the IBM Q experience. That seemed more like a toy for researchers than a way of getting any serious number crunching done. But 70,000 users worldwide have registered for it, and the qubit count in this
resource has now quadrupled. In the past few months, IBM and Intel have announced that they have made quantum computers with 50 and 49 qubits, respectively, and Google is thought to have one waiting in the wings. “There is a lot of energy in the community, and the recent progress is immense,” said physicist Jens Eisert of the Free University of Berlin.

There is now talk of impending “quantum supremacy”: the moment when a quantum computer can carry out a task beyond the means of today’s best classical supercomputers. That might sound absurd when you compare the bare numbers: 50 qubits versus the billions of classical bits in your laptop. But the whole point of quantum computing is that a quantum bit counts for much, much more than a classical bit. Fifty qubits has long been considered the approximate number at which quantum computing becomes capable of calculations that would take an unfeasibly long time classically. Midway through 2017, researchers at Google announced that they hoped to have demonstrated quantum supremacy by the end of the year. (When pressed for an update, a spokesperson recently said that “we hope to announce results as soon as we can, but we’re going through all the detailed work to ensure we have a solid result before we announce.”)

It would be tempting to conclude from all this that the basic problems are solved in principle and the path to a future of ubiquitous quantum computing is now just a matter of engineering. But that would be a mistake. The fundamental physics of quantum computing is far from solved and can’t be readily disentangled from its implementation.

Even if we soon pass the quantum supremacy milestone, the next year or two might be the real crunch time for whether quantum computers will revolutionize computing. There’s still everything to play for and no guarantee of reaching the big goal.
IBM’s quantum computing center at the Thomas J. Watson Research Center in Yorktown Heights, New York, holds quantum computers in large cryogenic tanks (far right) that are cooled to a fraction of a degree above absolute zero.

Shut Up and Compute

Both the benefits and the challenges of quantum computing are inherent in the physics that permits it. The basic story has been told many times, though not always with the nuance that quantum mechanics demands. Classical computers encode and manipulate information as strings of binary digits — 1 or 0. Quantum bits do the same, except that they may be placed in a so-called superposition of the states 1 and 0, which means that a measurement of the qubit’s state could elicit the answer 1 or 0 with some well-defined probability.

To perform a computation with many such qubits, they must all be sustained in interdependent superpositions of states — a “quantum-coherent” state, in which the qubits are said to be entangled. That way, a tweak to one qubit may influence all the others. This means that somehow computational operations on qubits count for more than they do for classical bits. The computational resources increase in simple proportion to the number of bits for a classical device, but adding an extra qubit potentially doubles the resources of a quantum computer. This is why the difference between a 5-qubit and a 50-qubit machine is so significant.

Note that I’ve not said — as it often is said — that a quantum computer has an advantage because the availability of superpositions hugely increases the number of states it can encode, relative to classical bits. Nor have I said that entanglement permits many calculations to be carried out in parallel. (Indeed, a strong degree of qubit entanglement isn’t essential.) There’s an element of truth in those descriptions — some of the time — but none captures the essence of quantum computing.
Inside one of IBM’s cryostats wired for a 50-qubit quantum system.
It’s hard to say qualitatively why quantum computing is so powerful precisely because it is hard to specify what quantum mechanics means at all. The equations of quantum theory certainly show that it will work: that, at least for some classes of computation such as factorization or database searches, there is tremendous speedup of the calculation. But how exactly?

Perhaps the safest way to describe quantum computing is to say that quantum mechanics somehow creates a “resource” for computation that is unavailable to classical devices. As quantum theorist Daniel Gottesman of the Perimeter Institute in Waterloo, Canada, put it, “If you have enough quantum mechanics available, in some sense, then you have speedup, and if not, you don’t.”

Some things are clear, though. To carry out a quantum computation, you need to keep all your qubits coherent. And this is very hard. Interactions of a system of quantum-coherent entities with their surrounding environment create channels through which the coherence rapidly “leaks out” in a process called decoherence. Researchers seeking to build quantum computers must stave off decoherence, which they can currently do only for a fraction of a second. That challenge gets ever greater as the number of qubits — and hence the potential to interact with the environment — increases. This is largely why, even though quantum computing was first proposed by Richard Feynman in 1982 and the theory was worked out in the early 1990s, it has taken until now to make devices that can actually perform a meaningful computation.

### Quantum Errors

There’s a second fundamental reason why quantum computing is so difficult. Like just about every other process in nature, it is noisy. Random fluctuations, from heat in the qubits, say, or from fundamentally quantum-mechanical processes, will occasionally flip or randomize the state of a qubit, potentially derailing a calculation. This is a hazard in classical computing too, but it’s not hard to deal with — you just keep two or more backup copies of each bit so that a randomly flipped bit stands out as the odd one out.

Researchers working on quantum computers have created strategies for how to deal with the noise. But these strategies impose a huge debt of computational overhead — all your computing power goes to correcting errors and not to running your algorithms. “Current error rates significantly limit the lengths of computations that can be performed,” said Andrew Childs, the codirector of the Joint Center for Quantum Information and Computer Science at the University of Maryland. “We’ll have to do a lot better if we want to do something interesting.”
Andrew Childs, a quantum theorist at the University of Maryland, cautions that error rates are a fundamental concern for quantum computers.

A lot of research on the fundamentals of quantum computing has been devoted to error correction. Part of the difficulty stems from another of the key properties of quantum systems: Superpositions can only be sustained as long as you don’t measure the qubit’s value. If you make a measurement, the superposition collapses to a definite value: 1 or 0. So how can you find out if a qubit has an error if you don’t know what state it is in?

One ingenious scheme involves looking indirectly, by coupling the qubit to another “ancilla” qubit that doesn’t take part in the calculation but that can be probed without collapsing the state of the main qubit itself. It’s complicated to implement, though. Such solutions mean that, to construct a genuine “logical qubit” on which computation with error correction can be performed, you need many physical qubits.

How many? Quantum theorist Alán Aspuru-Guzik of Harvard University estimates that around 10,000 of today’s physical qubits would be needed to make a single logical qubit — a totally impractical number. If the qubits get much better, he said, this number could come down to a few thousand or even hundreds. Eisert is less pessimistic, saying that on the order of 800 physical qubits might already be enough, but even so he agrees that “the overhead is heavy,” and for the moment we need to find ways of coping with error-prone qubits.

An alternative to correcting errors is avoiding them or canceling out their influence: so-called error mitigation. Researchers at IBM, for example, are developing schemes for figuring out
mathematically how much error is likely to have been incurred in a computation and then extrapolating the output of a computation to the “zero noise” limit.

Some researchers think that the problem of error correction will prove intractable and will prevent quantum computers from achieving the grand goals predicted for them. “The task of creating quantum error-correcting codes is harder than the task of demonstrating quantum supremacy,” said mathematician Gil Kalai of the Hebrew University of Jerusalem in Israel. And he adds that “devices without error correction are computationally very primitive, and primitive-based supremacy is not possible.” In other words, you’ll never do better than classical computers while you’ve still got errors.

Others believe the problem will be cracked eventually. According to Jay Gambetta, a quantum information scientist at IBM’s Thomas J. Watson Research Center, “Our recent experiments at IBM have demonstrated the basic elements of quantum error correction on small devices, paving the way towards larger-scale devices where qubits can reliably store quantum information for a long period of time in the presence of noise.” Even so, he admits that “a universal fault-tolerant quantum computer, which has to use logical qubits, is still a long way off.” Such developments make Childs cautiously optimistic. “I’m sure we’ll see improved experimental demonstrations of [error correction], but I think it will be quite a while before we see it used for a real computation,” he said.

**Living With Errors**

For the time being, quantum computers are going to be error-prone, and the question is how to live with that. At IBM, researchers are talking about “approximate quantum computing” as the way the field will look in the near term: finding ways of accommodating the noise.

This calls for algorithms that tolerate errors, getting the correct result despite them. It’s a bit like working out the outcome of an election regardless of a few wrongly counted ballot papers. “A sufficiently large and high-fidelity quantum computation should have some advantage [over a classical computation] even if it is not fully fault-tolerant,” said Gambetta.
One of the most immediate error-tolerant applications seems likely to be of more value to scientists than to the world at large: to simulate stuff at the atomic level. (This, in fact, was the motivation that led Feynman to propose quantum computing in the first place.) The equations of quantum mechanics prescribe a way to calculate the properties — such as stability and chemical reactivity — of a molecule such as a drug. But they can’t be solved classically without making lots of simplifications.

In contrast, the quantum behavior of electrons and atoms, said Childs, “is relatively close to the native behavior of a quantum computer.” So one could then construct an exact computer model of such a molecule. “Many in the community, including me, believe that quantum chemistry and materials science will be one of the first useful applications of such devices,” said Aspuru-Guzik, who has been at the forefront of efforts to push quantum computing in this direction.

Quantum simulations are proving their worth even on the very small quantum computers available so far. A team of researchers including Aspuru-Guzik has developed an algorithm that they call the variational quantum eigensolver (VQE), which can efficiently find the lowest-energy states of molecules even with noisy qubits. So far it can only handle very small molecules with few electrons, which classical computers can already simulate accurately. But the capabilities are getting better, as Gambetta and coworkers showed last September when they used a 6-qubit device at IBM to calculate the electronic structures of molecules, including lithium hydride and beryllium hydride. The work was “a significant leap forward for the quantum regime,” according to physical chemist
Markus Reiher of the Swiss Federal Institute of Technology in Zurich, Switzerland. “The use of the VQE for the simulation of small molecules is a great example of the possibility of near-term heuristic algorithms,” said Gambetta.

But even for this application, Aspuru-Guzik confesses that logical qubits with error correction will probably be needed before quantum computers truly begin to surpass classical devices. “I would be really excited when error-corrected quantum computing begins to become a reality,” he said.

“If we had more than 200 logical qubits, we could do things in quantum chemistry beyond standard approaches,” Reiher adds. “And if we had about 5,000 such qubits, then the quantum computer would be transformative in this field.”

What’s Your Volume?

Despite the challenges of reaching those goals, the fast growth of quantum computers from 5 to 50 qubits in barely more than a year has raised hopes. But we shouldn’t get too fixated on these numbers, because they tell only part of the story. What matters is not just — or even mainly — how many qubits you have, but how good they are, and how efficient your algorithms are.

Any quantum computation has to be completed before decoherence kicks in and scrambles the qubits. Typically, the groups of qubits assembled so far have decoherence times of a few microseconds. The number of logic operations you can carry out during that fleeting moment depends on how quickly the quantum gates can be switched — if this time is too slow, it really doesn’t matter how many qubits you have at your disposal. The number of gate operations needed for a calculation is called its depth: Low-depth (shallow) algorithms are more feasible than high-depth ones, but the question is whether they can be used to perform useful calculations.

What’s more, not all qubits are equally noisy. In theory it should be possible to make very low-noise qubits from so-called topological electronic states of certain materials, in which the “shape” of the electron states used for encoding binary information confers a kind of protection against random noise. Researchers at Microsoft, most prominently, are seeking such topological states in exotic quantum materials, but there’s no guarantee that they’ll be found or will be controllable.

Researchers at IBM have suggested that the power of a quantum computation on a given device be expressed as a number called the “quantum volume,” which bundles up all the relevant factors: number and connectivity of qubits, depth of algorithm, and other measures of the gate quality, such as noisiness. It’s really this quantum volume that characterizes the power of a quantum computation, and Gambetta said that the best way forward right now is to develop quantum-computational hardware that increases the available quantum volume.

This is one reason why the much vaunted notion of quantum supremacy is more slippery than it seems. The image of a 50-qubit (or so) quantum computer outperforming a state-of-the-art supercomputer sounds alluring, but it leaves a lot of questions hanging. Outperforming for which problem? How do you know the quantum computer has got the right answer if you can’t check it with a tried-and-tested classical device? And how can you be sure that the classical machine wouldn’t do better if you could find the right algorithm?

So quantum supremacy is a concept to handle with care. Some researchers prefer now to talk about “quantum advantage,” which refers to the speedup that quantum devices offer without making definitive claims about what is best. An aversion to the word “supremacy” has also arisen because of the racial and political implications.
Whatever you choose to call it, a demonstration that quantum computers can do things beyond current classical means would be psychologically significant for the field. “Demonstrating an unambiguous quantum advantage will be an important milestone,” said Eisert — it would prove that quantum computers really can extend what is technologically possible.

That might still be more of a symbolic gesture than a transformation in useful computing resources. But such things may matter, because if quantum computing is going to succeed, it won’t be simply by the likes of IBM and Google suddenly offering their classy new machines for sale. Rather, it’ll happen through an interactive and perhaps messy collaboration between developers and users, and the skill set will evolve in the latter only if they have sufficient faith that the effort is worth it. This is why both IBM and Google are keen to make their devices available as soon as they’re ready. As well as a 16-qubit IBM Q experience offered to anyone who registers online, IBM now has a 20-qubit version for corporate clients, including JP Morgan Chase, Daimler, Honda, Samsung and the University of Oxford. Not only will that help clients discover what’s in it for them; it should create a quantum-literate community of programmers who will devise resources and solve problems beyond what any individual company could muster.

“For quantum computing to take traction and blossom, we must enable the world to use and to learn it,” said Gambetta. “This period is for the world of scientists and industry to focus on getting quantum-ready.”

This article was reprinted on Wired.com.