

# Quantum Computer and Quantum Supremacy

CHONG YONUK

KOREA RESEARCH INSTITUTE OF STANDARDS AND SCIENCE



A hundred years after the invention of quantum mechanics, the field is once again the center of discussion, drawing the attention of both scientists and the general public. In particular, this is said to be the dawn of a “second quantum revolution” touched off by the area of quantum information, or the processing and transmission of information through quantum mechanical principles. Whereas last century saw the elaborate development of quantum physics as an academic framework for understanding and explicating nature, the present day has witnessed the beginnings of active quantum mechanical research that makes direct use of quantum mechanics phenomena to enable new things that were not possible before; within that context, such methods have been referred to as “quantum technology.” At the center of all that lies quantum computing.

As a theory, quantum mechanics is quite mathematically sophisticated and beautiful. On one hand, it is simply amazing that the abstract mathematical systems of quantum mechanics are able to explain natural phenomena so perfectly. (After all, there is no obvious reason that the world should have to operate according to these mathematical principles—nor is quantum mechanics even intuitive.) Not only that, but the stories of the scientific greats who abstracted from the observations of natural phenomena to develop such a sophisticated theory are as fascinating as the tales of heroes from Greek and Roman myths. Quantum mechanics can be viewed from several angles, but the key quantum mechanics concepts and phenomena in quantum information include superposition, entanglement, coherence, interference, and measurement. For a more detailed account, you can seek out a quantum information textbook; if there is just

one thing that I would like to add here, it's that it is not enough in quantum technology to simply demonstrate quantization phenomena. Central to the second quantum revolution is the need for quantum states to be controllable while maintaining coherence, and its core consists of research into quantum mechanical entities that are capable of producing or controlling entangled states between distant objects.

The constituent unit of quantum computing is the quantum bit, or “qubit.” A qubit must possess two quantum states, and the aforementioned characteristics must be well represented. The chief approach today involves the use of superconductors and ion traps, with research activities focused on qubits that make use of semiconductor quantum points, point defects in solids (such as diamonds), neutral atoms, and phase states. A qubit alone is not enough for quantum computing—we have to assemble qubits and connect them well, to operate them without error and to read their states effectively. A quantum computer is a system in which a number of qubits have been suitably prepared in their initial state, with their quantum state continuously maintained through operation such as creating superpositions in qubit state (1-qubit gate), creating entanglement between two qubits (2-qubit gate), and measuring an ancilla qubit to identify state (or create a collapse in state) before the qubits' state is finally read through a particular basis to solve a particular problem. If the number of qubits is equal to  $n$ , then there are  $n$  initial states, but one of the advantages of quantum computers is that it is ideally possible to explore an exponentially larger computational space of up to  $2^n$  during the calculation process. But because it is only possible to obtain  $n$  pieces of information through the final reading of  $n$  qubits with a particular substrate, an appropriate quantum algorithm is needed. One of the best examples is the Shor algorithm for prime factorization. Another addendum here is that it is better the more qubits there are, but a large number does not guarantee a better-performing quantum computer. Performance is determined by a number of different conditions—including errors in qubit operation, connectivity among qubits, coherence, and quantum gate speeds—and quantum computer performance is benchmarked with complex metrics that reflect different performance indicators simultaneously.

Google recently published a paper in which it claimed to have achieved “quantum supremacy.” Let's take a moment to have a look what that means. Google's processor (a chip known as “Sycamore”) is a circuit with 53 super-

conducting qubits arranged in a two-dimensional rectangular lattice structure, where each qubit is able to interact (entangle) directly with its four immediately neighboring qubits. The advantage of this system is that it has kept qubit gate errors down to a level far below 1%, even while simultaneously operating and reading 53 qubits. An experiment that involved showing a interference pattern—where the final state of the qubits when each was assigned a random calculation was represented like the speckles when a laser is scattered—concluded that its calculations were beyond the capabilities of even the top supercomputers today (due to limits on memory size). The tomography of fully reading the quantum states of all 53 qubits is also a difficult matter. This particular experiment measured a value known as cross-entropy benchmarking (XEB) fidelity; to explain this value in simple terms, it can be understood, as the authors described, as the “probability of no error occurring in the computation process.” The paper reported values of roughly 0.1–0.2% in 20-step calculations using 53 qubits, with an elapsed time of roughly 200 seconds; in contrast, it was estimated that it would take over 10,000 years to predict the value with the highest-performing supercomputer today (using the algorithms that we currently know of). Since that time will obviously be greatly reduced as existing computer performance and algorithms improve, the Google team presented the data from its qubit experiment online, where anyone can check it with improved calculations in the future. It was also noted that the gap relative to existing computers is poised to only grow larger, since the size of quantum computers increases at a roughly double exponential rate. The experiment's calculation was not actually especially useful—a toy model—but we can see it as a major tipping point, since it demonstrated the performance of something that can only be done by a quantum processor and not an existing computer, even if it is only this one operation. In reality, quantum computing is a long-term research topic, something that will still require a lot more time, and it helps sustain the momentum of research in the field to have continued successes with these kinds of little milestones.

The most important research topic in quantum computing today has to do with quantum error correction. We're now living in what has become known as the “NISQ (Noisy Intermediate-Scale Quantum) era,” which means a time when what's available is quantum computer hardware consisting of roughly 100 qubits, with a fair amount of error. This is a transitional period, with all the quantum computers provided through current cloud services

falling in this category. It's a self-evident fact to anyone who's dealt with quantum systems that it's impossible to completely eliminate error in qubit operations. But by placing an entangled ancilla qubit next to a data qubit and using suitable measurements to read the kind of error that has occurred and perform a unitary calculation in the opposition direction without allowing the data qubit's quantum state to collapse, we can correct for the error without directly measuring the data qubit. This is what is known as quantum error correction. Since the quantum error correction process is also a form of overhead, the error level must be very low, and the error correction needs to be efficient. For quantum computers to be ultimately successful, it will be critical to demonstrate the ability to scale up while overcoming qubit errors through quantum error correction, which is the biggest goal among all quantum computer researchers today. Sycamore, the Google processor that demonstrated quantum supremacy, is considered as having nearly achieved the necessary minimum performance for quantum error correction demonstration.

Personally, I do not care for the term "computer." A quantum computer is no substitute for current computers. In my opinion, a quantum computer is a "machine that operates entirely according to quantum mechanical principles (and can be fully controlled)," and while the functions can be determined in advance at the hardware

level, a good machine is one that can be "programmed" with the functions I want as needed—a machine with large scale and good coherence (a large number of qubits and little error, allowing for the assignment of long operations) that can be put to work to do complex things. The work given to that machine may be computing or simulations or fundamental quantum mechanics research—or, indeed, interesting and useful new things that we haven't yet been able to envision within the current digital paradigm. These days, most of us hear the word "computer" and think of a device on a desk with a monitor, or perhaps a tablet or supercomputer. But the word "computer" originally referred to people who did calculations by hand. (See the book *When Computers Were Human*.) It may be that the quantum machines of the distant future will perform highly useful functions and be known by the name "Quantum Such-and-Such." They may even just be known as "Such-and-Such," since the fact that they operate by quantum mechanics will be so obvious, and they will work in a perfectly quantum mechanical fashion. Perhaps when that day comes, people will joke about it all:

"You know, they used to call these devices 'quantum computers.'"

"Are you serious? That's awesome. 'Computers.' Hilarious."



**Yonuk Chong** was a principal research scientist in Korea Research Institute of Standards and Science, and now a professor at the SKKU Advanced Institute of Nanotechnology. He received BS, MS and PhD degree in physics from Seoul National University. His research interests include superconducting quantum devices, quantum standards, quantum information and quantum computing.