Going beyond Moore's Law with quantum computing

By Man-Hong Yung
Huawei's Chief Quantum Computing Software and Algorithm Scientist

Two of the greatest breakthroughs of the past century were the invention of computers and the discovery of quantum mechanics. Around thirty years ago, these two great ideas collided and quantum information science was born. Quantum computing is a subfield of quantum information science that may well surpass the limitations of classical computing physics, but has also become an unprecedented challenge for scientists and engineers.

The end of Moore's Law is also a beginning

Today, most computers work based on a "classical mechanics" framework where 1 is 1 and 0 is 0. In the past few decades, classical computer chips and computing power have constantly improved, mainly thanks to engineers who have been able to continually shrink the components inside chips. In this process, we can fit in more components and reduce the distance electric signals travels between components, thus boosting the speed of logical operations and reducing energy consumption. This is explained by the well-known Moore's Law, which describes how the density of industrial-produced chips has doubled every 18 months over the past few decades.

However, when Moore's Law was proposed, a time when the law would fail was also predicted – because physical components cannot be reduced in size infinitely. All matter consists of atoms and, at the atomic level, particles behave according to the laws of quantum mechanics rather than classical mechanics. Even defining 1s and 0s becomes a major problem at this level.

The failure of Moore's Law will not mean the end of the road for mankind's constant pursuit of more powerful computing power however. To borrow one of Winston Churchill's famous quotes: "Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning." Moore's Law will lead humanity up to the boundary between the classical and quantum worlds. And after we pass it, quantum computing will open up a new world.

Quantum mechanics enables us to realize the real world is full of counterintuitive physical laws that subvert our perceptions of it. In the quantum realm, many physical states that don't exist in classical physics become possible. For example, particles can exist in a state where they represent 1 and 0 at the same time. The main idea of quantum computing is using quantum mechanics as a framework to develop more powerful quantum computers and redefine our idea of the meaning of computing.

The second quantum revolution

Based on the quantum mechanics framework, we have a deeper understanding of various materials' characteristics, which has led to numerous cutting-edge technological inventions. Some examples include lasers (developed based on our understanding of the quantum properties of light), chips (the quantum properties of electrons), and MRI (the quantum properties of magnets). These technological advances were sparked by the study of the quantum properties of matter and belong to the first quantum revolution.

As our technology has advanced, our ability to adjust and control microscopic systems has increased dramatically. We can now manipulate the behavior of individual atoms and even the current generated by a single electron. These cutting-edge technologies permit us to repeatedly verify

We have a deeper understanding of various materials' characteristics, which has led to numerous cutting-edge technological inventions.

the fundamental characteristics of quantum mechanics, and this is driving the second quantum revolution.

The second quantum revolution is characterized by the development of new technologies based on the intrinsic qualities of quantum mechanics. Examples of this include using the principle of quantum superposition to develop quantum computers, developing quantum precision measurements using quantum entanglement, and developing quantum encryption systems using quantum non-cloning principles. We believe that the second quantum revolution will give rise to technological breakthroughs in many areas.

The potential of quantum computing

In quantum computers, the basic unit for storing and transmitting data is the "qubit" as opposed to the "bit" in classical computers. This is the biggest difference in the way quantum and classical computers work. According to the principle of quantum superposition, a qubit can be in a state of linear superposition of two logical states (0 and 1) at the same time; two qubits can be in a state of linear superposition of four logical states (00, 01, 10, 11) at the same time; and multiple qubits can have an exponential number of states. The main aim of quantum algorithms is to harness these quantum superposition states to speed up computational problem solving.

Published in 1994, the most famous quantum algorithm is Shor's algorithm for factoring large integers, which threatens the encryption system that classical computer networks depend on. Although we’ve yet to develop a general-purpose quantum computer, Shor's algorithm has sparked concern among more than a few network security experts. If an organization or individual were to develop a quantum computer in 50 years, all encrypted information we send through the public sphere – meaning the Internet – today would be cracked as soon as it were intercepted and stored. The possibility of quantum computers has triggered cyber security experts to develop new encryption methods that are capable of countering quantum attacks.

There have been quite a few major breakthroughs in the study of quantum computing in recent years, which has driven the development of quantum computational complexity. At the same time, our experience of using quantum algorithms has also had an impact on classical algorithms. Many new classical algorithms have been inspired by the study of quantum algorithms, which is a reflection of the overall value of quantum algorithm research.

The general belief among researchers is that in the future, quantum computers will be of enormous benefit in the fields of quantum chemical simulation and artificial intelligence (AI). As has been the case with many great inventions in history, once we successfully develop quantum computers, we will discover many more applications that we can’t imagine today.

Multiple routes for quantum computers

A quantum is not in fact an elementary particle like an electron or neutron, and qubits are not a scarce substance. In quantum mechanics, "quantum" refers to how in the macroscopic world the energy of physical systems isn't continuous. In principle therefore two energy levels in any quantum system can act as qubits as long as experimental means for manipulation and readout exist.

At present, systems that are relatively mature in terms of development include: superconducting quantum devices, quantum dots, trapped ions, diamond color centers, nuclear magnetic resonance (NMR) systems, and linear optical systems. Qubits of different physical systems characteristics vary. In the past, different directions of quantum computing hardware research and development used to be carried out separately but at the same time. A technology developed in a physical system might be demonstrated on a different system. But in the future, the development of quantum hardware might involve a mixture of different quantum systems, in which the strengths of some systems compensate for the weaknesses of others, improving overall performance. This will be a major challenge for the advancement of science and technology.

Once we successfully develop quantum computers, we will discover many more applications that we can’t imagine today.

The HiQ cloud service platform includes a quantum computing simulator and a quantum programming framework developed on the simulator.

The era of quantum hegemony

A quantum computer would likely be a powerful computing machine. However, we're unable to prove from a theoretical perspective that quantum computers would be able to "quickly" solve the problems that classical computers can't solve. For example, although the computational complexity of Shor's quantum algorithm is lower than any known classical algorithm, the existence of equivalent or even faster classical algorithms for large number factoring cannot be ruled out. If such a classical algorithm were discovered, it would significantly diminish the influence of Shor's quantum algorithm.

In the past few years, under strong promotion by governments and enterprises, we've seen a steady increase in the number and quality of qubits achieved in the lab. For quantum computing researchers, this is both a surprise and a delight. The problem before us that we need to ponder isn’t the "ideal quantum computer" from textbooks, but the "quasi-quantum computer" – complex computing machines based on the principles of quantum mechanics. Although the logical operation of these quasi-quantum computers hasn’t yet reached the standards of general-purpose quantum computing, their behavior for the most part cannot be effectively simulated by classical computers. In the field of quantum computing, this is generally referred to as "quantum hegemony."

In this era of quantum hegemony, there are a number of things we need to achieve to drive the development of quantum computers, including tailoring quantum operating systems, quantum algorithms, quantum software, and a complex set of systems engineering for quasi-quantum computers.

HiQ quantum cloud service platform

If we're being truthful, there’s still a wide disparity between the computing power of research institutions' quantum equipment and quantum simulators and modern computers. The main strategy of research institutions and commercial companies around the world have for manufacturing quantum computers at the physical level is gradually increasing the number of qubits.

Before we have mature quantum computing hardware systems, we need to carry out quantum software and algorithm research based on quantum computing simulators. Huawei has achieved initial success in this with the HiQ cloud service platform for quantum computing simulators.

Released at HUAWEI CONNECT 2018, the HiQ cloud service platform includes a quantum computing simulator and a quantum programming framework developed on the simulator. Based on Huawei Cloud's powerful computing infrastructure, HiQ is equipped with a distributed architecture and an algorithmic optimizer to overcome challenges of memory capacity and network broadband latency faced by full-amplitude simulators.

HiQ provides a cloud service with full-amplitude simulation and single-amplitude simulation for external customers. The HiQ platform can simulate quantum circuits with 42 qubits for full-amplitude simulations, and 81 qubits for single amplitudes. For low-depth single-amplitude circuits, it can simulate 169 qubits (20 layers) – the solution is the industry's leading cloud service for quantum circuit simulation. Moreover, a quantum error-correction simulator has been integrated for the first time in a cloud service platform. It can perform error-correction simulations of circuits with tens of thousands of qubits, with a performance that’s 5 to 15 times better than similar simulators.

Huawei also showcased its quantum programming framework at HUAWEI CONNECT 2018 for the first time. As well as being compatible with open-source ProjectQ, the framework significantly improves the parallel computational performance of quantum algorithms. It also provides new features such as a user-friendly quantum circuit orchestration Graphical User Interface (GUI), and a Block User Interface (BlockUI), making hybrid classical-quantum programming easier and more intuitive.

Huawei's vision of quantum computing

Years ago we were already calling quantum computing a potentially disruptive future computing technology. If we can achieve exponential acceleration, quantum computers will be able to complete in minutes or seconds computing tasks that would take classical computers tens of thousands of years. Although quantum computing involves complex system engineering and faces many technical challenges in terms of hardware, software, algorithms, and systems, based on the rapid development in quantum computing in recent years, we predict that it will lead to a new revolution in multiple fields including AI, drug development, quantum chemistry, new material design, and complex optimized scheduling.

Huawei continues to monitor the latest developments in quantum computer hardware, and participates in exploratory research where it can contribute its R&D strength to help make the quantum computer a reality as soon as possible.

Quantum computation is a revolutionary technology that’s different from classical computing. Above all, it’s a future-oriented core technology for cloud computing. Quantum algorithms provide a new perspective on AI algorithms, inspiring better classical AI algorithms and offering faster computing capability. The launch of the HiQ cloud service platform marks a key step in research and innovation in quantum computing.

In the future, Huawei will continue to research and invest in the field. Huawei upholds the ideals of openness and cooperation, and so the HiQ quantum computing simulator cloud service will be fully open to the public. Developers, researchers, teachers and students of higher education institutions, will be invited to engage in joint innovation, which will promote academic breakthroughs and accelerate the industrialization of quantum computing.