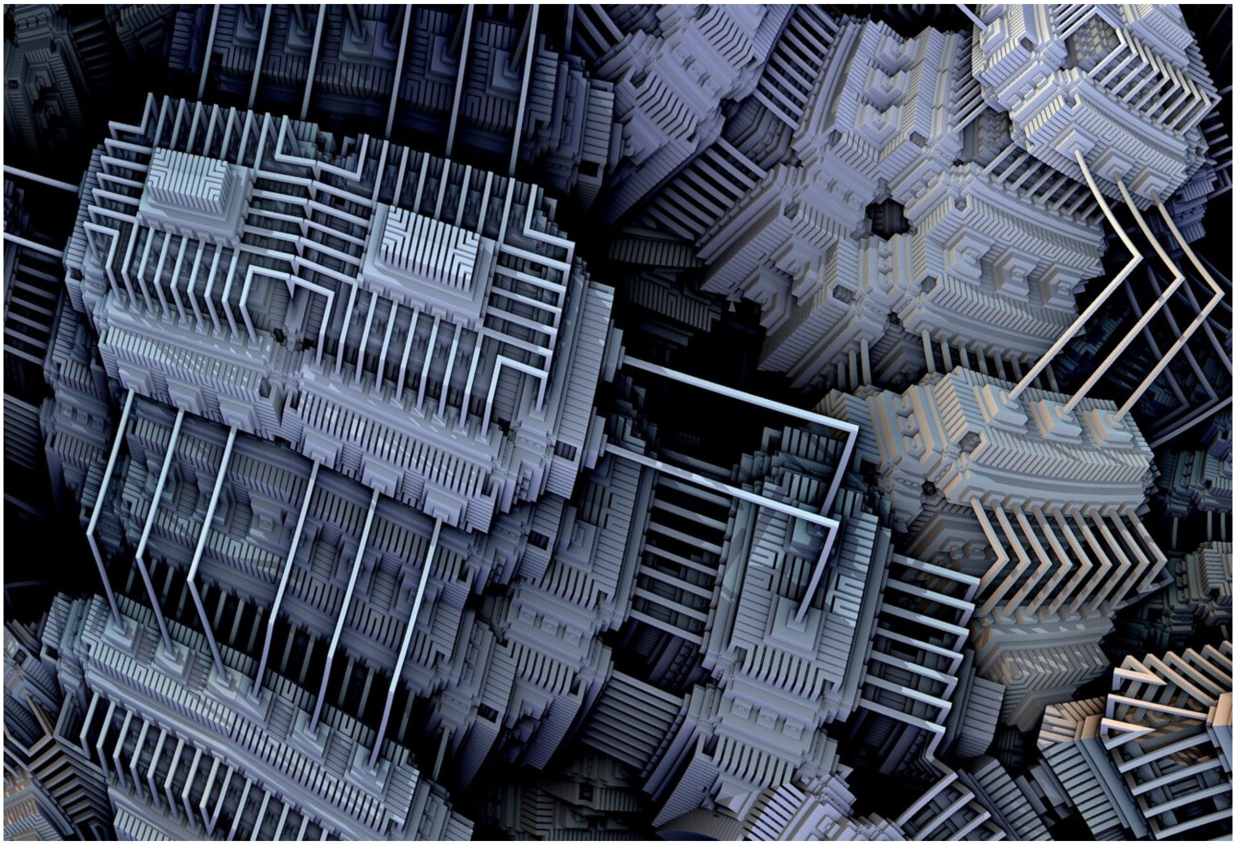
PHYS.ORG

A scientist explains an approaching milestone marking the arrival of quantum computers

November 20 2023, by Daniel Lidar



Credit: Pixabay/CC0 Public Domain

Quantum advantage is the milestone the field of quantum computing is fervently working toward, where a quantum computer can solve problems that are beyond the reach of the most powerful non-quantum, or classical, computers.

Quantum refers to the scale of atoms and molecules where the laws of physics as we experience them break down and a different, counterintuitive set of laws apply. Quantum computers take advantage of these strange behaviors to solve problems.

There are some types of problems that are impractical for classical computers to solve, such as cracking state-of-the-art encryption algorithms. Research in recent decades has shown that quantum computers have the potential to solve some of these problems. If a quantum computer can be built that actually does solve one of these problems, it will have demonstrated quantum advantage.

I am a physicist who studies quantum information processing and the control of quantum systems. I believe that this frontier of scientific and technological innovation not only promises groundbreaking advances in computation but also represents a broader surge in quantum technology, including significant advancements in quantum cryptography and quantum sensing.

The source of quantum computing's power

Central to quantum computing is the quantum bit, or qubit. Unlike classical bits, which can only be in states of 0 or 1, a qubit can be in any state that is some combination of 0 and 1. This state of neither just 1 or just 0 is known as a quantum superposition. With every additional qubit, the number of states that can be represented by the qubits doubles.

This property is often mistaken for the source of the power of quantum computing. Instead, it comes down to an intricate interplay of superposition, interference and entanglement.

Interference involves manipulating qubits so that their states combine constructively during computations to amplify correct solutions and destructively to suppress the wrong answers. Constructive interference is what happens when the peaks of two waves—like sound waves or ocean waves—combine to create a higher peak. Destructive interference is what happens when a wave peak and a wave trough combine and cancel each other out. Quantum algorithms, which are few and difficult to devise, set up a sequence of interference patterns that yield the correct answer to a problem.

Entanglement establishes a uniquely quantum correlation between qubits: The state of one cannot be described independently of the others, no matter how far apart the qubits are. This is what Albert Einstein famously dismissed as "spooky action at a distance." Entanglement's collective behavior, orchestrated through a quantum computer, enables computational speed-ups that are beyond the reach of classical computers.

Applications of quantum computing

Quantum computing has a range of potential uses where it can outperform classical computers. In cryptography, quantum computers pose both an opportunity and a challenge. Most famously, they have the potential to decipher current encryption algorithms, such as the widely used RSA scheme.

One consequence of this is that today's encryption protocols need to be reengineered to be resistant to future quantum attacks. This recognition has led to the burgeoning field of post-quantum cryptography. After a long process, the National Institute of Standards and Technology recently selected four quantum-resistant algorithms and has begun the process of readying them so that organizations around the world can use them in their encryption technology.

In addition, quantum computing can dramatically speed up quantum simulation: the ability to predict the outcome of experiments operating in the quantum realm. Famed physicist Richard Feynman envisioned this possibility more than 40 years ago. Quantum simulation offers the potential for considerable advancements in chemistry and materials science, aiding in areas such as the intricate modeling of molecular structures for drug discovery and enabling the discovery or creation of materials with novel properties.

Another use of quantum information technology is quantum sensing: detecting and measuring physical properties like electromagnetic energy, gravity, pressure and temperature with greater sensitivity and precision than non-quantum instruments. Quantum sensing has myriad applications in fields such as environmental monitoring, geological exploration, medical imaging and surveillance.

Initiatives such as the development of a quantum internet that interconnects quantum computers are crucial steps toward bridging the quantum and classical computing worlds. This network could be secured using quantum cryptographic protocols such as quantum key distribution, which enables ultra-secure communication channels that are protected against computational attacks—including those using quantum computers.

Despite a growing application suite for quantum computing, developing new algorithms that make full use of the quantum advantage—in particular in machine learning—remains a critical area of ongoing research.

Staying coherent and overcoming errors

The quantum computing field faces significant hurdles in hardware and software development. Quantum computers are highly sensitive to any unintentional interactions with their environments. This leads to the phenomenon of decoherence, where qubits rapidly degrade to the 0 or 1 states of classical bits.

Building large-scale quantum computing systems capable of delivering on the promise of quantum speed-ups requires overcoming decoherence. The key is developing effective methods of suppressing and correcting quantum errors, an area my own research is focused on.

In navigating these challenges, numerous quantum hardware and software startups have emerged alongside well-established technology industry players like Google and IBM. This industry interest, combined with significant investment from governments worldwide, underscores a collective recognition of quantum technology's transformative potential. These initiatives foster a rich ecosystem where academia and industry collaborate, accelerating progress in the field.

Quantum advantage coming into view

Quantum computing may one day be as disruptive as the arrival of generative AI. Currently, the development of quantum computing technology is at a crucial juncture. On the one hand, the field has already shown early signs of having achieved a narrowly specialized quantum advantage. Researchers at Google and later a team of researchers in China demonstrated quantum advantage for generating a list of random numbers with certain properties. My research team demonstrated a quantum speed-up for a random number guessing game.

On the other hand, there is a tangible risk of entering a "quantum winter," a period of reduced investment if practical results fail to materialize in the near term.

While the technology industry is working to deliver quantum advantage in products and services in the near term, academic research remains focused on investigating the fundamental principles underpinning this new science and technology. This ongoing basic research, fueled by enthusiastic cadres of new and bright students of the type I encounter almost every day, ensures that the field will continue to progress.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: A scientist explains an approaching milestone marking the arrival of quantum computers (2023, November 20) retrieved 28 April 2024 from https://phys.org/news/2023-11-scientist-approaching-milestone-quantum.html