**The Race to Quantum Supremacy**

Kidus Negesse

The computer is one of the most revolutionary devices ever invented, and it distinctively marks the landscape of the digital era. We use it to work, learn, teach, read, write, speak, share information, access the government, power hospitals, run businesses, automate industry, perform research, make purchases, secure data, watch movies, drive cars, fly planes, and even travel to space. Everything we do is centered around it and completely dependent on it. The computer has become an indispensable facet of modern life.

And yet, they are aging—big time. We have reached the point where the computer industry is approaching physical limits on how small we can make transistors, the billions of switches that provide us with computational power. For that reason, the power of our computers is capped, and while that may not be in issue for browsing internet memes, it is affecting work in cryptography, physical simulations, and other fields with computationally demanding processes. As we inch closer and closer to our limitations, researchers have been working behind the scenes to create quantum computers, which use the special properties of quantum mechanics to process unimaginable streams of information. To realize the importance of these new developments, we will first examine the issues with our current computers, then cover the beautiful theory behind quantum computation, and finally explore some of the most remarkable breakthroughs in this field here at Harvard and around the world.

The Limitations of Classical Computers

Classical computers are the bread and butter of modern technology. They are made up of large electronic circuits that contain switches called transistors that can allow or block the flow of electricity by manipulating electric fields. A bit is a piece of information that tells us whether there is electricity flowing through a transistor, and it is binary, meaning it can have one of two states: 1 when there is electricity, and 0 when there is not.1

We can then combine many transistors into an even larger structure called a logic gate, which checks whether electricity is flowing through its individual transistors. Using that information and a set of rules, it either allows or blocks electricity out of the gate. Those rules are statements of logic, and since basic math operations are based on logic, all the calculations and computation behind our computers are built on top of these logic gates.2

Computing power, the speed with which computer operations are carried out, has grown exponentially during the past few decades as we became able to fit more and more transistors onto chips. In 1971, the Intel 4004 processor had a mere 2300 transistors; in 2016, Intel’s Xeon processor contained 7.2 billion. Gordon Moore, the co-founder of Intel, was so optimistic about this growth that he predicted that the number of transistors in a chip would double every two years. His observation became known as Moore’s Law after it proved to be true throughout the late 20th century. But Moore failed to consider that as we construct smaller and smaller transistors, we start to dive into the bizarre world of quantum mechanics.3

As transistors shrink down to atomic sizes, they begin to face weird quantum effects. In particular, a transistor on the scale of an electron encounters quantum tunneling, a phenomenon where a particle can pass through a barrier that it classically could not penetrate. This is because as we enter the quantum scale, particles become defined by wave functions that describe the probability of finding the particles in particular regions of space. If a barrier is on the same scale as the particle, then the wave function will necessarily show that there is a non-zero probability that the particle might exist in the space beyond the barrier. The terminology of “tunneling” through the barrier then is really a classical metaphor to help us comprehend what is happening—the particle simply has a chance of showing up beyond the barrier (4).

We would not be able to use transistors as binary devices that output 1s and 0s because the probabilistic nature of the location of the electrons would not return definite values for the presence of current. Thus, the physical limit of the size of transistors, our source of computing power, will come to stall the continuation of Moore’s Law. But why not consider the possibility that the very phenomenon that limits us could be used to our advantage?5

The Quantum Computer

Quantum mechanics poses a physical limit to the power of a system built on top of binary bits. But what about non-binary information? The information of particle, such as its position or momentum, is determined by quantum probability functions. Underlying these functions is something called the principle of superposition, which states a particle exists across all of its possible states at the same time, like overlapping waves. Once you measure the system, however, it will collapse into a single state; otherwise, the system exists as a probability distribution across states.6

The bits of information on a computer could also be described by superposition. These theoretical information packets are known as qubits, and unlike binary bits, they can simultaneously be in a state of 1 and 0. This would allow a qubit to contain two pieces of information at the same time! For example, a system of 4 classical bits carries 4 bits of information since each classical bit has 1 value. But because each qubit is in a superposition of 1 and 0, it carries 2 possible bits of information. Thus, with 4 qubits, we would have possible states or 16 bits of information. We can generalize this to say that N qubits will contain bits of information. The power of exponentials is on our side; for example, a system of 20 qubits would be equivalent to the computing power of = 1,048,576 classical bits!6

Similar to how we use the flow of electricity to encode classical bits, we can use properties of quantum systems, like the spin of electrons or the polarization of light, to represent qubits. Then, quantum gates—the equivalent of logic gates for quantum computers—take in incoming qubits and output a result. To get values from the output, however, we have to measure it. What happens again when you measure a quantum system? It collapses into a single state and gives one classical value—it seems as if the incredible magnitude of information held by the qubits simply disappears. Getting around this is quite difficult and requires quantum algorithms that filter the outputs to return useful results. The development of these quantum algorithms is one of the largest areas of research in quantum computing, and we will cover them in more detail later.6

Experts view quantum computers as machines best suited for operations that can take advantage of these superpositions to run many different calculations all at once, a process called parallel computation. The beauty of quantum computation is exactly this—the improvement is not in the speed of each individual operation but rather in the reduction of the total number of operations required.

One quantum algorithm called Shor’s algorithm exhibits this quality from its ability to crack the cryptography system called RSA that is used everywhere today. RSA creates secure keys by multiplying large prime numbers, and in order to crack the keys, you have to figure out what its factors—the prime numbers—are. It would take classical computers longer than the age of the universe to crack these keys; for quantum computers on the order of seconds. For some, this has scary implications, and rightfully so. Quantum computing seems to be lurking beneath our stable layer of security, ready to crack through at any second. But for many researchers, as we will see, this perspective is narrow in vision. To them, something of boundless potential, something unseen and not yet realized, lies in the future of quantum computing.6

Breakthroughs

Harvard physicist Mikhail Lukin is already at the forefront of quantum computing, building a remarkable 51-qubit quantum simulator in the last two years. In a HSR interview with Lukin, he first described that a quantum simulator is a little different from a general quantum computer because it’s a system specially designed to solve a specific set of problems. For Lukin, this specific problem is what’s known as “a many body problem” in quantum mechanics, where the objective is to figure out how a collection of particles interact with each other. To build this machine, his team focused more than 100 laser beams into a cloud “of rubidium atoms so tightly that the laser beams acted as optical tweezers which could each capture exactly one atom.”7

“We take a picture to determine which tweezers are holding atoms and then we rearrange the atoms into a crystal of arbitrary shape,” Lukin said. This arrangement is essentially the input that his team programs into the quantum simulator.

After setting this arrangement into place, “the atoms all start in an identical state and transform into a final state that is determined by interactions in the system.” This is how his simulator computes, and the computation is what Lukin describes as a phase transition, like “water that transforms into ice from a temperature change.” In this case, the phase transition is driven by quantum interactions in the system.

“This transformation finds the lowest energy state,” said Lukin, “and we compare the result of the simulation to what we actually know, which allows us to quantify the accuracy of the machine.”

Essentially, by putting the configuration into place—the input—and allowing it to evolve, they receive a certain energy state—the output—that is the result of their computation. While this specific quantum simulation may not be able to perform universal computational tasks, it provides a way to simulate a physical quantum mechanical system that was previously very hard to do with classical computers. In the words of Alexander Keesling, a Ph.D. student on the project, “the way around that is to actually build the problem with particles that follow the same rules as the system you’re simulating,” which is precisely what Lukin’s team did.8

But why 51 qubits? Lukin explains that it is exactly around 50 atoms where classical computers are not capable of simulating that number of particles interacting with each other.

“What’s exciting about approaching these system sizes is that we are crossing this boundary where quantum machines will outperform classical machines,” he added.

If quantum machines with this number of qubits already have tremendous capabilities, why not just add more qubits? Unfortunately, the quantum world has never been easy with us. Methods of constructing qubits involve trapping little particles and using complex optical equipment, like with Lukin’s project, and they become very hard to scale when you add more qubits. This is due to quantum decoherence, a property of quantum systems that require that they be isolated from outside forces which can collapse the superposition states.9

“You must have a high degree of quantum coherence to process these bits of information in spite of the number of qubits,” said Lukin.

The spotlight in quantum computing, at one point, was centered on Canadian start-up D-Wave Systems, which had introduced a 2000-qubit quantum computer. D-Wave uses a process called quantum annealing that uses magnetic fields to change the energy states of superconducting loops. Similar to Lukin’s quantum simulator, quantum annealing is used to solve specific optimization problems and does not function as a universal quantum computer. Although the number of qubits they boast sounds strikingly impressive, Lukin adds that “their qubits have a very short quantum memory time and decohere very rapidly”—on the order of nanoseconds. Nonetheless, they’ve caught the attention of Google and NASA, who have partnered together to purchase one of D-Wave’s 2000 qubit computers for $15 million for further experimentation.10

Google itself has been ferociously fighting decoherence. They have created qubits out of supercooled aluminum wires hooked up to classical circuits, and their error-correction methods allowed them to construct a 9-qubit quantum chip in 2015. Their current goal is to come out with a 49-qubit machine within the next few months. The tech giant is primarily focused on reaching quantum supremacy, which Lukin described as the time when quantum systems will become accurate and efficient enough to easily solve problems that our best supercomputers cannot in a reasonable time frame. At this point in time, Google has been able to maintain qubits in coherent states on the order of a microsecond. While it sounds small, operations on quantum computers take nanoseconds to complete, so these coherent states currently allow for thousands of operations to run at once.11-15

“Google’s 49-qubit project is interesting work,” Lukin agrees. “But they haven’t yet operated the machine, and even when implemented will be quite hard to compete with our approach in terms of coherence and programmability.”

Competition is flaring, however. IBM, quite possible the oldest player in the game, has been working on quantum computing for decades and came out with a proof-of-work of a 50-qubit quantum computer in November, 2017 that could put them ahead of Google in the current race. They constructed their current system in quite a unique way by supercooling a metal into a state of superconductivity where a current can simultaneously flow in two different directions, representing a superposition of 1 and 0. As of now, they have achieved 9-qubits with this set up and hope that as they scale to 50-qubits, decoherence does not scale out of control.16

Decoherence is not even the biggest problem—designing algorithms for quantum computation has proved to be a major theoretical challenge for researchers like Lukin. Remember that the beauty behind quantum computing is that it drastically reduced the number of operations required to compute something by being able to run many calculations at once. “This is the idea of parallel computing, and that’s where this exponential speed up occurs at ,” Lukin said.7

However, the issue was that taking measurements of quantum systems collapsed the superposition into a single classical state, and the challenge is to make sure that the classical information returned is accurate and useful.

“You want to design a quantum algorithm such that it’s easy to encode the quantum problem in a state or in a system of interactions,” said Lukin. “And then you can efficiently extract some classical information.”

These quantum algorithms that return useful classical results do not follow the same logic as our current ones, like Fourier Transform, RSA, or link analysis.17

“That’s what makes it hard, that’s why you can’t just take conventional algorithms and implement it on a quantum machine,” Lukin explained, because there is no guarantee that they will be accurate and efficient.

Is Lukin’s project a means of developing a universal quantum computer?

“It is on one hand a stepping stone, but it’s also the case that to implement useful and practical algorithms, we might not need a fully universal quantum computer,” he said. “We need it to be programmable to encode a problem into the machine, but it doesn’t necessarily need to be fully universal.”

The Uncertain Future

Quantum computing, as we have seen so far, is experiencing rapid growth, and the desire for the potential power it can provide has spread far beyond the tech industry. According to classified documents revealed by Edward Snowden, the NSA has put $80 million into use to build “a cryptologically useful quantum computer” as part of a project they call “Penetrating Hard Targets.” The controversial government agency fears that people could use powerful quantum computers with methods like Shor’s algorithm to break encryption that secures classified government information and communication.18

“Some people are actually worried that this quantum computer power will be mostly destructive, but in practice this might be just the other way around,” he claimed.

Quantum cryptography can allow one to encrypt information much more securely so that “this encryption is protected by the laws of quantum mechanics, which would be impossible to break.” The NSA thus believes that it is crucial for them to get a head start now and construct quantum computers that can protect their information from attacks in the future. Not much is known about their progress, but their work calls into question the threatening implications quantum computing has on security. Lukin, however, remains optimistic.

“I would venture to guess that way before the time that we have quantum computers that are powerful enough to use Shor’s algorithm, we will be using them to do other things, like optimization problems, which are at the root of tasks like machine learning and artificial intelligence,” Lukin explained.

Google and NASA have already begun research on applying quantum computing to artificial intelligence because much of the challenging work in that field is due to difficult optimization problems that quantum machines can solve. The combined power of these two giants might lead us to a breakthrough in machine learning.19

“Shor’s algorithm is important because it was one of the earliest examples showing the power of quantum computers and it got people sort of talking about it,” Lukin stressed, “but if you think about the classical computer, we also initially had some ideas of what classical computers would be good for.”

When computer engineers built the first programmable computers, like the Colossus, they used them to aid the British military in breaking encrypted German communication and calculating projectile trajectories during WWII. For the purposes of the war, these machines were much more efficient than humans, but after transistors and integrated circuits were developed, computers got smaller and were able to store programs and run software that allowed them to do things never thought of before.20-21

“When they tried to implement the algorithms which motivated building these classical machines, they only performed okay, but other algorithms which were completely unproven worked remarkably well, and I think there are some indications that the same story will be true for quantum computers,” Lukin exclaimed.

The comparison he drew was optimistic, and it put into perspective the potential scale and reach of quantum computing. It has the power to completely restructure data science, it has the power to take us to unimaginable heights in computing efficiency and security, and it has the power to change the planet.

“We don’t realize it yet,” Lukin said. “We just really need to build these machines to figure this out, and that’s what we are going to do.”

**Works cited**

[1] Bits and Bytes. Stanford University. <https://web.stanford.edu/class/cs101/bits-bytes.html> (accessed \_\_\_\_\_\_).

[2] Sangosanya, W. Basic Gates and Functions. University of Surrey, 2005.

<http://www.ee.surrey.ac.uk/Projects/CAL/digital-logic/gatesfunc/> (accessed \_\_\_\_\_\_).

[3] Moore, G.E. *Proceedings of the IEEE.* 1998, *86,* 82-85.

[4] Quantum Tunneling. University of Oregon. <http://abyss.uoregon.edu/~js/glossary/quantum_tunneling.html> (accessed \_\_\_\_\_\_).

[5] Condliffe, J. World’s Smallest Transistor Is Cool but Won’t Save Moore’s Law. *MIT Technology Review*, Oct. 7, 2017. <https://www.technologyreview.com/s/602592/worlds-smallest-transistor-is-cool-but-wont-save-moores-law/> (accessed \_\_\_\_\_\_).

[6] Aaronson, S. The Limits of Quantum. *Scientific American*, Mar. 2008. <http://www.cs.virginia.edu/~robins/The_Limits_of_Quantum_Computers.pdf> (accessed \_\_\_\_\_\_).

[7] Lukin, M. D. *et al. Nature.* 2017, *551*, 579-584.

[8] Reuell, P. Researchers create quantum calculator. *The Harvard Gazette*, Nov. 30, 2017. <https://news.harvard.edu/gazette/story/2017/11/researchers-create-new-type-of-quantum-computer/> (accessed \_\_\_\_\_\_).

[9] Neill, C. et al. ArXiv:1709.06678. 2017.

[10] Gibney, E. D-Wave upgrade: How scientists are using the world’s most controversial quantum computer. *Nature*, Jan. 24, 2017. <https://www.nature.com/news/d-wave-upgrade-how-scientists-are-using-the-world-s-most-controversial-quantum-computer-1.21353> (accessed \_\_\_\_\_\_).

[11] Emerging Technology from the arXiv. Google Reveals Blueprint for Quantum Supremacy. *MIT Technology Review*, Oct. 4, 2017. URL (accessed \_\_\_\_\_\_).

[12] Hsu, J. Google Tests First Error Correction in Quantum Computing. *IEEE SPECTRUM*, Mar. 4, 2015. <https://spectrum.ieee.org/tech-talk/computing/hardware/google-tests-first-error-correction-in-quantum-computing> (accessed \_\_\_\_\_\_).

[13] Nave, K. Quantum computing is poised to transform our lives. Meet the man leading Google's charge. *Wired*, Oct. 31, 2016. <http://www.wired.co.uk/article/googles-head-of-quantum-computing> (accessed \_\_\_\_\_\_).

[14] Russell, J. Quantum Bits: D-Wave and VW; Google Quantum Lab; IBM Expands Access. *HPC Wire*, Mar. 21, 2017. <https://www.hpcwire.com/2017/03/21/quantum-bits-d-wave-vw-google-quantum-lab-ibm-expands-access/> (accessed \_\_\_\_\_\_).

[15] Nicas, J. How Google’s Quantum Computer Could Change the World. *Wall Street Journal*, Oct. 17, 2017. <https://www.technologyreview.com/s/609035/google-reveals-blueprint-for-quantum-supremacy/> (accessed \_\_\_\_\_\_).

[16] Knight, W. IBM Raises the Bar with a 50-Qubit Quantum Computer. *MIT Technology Review*, Nov. 10, 2017. <https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/> (accessed \_\_\_\_\_\_).

[17] Otero, M. The real 10 algorithms that dominate our world. *Medium*, May 26, 2014. <https://medium.com/@_marcos_otero/the-real-10-algorithms-that-dominate-our-world-e95fa9f16c04> (accessed \_\_\_\_\_\_).

[18] Rich, S.; Gellman, B. NSA seeks to build quantum computer that could crack most types of encryption. *Washington Post*, Jan. 2, 2014. <https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html?utm_term=.ac7150def805> (accessed \_\_\_\_\_\_).

[19] Quantum A.I. Google. <https://research.google.com/pubs/QuantumAI.html> (accessed \_\_\_\_\_\_).

[20] History of Computers. University of Rhode Island.

<https://homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.htm> (accessed \_\_\_\_\_\_).

[21] When was the first computer invented? Computer Hope, Jan. 24, 2018.

<https://www.computerhope.com/issues/ch000984.htm> (accessed \_\_\_\_\_\_).