Date
26 Jan 2022

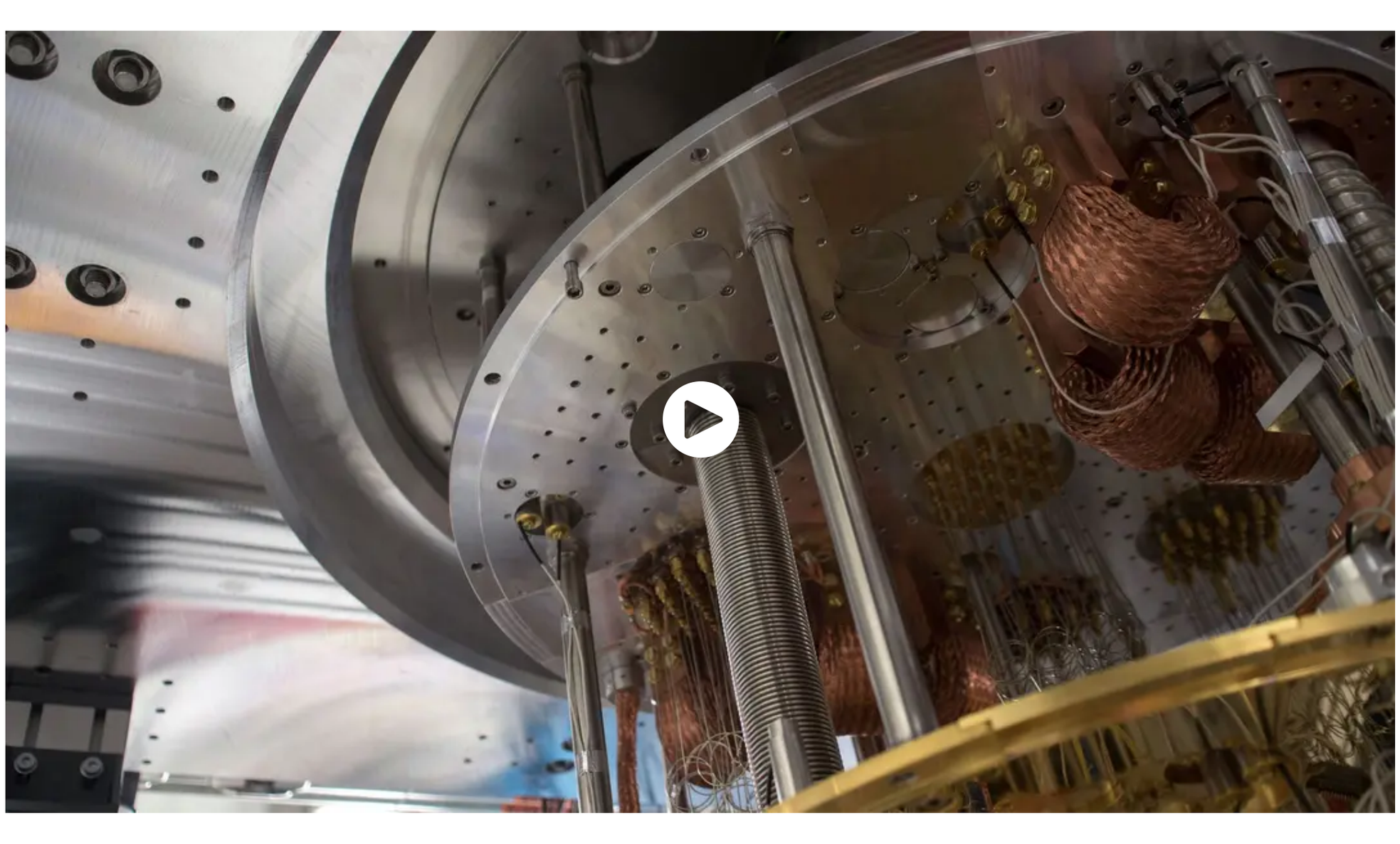
Authors
Robert Davis

Topics
Quantum Research

Explainer   17 minute read

It's been 20 years since "15" was factored on quantum hardware

What are the prime factors of the number 15? That might seem like a simple question, even for a middle school student, but factoring is surprisingly challenging for classical computers.



Classical factoring algorithms are generally quite computationally expensive, especially when it comes to factoring large integers. This simple truth forms the basis of many modern encryption algorithms, which use large numbers and their prime factors to secure data. The inefficiency of classical factoring techniques also drives much of the excitement surrounding quantum computers, which might be able to factor large numbers much more efficiently using Peter Shor's landmark algorithm. Not only does this have potential impact for cryptography, but it could provide exciting advances in fields like machine learning. Twenty years ago, a team of researchers became the first to demonstrate this algorithm on real quantum hardware, changing the field of quantum computing forever.

Last month marked the 20th anniversary of the first published experimental realization of Shor's algorithm, which appeared in the December 2001 issue[1] of *Nature*. That experiment was conducted by researchers at IBM Research-Almaden in San Jose, CA, who used an early kind of quantum computer called a liquid state nuclear magnetic resonance quantum computer to successfully factor the number 15.

Their work was among the first to show that quantum computing was more than just an interesting thought experiment, and that researchers could exercise enough control over quantum systems to execute hundreds of complex operations and generate meaningful results. This helped kick off a boom in quantum hardware development that continues to this day. Now, as we celebrate a major milestone in the history of quantum computing, let's take a look back at this historic achievement and its impact on the broader quantum community.

A Shor bet on quantum computing

Quantum computing pioneer Isaac "Ike" Chuang says that the 2001 factoring experiment was significantly more ambitious than similar efforts that preceded it. "All of the experiments people had been doing with quantum computation until that time were small scale," Chuang said in a recent interview.

Chuang, a former IBM researcher and leader of the 2001 experiment, had previously used NMR techniques to help develop one of the very first functional quantum computers in 1998. However, that system was incapable of solving meaningful problems. By 2001, Chuang and his colleagues were eager to "show off" what they could do using IBM's engineering prowess and ability to perform experiments at scale. Implementing Shor's algorithm would be a formidable test of those capabilities.

"We knew nobody else could do it," Chuang said.

For most classical factoring algorithms, the computational effort that goes into finding the factors of any given integer grows exponentially with the number of digits in the integer itself. This means classical factoring algorithms generally have exponential "time complexity," which is the measure of how long it takes to run an algorithm relative to the length of its input. Exponential time is much slower than the algorithms used for common mathematical operations like addition, multiplication, or calculating square roots, which all have polynomial time complexity.

Some classical algorithms can factor large integers in sub-exponential time, but theorists have yet to find a classical method that can get the job done in polynomial time. Shor's factoring algorithm, however, does just that by leveraging the properties of quantum superposition and interference. First devised in 1994 by mathematician Peter Shor, the algorithm remains one of the most famous in all of quantum computing, and represents one of the starkest examples of theoretical quantum advantage.

> "First devised in 1994 by mathematician Peter Shor, the algorithm remains one of the most famous in all of quantum computing, and represents one of the starkest examples of theoretical quantum advantage. "

That's at least one reason why, when then-PhD student Lieven Vandersypen approached Chuang expressing an interest in leading an experiment, Chuang urged the young researcher to take on the first-ever realization of Shor's algorithm on quantum hardware. "We sat down and I said, 'Look, Lieven. Leaders go off and explore areas that show other people what is possible,'" Chuang said. "'Do you want to charge forth with this?'"

Vandersypen, who would go on to be first author of the experiment and who today serves as director of research at the quantum technology research center QuTech, remembers that moment as well — albeit from a different perspective. "Early on in my PhD, Ike challenged me to aim at doing these experiments," Vandersypen said. "I didn't know too well how hard it would be."

Chuang and Vandersypen set their sights on factoring the number 15, arguably the smallest example of a meaningful factorization problem. They knew they had to start small, since factoring a larger number would have been far beyond the capabilities of the quantum computing technology of the day. At the same time, they also ruled out the integers 1 through 14 since all were either even numbers that are clearly divisible by 2, prime numbers that aren't divisible by anything (other than themselves and 1), or squares that are relatively easy to factor with classical algorithms.

Building a quantum computer in a test tube

To implement Shor's algorithm, Vandersypen would employ the same liquid state nuclear magnetic resonance (NMR) techniques that he and Chuang had used to build one of the very first quantum computers years prior. In terms of their physical structure, liquid state NMR quantum computers have little in common with the computers we use to read emails, or even with the quantum processors IBM develops today.

Imagine a small sample of clear liquid in a test tube. Inside that sample is an ensemble of identical molecules dissolved in a solvent. Each one of those molecules is essentially a tiny quantum computer. To boost the signal they detect, researchers manipulate the entire molecular ensemble when performing quantum computations.

There are several different kinds of molecules that are suitable for different types of quantum computing applications — some synthetic, some naturally available. However, all must meet certain criteria to be of practical use, such as possessing a number of spin-1/2 nuclei that is equal to or greater than the number of qubits needed for a given computation. Having a spin value of 1/2 means that each atom acts like a tiny bar magnet — they can point up or point down. For the factoring 15 experiment, IBM chemists Constantino Yannoni and Gregory Breyta worked with Vandersypen to design and synthesize a special seven-spin molecule — a "perfluorobutadienyl iron complex" — that the research team would use to run Shor's algorithm.

"Our quantum computer had to be built by synthesizing a molecule that never existed before," Chuang said. "It took an organization with many, many different aspects to build this thing together...We had to assemble it from scratch by convincing colleagues in far flung departments to go and do this."

The perfluorobutadienyl iron complex molecule.

Once the IBM team was sure they'd found the right molecule, Vandersypen began the factoring 15 experiment in earnest, working closely with Matthias Steffen, who today is an IBM Fellow, and serves as chief quantum scientist at IBM Quantum. The pair spent months attempting to run Shor's algorithm on their seven-qubit quantum computer.

Steffen recalls the excitement and the sense of discovery that surrounded the project. "We were paving the way for all sorts of new things," Steffen said. "Almost everything was the first, and almost everything was an innovation to try to get it working with these systems."

To control the qubits in a liquid state NMR computer, researchers rely on the magnetic properties of the molecule's spin-1/2 nuclei. The molecules' up and down states serve as a proxy for the logical 0 and 1 states that are fundamental to quantum computing. By placing the molecular sample in an NMR spectrometer — a device that enables the analysis of the magnetic fields surrounding the nuclei — and applying an external magnetic field to the nuclei, researchers can force the nuclei into the state of their choosing. The NMR spectrometer allows them to determine the nuclear spin states. Researchers apply quantum gates by exciting the qubits with radio-frequency (RF) pulses that are tuned to a particular resonance frequency, and they can implement two-qubit gates by leveraging the interaction between nuclei that comes from the natural coupling of neighboring nuclei that share electrons.

Controlling an NMR quantum computer may sound fairly straightforward in theory, but Steffen says that he and Vandersypen found it to be exceedingly challenging in practice. Unlike today's refrigerated quantum systems, which use sub-zero temperatures to keep their qubits in a ground state, the researchers had to run their system at room temperature, meaning they had to use a complicated technique called temporal labeling to get their system to behave as though it was in a ground state. Additionally, the limited ratio of the system's coherence times relative to gate operation times made it hard to fit enough quantum circuits into the system to run the algorithm, and it was difficult to manage the interactions that were happening simultaneously between all the qubit pairs as researchers tried to apply their gates.

"Today, we have much better control given the optimal control techniques that have been invented," Steffen said.

In 2001, however, the researchers had to overcome these hurdles using a combination of less-than-optimal control techniques developed in previous experiments, and other techniques they developed on the fly. Steffen and Vandersypen eventually reached a point where they were able to get the system to generate the answers they were looking for, the factors 3 and 5, but Steffen says the initial results were far from ideal. "We saw a bunch of other signals, and the question was — why were these signals there? Do you at least have a predictive tool that tells you why they're there?"

This led to what Vandersypen says was the final breakthrough that enabled them to complete their experiment. "We were trying to improve the results and were hitting a hard wall," he said. "Then I actually modeled the effects of decoherence in the experiment, and I could show that decoherence was limiting us, rather than the underperforming control techniques."

This was a crucial point, as it meant that their experiment would be the first in NMR quantum computation for which decoherence was the dominant source of errors. Creating this decoherence model was the last step in validating their experimental results, and proving they were ready for publication.

Researchers Lieven Vandersypen (L) and Matthias Steffen (R) in the lab during the 2001 factoring experiment. The large metal cylinder near the center of the image is an 11.7 T Oxford magnet, room temperature bore. The gray rectangular device with a small black screen immediately to Vandersypen's right is a 4-channel Varian spectrometer.

Factoring 15... Twenty years later

The 2001 factoring 15 experiment was neither the largest, nor the longest demonstration of a quantum circuit that had been performed at the time, but it may well have been the most complex. The researchers' seven-spin molecule was one of the largest quantum computers that had ever been built, and with so many interactions between spins, their ability to maintain enough control over the system to run a meaningful instance of a quantum algorithm represented a monumental breakthrough in the field.

The experiment's publication[1] provided the quantum community with essential proof of concept that helped galvanize a new wave of quantum hardware development. Within the next decade, the first commercially available quantum computer would hit the market. Within two decades, the community would see IBM make quantum computing widely accessible via the cloud.

For Chuang, it's clear that quantum computers have advanced a great deal in the 20 years since the 2001 factoring experiment. "You yourself could go and factor 15 on the IBM Quantum computer system over the cloud in 10 minutes," he said. "That is incredible. To have reached that level of sophistication and control is testimony towards the type of system engineering ability that IBM Quantum has brought to us. We did not have that in 2001."

However, it's also important to note that the ability to factor 15 on current quantum hardware assumes some amount of simplification of Shor's algorithm. "There are different ways to write the factor 15 algorithm, and if you simplify it sufficiently, well, then you can run it, but it's not terribly meaningful," Chuang said. "If you write it in a way that can scale such that not only could it factor 15, but also 21 and larger numbers, that is hard, and that's an extremely good test of the sophistication of a system."

Lieven Vandersypen says the factoring experiment had several important implications. "One, quantum computing is not science fiction, the concepts work for real. Two, if you understand your system well enough, you can systematically account for a variety of subtle cross-talk effects and artefacts, and make your qubits 'do the dance' — that is, take them through the steps of a quantum algorithm. Three, we still have a long way to go from toy problems to relevant applications. After all, we knew what the answer would be when we set out to factor the number 15."

Matthias Steffen concurs, and says the factoring 15 experiment made an important impact on the research community, one that can still be felt today. "I think looking back, the impact was really providing proof of concept that a quantum computer can work. If you have quantum bits, if you can make them with good enough coherence times, and if you can exercise enough control over these systems, they will behave as we think they should behave."

For evidence of this enduring impact, Steffen points to the experiment's still-growing citation count. "This particular paper is still getting about 100 citations a year, which is pretty impressive," he said.

Isaac Chuang agrees with Vandersypen and Steffen's assessment of the experiment's impact, and goes even further, noting that the experiment actually directly helped to spur greater investment in the field. "Before this, people thought quantum computing was a scientific curiosity — a mathematical paradigm that was beautiful, but only in principle," he said.

The experiment was a significant step towards putting an end to that idea, and proving that quantum computing was very real. Chuang says this helped drive more funding toward quantum computing research. "A lot more investment poured into the area," he said. "That then triggered another wave of development and now we are where we are, in many ways because of those perceptions that were changed."

Still, the factoring 15 researchers all agree that it's important to remain realistic about how far quantum computing has progressed, and how much further it still has to go. "Quantum computers today are too small and still have too many errors to solve large-scale, business relevant problems," Steffen said. "We need more qubits. We need better qubits. We need to improve our theoretical understanding of quantum error correction and error mitigation. And then we have to run experiments that will tell us what else is still needed."

At the same time, Steffen is optimistic. "If you had told me 10 years ago that I needed to build the equipment and the capabilities that we actually have in our labs today, I probably would have panicked. But at the end of the day, you just have to do what we always do, and solve one problem at a time to get where you need to go."

References

1. Vandersypen, L., Steffen, M., Breyta, G. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* 414, 883–887 (2001). ↩ ↩2