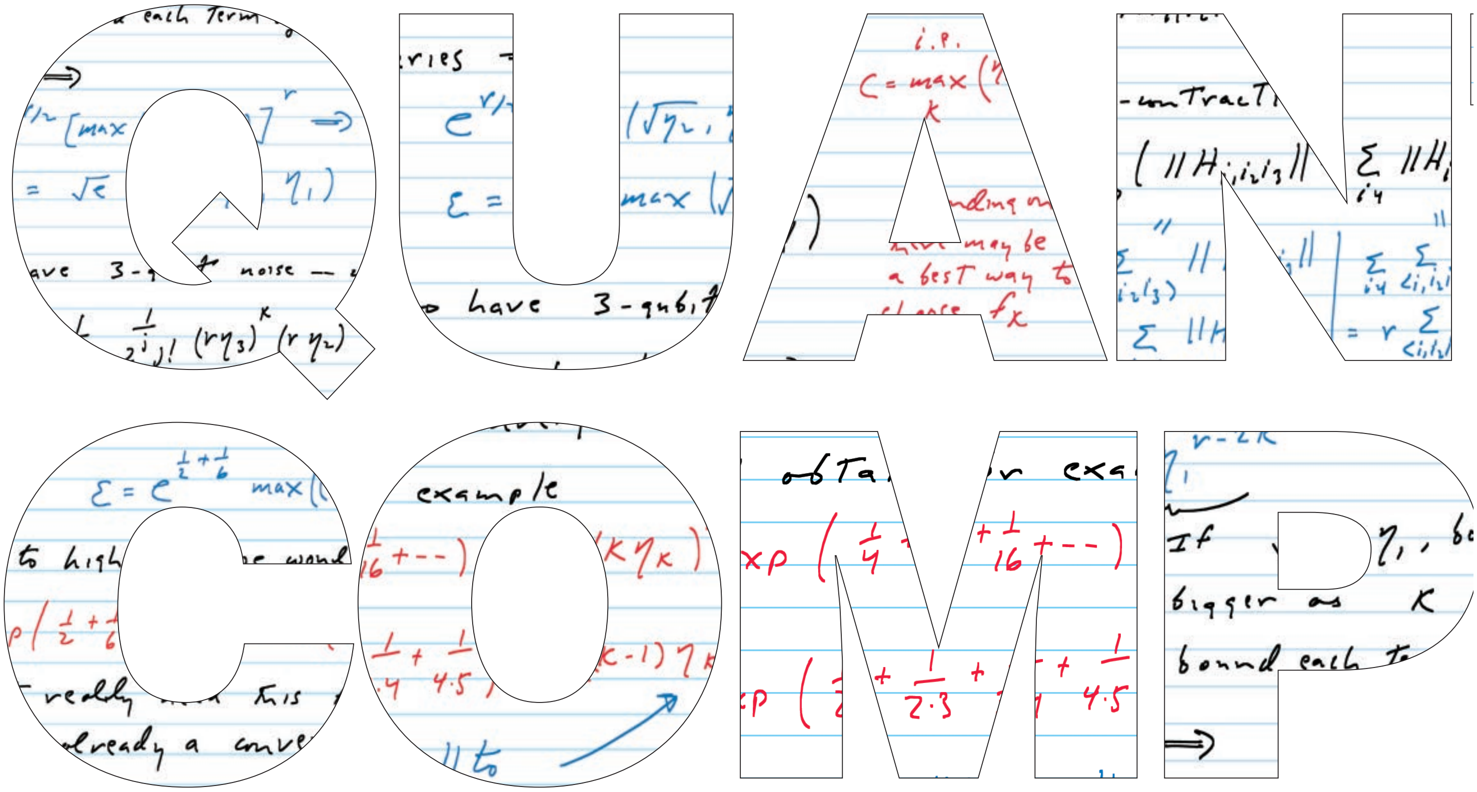
WHAT IS A QUAN COMP



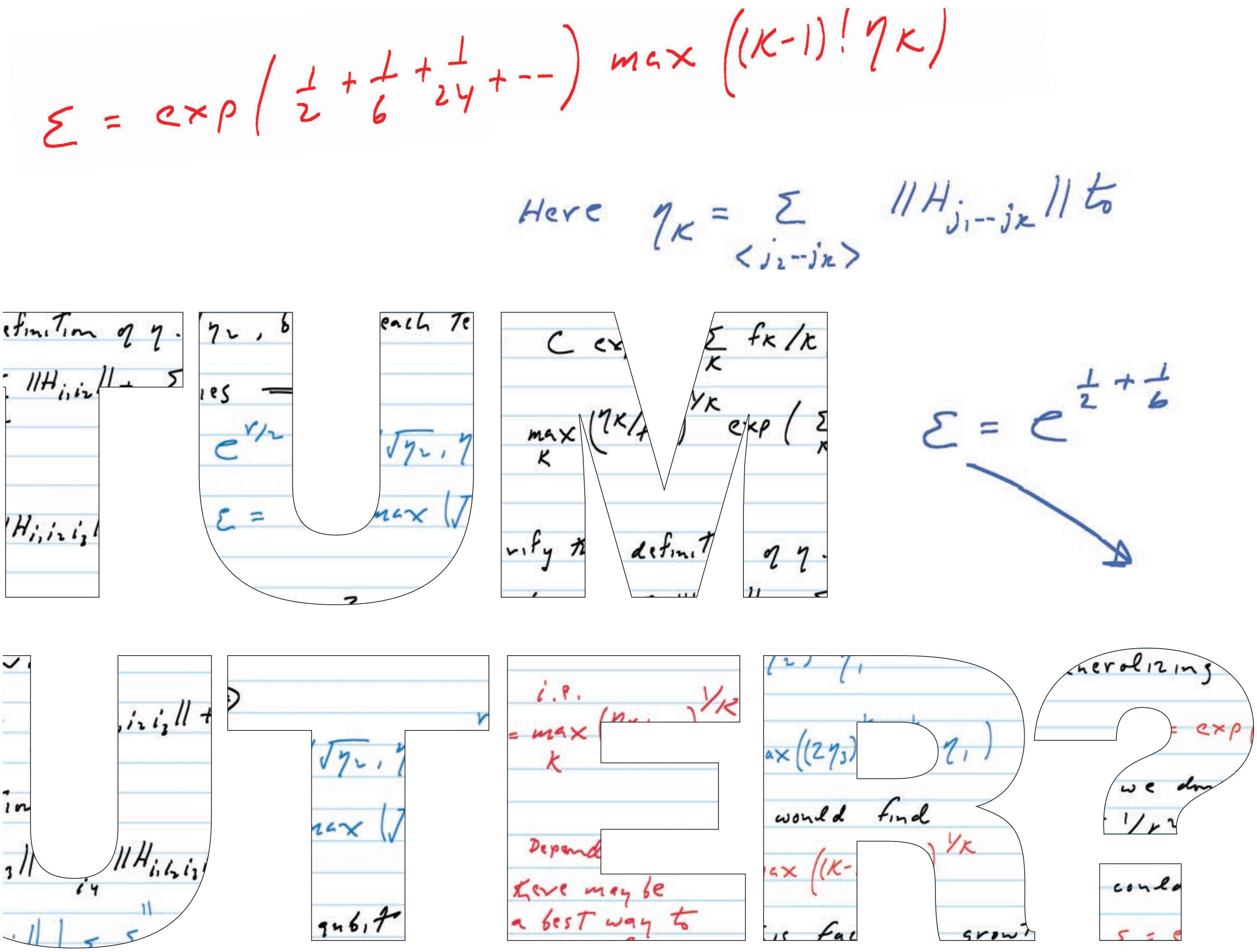
By Marcus Y. Woo

How Caltech physicists are helping to bring us ever closer to our quantum future

The quantum world is bizarre. It's a world where particles are waves and waves are particles, where an electron doesn't have to choose between door number one or door number two but can zip through both *at the same time.*

Still, that weirdness serves a purpose; it has a use. In the last few decades, physicists have come to realize that such scientific eccentricities can be harnessed to create a whole new breed of computers—computers that need only seconds to solve problems that would take thousands of years to crack if fed into a conventional computer. Indeed, quantum computers have been touted as the Next Big Thing: the advance that will usher in a new technological revolution. If you thought the computer age was amazing, experts say, wait until you see the *quantum* computer age.

Thing is, you really are going to have to wait. No one has yet built a truly useful quantum computer, and a lot of the talk about what such machines will be able to do is purely speculative. But it's not all hype. After all, the principles of quantum computing are based on the well-tested laws of quantum mechanics—one of the triumphs of 20th-century physics—which describe the behavior of all things very tiny, a realm unlike anything we encounter in our not-so-tiny everyday lives. Buoyed by their ever-strengthening grasp



ε = exp(1/2 + 1/6 + 1/24 + --) max ((K-1)! η_K)
Here η_K = Σ_{<j_1--j_K>} ||H_{j_1--j_K}|| to
TUM
UTER?
ε = e^{1/2 + 1/6}

of quantum mechanics, physicists, computer scientists, and engineers from around the world are now racing to be the first to make quantum computing a reality. Even industry giants like IBM and Microsoft have joined the fray.

Thanks to all this effort, the field is progressing rapidly—and the world has taken notice. The 2012 Nobel Prize in Physics was awarded for the experimental techniques that have allowed scientists to manipulate light and matter in the quantum world—tools that are essential for building a quantum computer. And, last summer, Caltech physicist Alexei Kitaev won the first Fundamental Physics Prize (and a record-setting $3 million) for his ideas on how to make quantum computers feasible. Today, he and others at Caltech are working to take those ideas to the next level—to envision just how this technology might work—and thus bring us closer to our quantum future.

WHAT'S SO GREAT ABOUT A QUANTUM COMPUTER ANYWAY?

Many credit legendary Caltech physicist Richard Feynman with being among the first to recognize the potential for quantum computers, suggesting in a well-known 1981 talk that such a computer could be a powerful tool with which to simulate the physics of quantum systems—for example, a collection of electrons. Although today's computers are able to simulate and probe, say, simple chemical reactions between individual molecules, deciphering the quantum details of anything more complex would require an inordinate number of variables—more information than a conventional computer could ever handle.

Indeed, it's our current inability to simulate quantum systems that's behind much of the push to develop a quantum computer. Quantum computers should be able to help biologists and chemists not only design a new drug but understand its chemistry in unprecedented detail; they should also be able to help physicists probe the quantum

$k=0\ 2^k k!$

The 7

If

umm

We

secrets of an atom or solve such longstanding mysteries as how high-temperature superconductors work.

But the full potential of quantum computing wasn't apparent until 1994, when theoretical computer scientist Peter Shor (BS '81) developed an algorithm that exploits the laws of quantum mechanics and could be used by a quantum computer to factor enormous numbers that are a thousand digits long. Such a problem would take a regular computer billions of years—literally—to solve.

“That just blew me away,” says Caltech physicist John Preskill, who works on ways to make quantum computers not only feasible but reliable. “Factoring a thousand-digit number is so far beyond what we can do now—it's not going to happen. What Shor said was if you just build a quantum computer, then it's a cinch.”

Physicist Alexei Kitaev (left) talks with physicist John Preskill, whose equations and notes are scattered across these pages.

The ability to factor huge numbers highlights one major potential application of quantum computing: quantum cryptography. Because it's so monumentally difficult to calculate factors of big numbers, such a task is at the heart of the sorts of encryption algorithms used to secure data and communications. Someone with a quantum computer and Shor's algorithm could thus, in principle, crack such codes and hack into the world's computer and communications systems. To protect against future quantum hackers, researchers are developing new quantum encryption methods. And over the last several years they have been fairly successful, according to Leonard Schulman, a theoretical computer scientist at Caltech who works on quantum cryptography and algorithms.

Perhaps more importantly, however, Shor's breakthrough showed that a quantum computer could be a transformative technology, making the impossible possible.

WHAT MAKES A QUANTUM COMPUTER SO POWERFUL?

Like all things quantum, the question of how a quantum computer could be imbued with such unprecedented computational muscle is hard to pin down.

“There have been actual debates on this question at some of the quantum-computing meetings where everybody in the room knows the math perfectly well and knows exactly what they're talking about,” says Schulman. “And still, they manage to argue over the answer.”

Understanding quantum computers requires a basic comprehension of the conventional computers from which they are derived. Today's computers rely on electronic transistors that switch on or off—positions that are represented by a zero (off) or one (on). Each on or off value is called a digital bit (short for binary digit) and is the smallest unit of information on a computer. To compute is to process these bits—to rearrange and connect them in various ways—all of which is done on a silicon chip.

A quantum computer is also based on bits: quantum bits, or qubits (pronounced CUE-bits). Instead of being either a zero or a one, however, a qubit—in true quantum fashion—can be both at the same time. This phenomenon, called superposition, allows quantum computers to work much faster than regular computers.

This peculiar property of being in two states at once is an essential and inseparable feature of quantum computing—so much so that most general descriptions of the field usually end there. Still, superposition isn't the whole story.

In fact, the crux of what truly makes quantum computing powerful remains a bit nebulous. “It's hard to put a finger on it exactly,” Preskill says. “But the closest I

can come to characterizing what makes quantum computing different is that it exploits entanglement."

If you thought superposition was odd, you're going to love entanglement. Quantum entanglement is a phenomenon in which two quantum states—the directions in which two particles can spin, for instance—are inextricably correlated. To simplify: Imagine you have a pair of gloves, and that you put the left-handed glove in one box and the right-handed glove in another. Now imagine you don't know which glove is in which box. By opening one of the boxes, not only will you be able to see which glove is inside that box; you'll also immediately know which glove is in the other box—even without opening it. After all, that box *has to* contain the opposite glove. The "states" (or handedness) of the two gloves are correlated; the information you learn about one gives you information about the other. In quantum mechanical terms, the gloves are entangled.

So, too, can a quantum computer's qubits become entangled with one another. And they don't only pair up one to one; in fact, as you squeeze more qubits into a quantum computer, the correlations between those qubits rise exponentially, becoming so numerous and complex that it's impossible to represent the relationships between them using nonquantum, classical physics.

All of this means simply that, thanks to entanglement, a quantum computer has at its disposal a tremendous amount of complexity and, thus, an ability to store and process information far beyond the reach of a regular computer. This sort of unparalleled complexity is intrinsic to the laws of quantum mechanics, and therefore to nature. "The idea is to exploit this complexity so that nature does the computation for us," Kitaev says.

It's impossible to attribute the power of quantum computing to any single factor. It's not just superposition; it's not just entanglement. Instead, it's the overall weirdness of quantum mechanics—in which both superposition and entanglement play critical roles—that packs such a large amount of complexity and information into qubits, despite the fact they take up only a tiny amount of physical space.

"I can't stress too much how amazing this is," Schulman says. "It doesn't make sense from our classical intuitions."

HOW DO YOU BUILD A QUANTUM COMPUTER?

Qubits. Superposition. Entanglement. It's all very abstract. But a quantum computer would need to be a concrete object, visible and usable. And so, to make the abstract concrete, researchers are trying to figure out the best way to physically represent a qubit, in much the same way a regular bit is embodied in an electronic switch.

They've come up with a myriad of possibilities. Some have built qubits out of charged atoms, whose individual spin states—whether that particular atom is spinning clockwise or counterclockwise—represent the qubit's zero-one or on-off states. The process by which these ions can be trapped in a vacuum by lasers and electromagnetic fields is what won David Wineland his half of this year's physics Nobel. Another idea involves tiny loops of superconducting wires with electrical currents flowing through them. The two directions of the current—whether it flows clockwise or counterclockwise—create the qubit. Yet another proposal is to use the spin states of electrons inside semiconductors as qubits.

Using these ideas as their basis, researchers have been able to build working quantum computers with around a dozen or so qubits—not enough to calculate anything a regular computer can't, but still an impressive feat. Scaling up to a truly powerful version, however, isn't going to be as simple as it might seem.

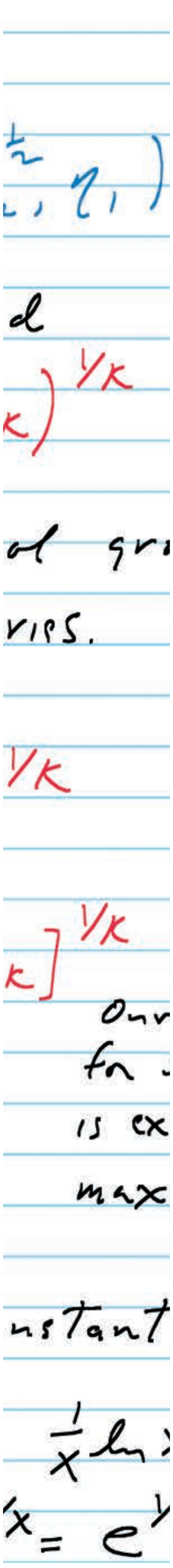
The problem? Quantum systems are exquisitely delicate. If some foreign, stray particle—like an atom or photon—bumps into or otherwise interacts with the qubits, it can change or disturb the quibits' quantum state, ruining whatever calculation the computer might be doing. Since it's impossible to completely shield such a computer from the rest of the universe, these disturbances—and the errors they cause—are inevitable. "If we don't do anything, the errors will accumulate throughout the computation and destroy everything very quickly," Kitaev says.

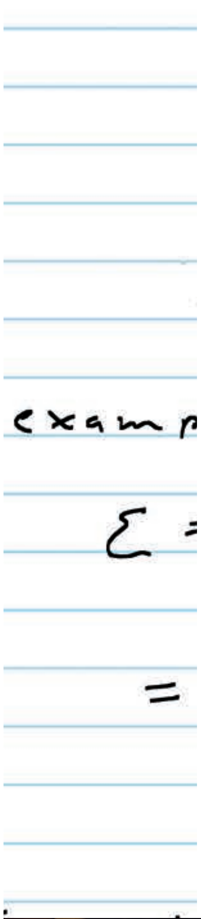
One way to solve this problem is to design algorithms that fix the errors—and indeed, developing this kind of error-correcting code is a major effort in quantum-computing research. But they're not easy to write, says Kitaev. And, besides, wouldn't it be better to just devise a computer that is error-proof—or at least error tolerant—instead?

Kitaev thinks so. Which is why he's worked to come up with a plan for a quantum computer based on an exotic type of particle called an anyon. Unlike electrons or protons—which can exist in isolation—anyons can only exist inside exotic quantum systems, in certain kinds of materials under certain conditions.

As a result of the particle's strange properties, a pair of anyons share a single quantum state—that on-off, zero-one property that is normally the hallmark of a single particle. And since the two anyons share a quantum state, that means the pair can act as a single qubit.

Now, here's the key point: it turns out that an anyon pair can still act as a qubit even if you separate the two quasiparticles. For the qubit to be disturbed—by that stray photon or electron we talked about earlier—the photon or electron would have to interfere with *both* anyons. But if you keep the anyons far enough apart—say,





a micron or so, which is a long, long distance in the quantum world—that stray particle would impact only one of the anyons, meaning that the qubit as a whole would remain safe and error free.

"This is a beautiful, elegant way of doing quantum computing," Preskill says. "It is an illustration of the type of thing we might do to get quantum hardware to work reliably."

While a conventional computer works by turning bits on and off, a quantum computer processes qubits by changing their quantum state. In Kitaev's computer, that change happens by physically moving the anyons around—for example, by making the anyons swap places with one another.

It was for coming up with the concept behind this kind of computer—called a topological quantum computer—that Kitaev won the Fundamental Physics Prize. Indeed, his insights into this type of error prevention essentially created a new field of research when they were first published in 1997.

"It's pretty amazing how ahead of the game he was," says Caltech physicist Jason Alicea. "He really laid the groundwork for what everybody is doing today in this field—including me."

What Alicea—along with Caltech theoretical physicist Gil Refael and their colleagues—has been doing is drawing the theoretical blueprints by which one could turn Kitaev's ideas into a physical computer.

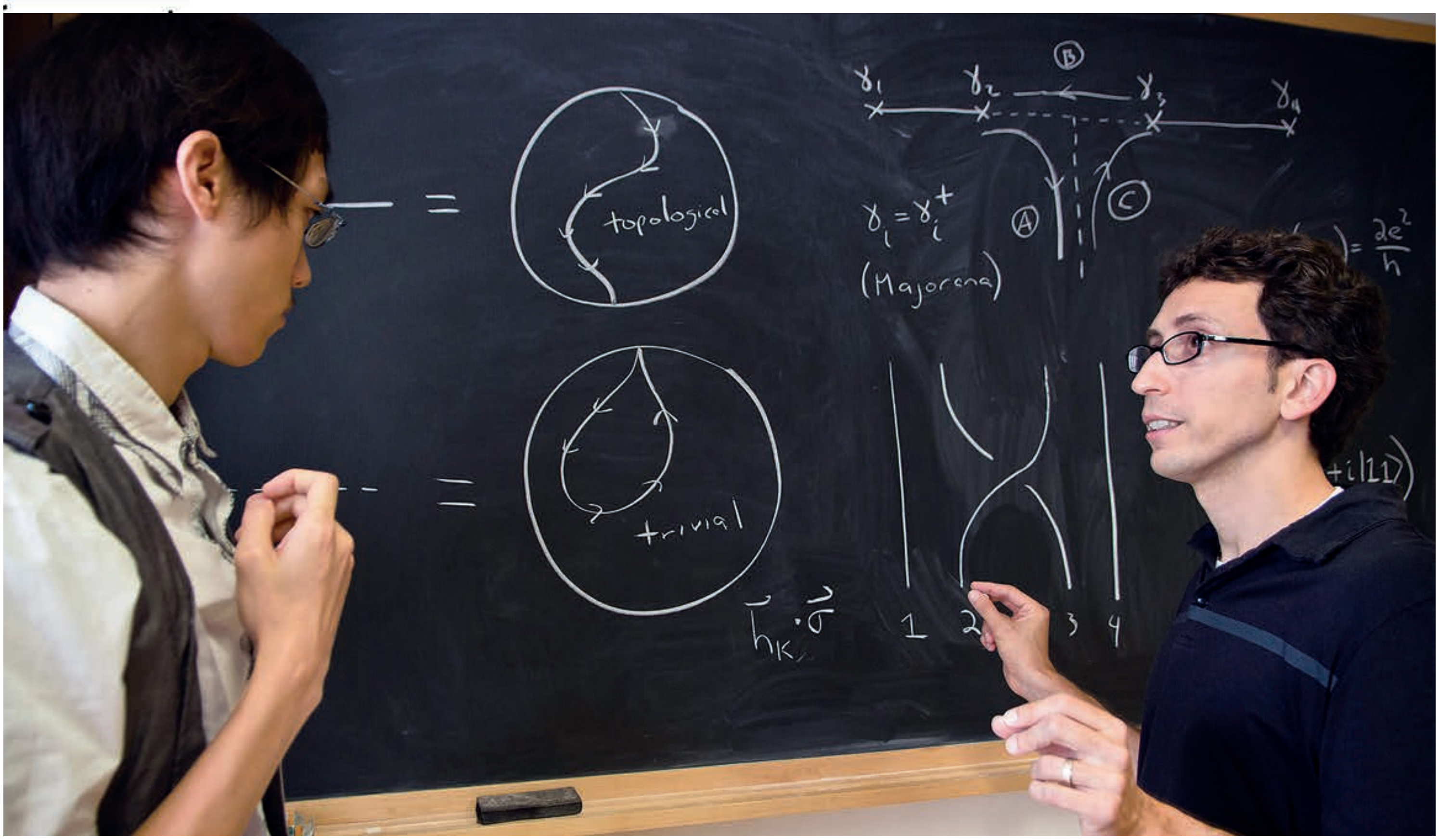
Their proposal starts with a network of quantum wires, each only tens of nanometers thick. The wires are designed so that at each of their two ends is an anyon that traps a hypothesized object called a Majorana mode, which has long been theorized to exist in certain exotic states of matter. Two of these modes can form a qubit.

In keeping with Kitaev's theories, the modes at each end of the quantum wire will be protected against outside disturbances as long as they remain sufficiently separated—in this case, about a micron apart. And just as in Kitaev's original idea—in which the computer processes data by moving the anyons around—the quantum-wire computer processes its qubits by using capacitors to adjust the voltage along the wires, which then moves the modes around.

Quantum wires, says Alicea, could be built out of fairly common superconductors and semiconductors surrounded by a magnetic field. "That's the beauty of it," Alicea says. "These are extremely rudimentary building blocks that one can combine in a way that lets you get something extraordinarily exotic out."

SO WHEN CAN I BUY A QUANTUM COMPUTER?

What we can do and what we have done are two very different things in the field of quantum computing, its practitioners admit. Kitaev's envisaged topological computers may have the most potential for scaling up to a workable machine containing hundreds or even thousands of qubits, but to date



no one has built a single quantum-wire qubit. "We're a long way off—decades, probably—from using these things to actually build hardware in a computer," Alicea admits. "But the research is advancing rapidly. The experimental pace has just been fantastic."

Other types of quantum computers—those based on the spin states of single atoms, for example—may be developed sooner. In fact, primitive quantum computers already exist—such as the handful of photon-based qubits that researchers in the United Kingdom used this past year to factor the number 21 with the help of Shor's algorithm. But while some researchers claim that useful quantum computers will exist within the next decade, most experts think otherwise. "When I started working on quantum computing around 1995, I gave an estimate of 30 years," says Kitaev. "Now I'm more cautious."

To create a true quantum computer—one that can outcompute a conventional computer—however, you'd need at least 50 qubits, says Preskill. But even that—even *double* that—might not be powerful enough to solve the problems that today's machines can't even begin to fathom. In order to factor large numbers, he says, you'd probably need a few thousand qubits. And to implement the necessary error-correcting algorithms if you're not using a topological quantum computer? Well, then the count goes up to a few hundred thousand.

Still, Preskill and his colleagues say, the question isn't if, but when. "Quantum computers will be built in the 21st century," he says. "And the technology will have an impact on society in ways we can't fully anticipate. I think most people who work on quantum computing will agree with that."

A QPHONE ANYONE?

Although quantum computing may indeed lead to a science-fiction future, the truth is that scientists are still in the early stages of even creating the *field* of quantum computing. Their first full-power quantum computers will likely rely on huge cooling systems, and will probably resemble the fledgling electronic computers of the mid-20th century, which weighed a ton and filled entire rooms.

In fact, researchers say, even later and more advanced quantum computers will likely be too large, expensive, and complex to ever replace our desktops and laptops. "It's hard to envision doing your email on a quantum computer," Preskill says. The expectation is that they'll be used for specialized, computationally intensive tasks—just like today's supercomputers. Scientists will likely send their most difficult problems to quantum-computing centers distributed around the world, in the hopes that they can be calculated, simulated, and solved.

But many physicists are excited about quantum computing for an even deeper reason: they hope that it may help them gain insight into nature itself. "Quantum mechanics is kind of preposterous—outlandish may be a better word," Schulman says. Bring quantum computing into the mix, he adds, and you may have a direct test of quantum mechanics, with quantum computing providing the ability to probe how quantum physics gives way to classical physics as you go from the microscopic to the macroscopic.

Of course, no one truly knows what the quantum future will hold. After all, in the early days of mainstream computers, no one had any inkling of how ubiquitous they would one day become. "I think we've just scratched the surface of understanding what quantum computers will be good for," Preskill says. "Maybe we're not being visionary enough. Maybe everyone's going to want to play quantum games. Quantum games might be pretty cool." e&s

Jason Alicea is an associate professor of theoretical physics whose quantum computing work is supported by the Sloan Foundation and the National Science Foundation (NSF).

Alexei Kitaev is a professor of theoretical physics, computer science, and mathematics. In addition to the Fundamental Physics Prize funding, his work is supported by the NSF and the Air Force Office of Scientific Research (AFOSR).

John Preskill is the Richard P. Feynman Professor of Theoretical Physics. His research is funded by the NSF, the AFOSR, the Army Research Office (ARO), and the Intelligence Advanced Research Projects Activity.

Gil Refael is a professor of theoretical physics. His work in the field is funded by the Packard Foundation.

Leonard Schulman is a professor of computer science. His research is supported by the NSF and the ARO.

All of the researchers are members of Caltech's Institute for Quantum Information and Matter, an NSF Physics Frontiers Center with support from the Gordon and Betty Moore Foundation.

Left: Graduate student Shu-Ping Lee (left) and physicist Jason Alicea

Above, right: Theoretical physicist Gil Refael