PHYSICS

Beyond the Quantum Horizon

Once viewed as imposing absolute limits on knowledge and technology, quantum theory is now expanding the power of computers and the vistas of the mind

By David Deutsch and Artur Ekert

LATE IN THE 19TH CENTURY AN UNKNOWN ARTist depicted a traveler who reaches the horizon, where the sky meets the ground. Kneeling in a stylized terrestrial landscape, he pokes his head through the firmament to experience the unknown [*see illustration on page 89*]. The image, known as the Flammarion engraving, illustrates the human quest for knowledge. Two possible interpretations of the visual metaphor correspond to two sharply different conceptions of knowledge.

Either it depicts an *imaginary* barrier that, in reality, science can always pass through, or it shows a *real* barrier that we can penetrate only in our imagination. By the latter reading, the artist is saying that we are imprisoned inside a finite bubble of familiar objects and events. We may expect to understand the world of direct experience, but the infinity outside is inaccessible to exploration and to explanation. Does science continually transcend the familiar and reveal new horizons, or does it show us that our prison is inescapable—teaching us a lesson in bounded knowledge and unbounded humility?

Quantum theory is often given as the ultimate argument for the latter vision. Early on, its theorists developed a tradition of gravely teaching willful irrationality to students: "If you think you understand quantum theory, then you don't." "You're not allowed to ask that question." "The theory is inscrutable and so, therefore, is the world." "Things happen without reason or explanation." So textbooks and popular accounts have typically said.

Yet the developments of the past couple of decades contradict those characterizations. Throughout the history of the field, physicists often assumed that various kinds of constraints from quantum physics would prevent us from fully harnessing nature in the way that classical mechanics had accustomed us to. None of these impediments have ever materialized. On the contrary, quantum mechanics has been liberating. Fundamentally quantum-mechanical attributes of objects, such as superposition, entanglement, discreteness and randomness, have proved not to be limitations but resources. Using them, inventors have fashioned all kinds of miraculous devices, such as lasers and microchips.

These were just the beginning. We will increasingly use quantum phenomena for communications and computation systems that are unfathomably powerful from a classical point of view. We are discovering novel ways of harnessing nature and even of creating knowledge.

BEYOND UNCERTAINTY

IN 1965 INTEL co-founder Gordon Moore predicted that engineers would double the number of transistors on a chip every two years or so. Now known as Moore's Law, this prediction has held true for more than half a century. Yet from the outset, it

Illustration by Goñi Montes

David Deutsch, University of Oxford physicist and inventor of the concept of universal quantum computers, says he got interested in physics as a child when he rebelled at the claim that no one can understand everything that is understood.

Artur Ekert pioneered entanglement-based cryptography as a graduate student. He is now director of the Center for Quantum Technologies in Singapore and a professor at Oxford's Mathematical Institute. He is a keen pilot and diver.

IN BRIEF

Quantum mechanics used to be described as a theory of limits, implying that our observations are unavoidably uncertain, that randomness rules the world, and that the theory itself is too weird to master and forces us to abandon the very idea that there is a world out there that science could describe. **Those misconceptions** are rooted in philosophical doctrines, such as logical positivism, that were popular during the period when physicists developed and honed the theory. **In truth,** quantum mechanics imposes no significant limits. The quantum world has a richness and intricacy that allows new practical technologies and kinds of knowledge.

rang warning bells. If the law continued to hold, you could predict when transistors would reach the size of individual atoms—and then what? Engineers would enter the realm of the unknowable.

In the traditional conception of quantum theory, the uncertainty principle sets a limit that no technological progress could ever overcome: the more we know about some properties, such as a particle's position, the less we can know about others, such as the particle's speed. What cannot be known cannot be controlled. Attempts to manipulate tiny objects meet with rampant randomness, classically impossible correlations, and other breakdowns of cause and effect. An inescapable conclusion followed: the end of progress in information technology was nigh.

Today, however, physicists routinely exert control over the quantum world without any such barrier. We encode information in individual atoms or elementary particles and process it with exquisite precision, despite the uncertainty principle, often creating functionality that is not achievable in any other way. But how?

Let us take a closer look at a basic chunk of information, as traditionally conceived: the bit. To a physicist, a bit is a physical system that can be prepared in one of two different states, representing two logical values: no or yes, false or true, 0 or 1. In digital computers, the presence or absence of a charge on the plates of a capacitor can represent a bit. At the atomic level, one can use two states of an electron in an atom, with 0 represented by the lowest-energy (ground) state and 1 by some higher-energy state.

To manipulate this information, physicists shine pulses of light on the atom. A pulse with the right frequency, duration and amplitude, known as a π-pulse, takes state 0 into state 1, and vice versa. Physicists can adjust the frequency to manipulate two interacting atoms, so that one atom controls what happens to the other. Thus, we have all the ingredients for one- and two-bit logic gates, the building blocks of classical computers, without any impediment from the uncertainty principle.

To understand what makes this feat of miniaturization possible, we have to be clear about what the uncertainty principle does and does not say. At any instant, some of the properties of an atom or other system, called its observables, may be "sharp"—possess only one value at that instant. The uncertainty principle does not rule out sharp observables. It merely states that not all observables in a physical system can be sharp at the same time. In the atom example, the sharp observable is energy: in both the 0 and 1 states, the electron has a perfectly well-defined energy. Other observables, such as position and velocity, are not sharp; the electron is delocalized, and its velocity likewise takes a range of different values simultaneously. If we attempted to store information using position and velocity, we would indeed encounter a quantum limit. The answer is not to throw up our hands in despair but to make a judicious choice of observables to serve as computer bits.

This situation recalls the comedy routine in which a patient tells a doctor, "It hurts when I do this," to which the doctor replies, "Don't do that." If some particle properties are hard to make sharp, there is a simple way around that: do not attempt to store information in those properties. Use some other properties instead.

BEYOND BITS

IF ALL WE WANT TO DO is build a classical computer using atoms rather than transistors as building blocks, then sharp observables are all we need. But quantum mechanics offers much more. It allows us to make powerful use of nonsharp observables, too. The fact that observables can take on multiple values at the same time greatly enriches the possibilities.

For instance, energy is usually a sharp observable, but we can turn it into a nonsharp one. In addition to being in its ground state or its excited state, an electron in an atom can also be in a superposition—both states at once. The electron is still in a perfectly definite state, but instead of being either 0 or 1, it is 0 *and* 1.

Any physical object can do this, but an object in which such states can be reliably prepared, measured and manipulated is called a quantum bit, or qubit. Pulses of light can make the energy of an electron change not only from one sharp value to another but from sharp to nonsharp, and vice versa. Whereas a π-pulse swaps states 0 and 1, a pulse of the same frequency but half the duration or amplitude, known as a $\pi/2$-pulse, sends the electron to a superposition of 0 and 1.

If we attempted to measure the energy of the electron in such a superposition, we would find it was either the energy of the

ground state or the energy of the excited state with equal probability. In that case, we would encounter randomness, just as the naysayers assert. Once again, we can readily sidestep this apparent roadblock—and in doing so create radically new functionality. Instead of measuring the electron in this superposition, we leave it there. For instance, start with an electron in state 0, send in a $\pi/2$-pulse, then send in a second $\pi/2$-pulse. Now measure the electron. It will be in state 1 with a 100 percent probability [*see box on next page*]. The observable is sharp once again.

To see the significance, consider the most basic logic gate in a computer, NOT. Its output is the negation of the input: 0 goes to 1, 1 to 0. Suppose you were given the following assignment: design the square root of NOT—that is, a logic gate that, acting twice in succession on an input, negates it. Using only classical equipment, you would find the assignment impossible. Yet a $\pi/2$-pulse implements this "impossible" logic gate. Two such pulses in succession have exactly the desired effect. Experimental physicists have built this and other classically impossible gates using qubits made of such things as photons, trapped ions, atoms and nuclear spins [see "Quantum Computing with Ions," by Christopher R. Monroe and David J. Wineland; Scientific American, August 2008]. They are the building blocks of a quantum computer.

BEYOND CLASSICAL COMPUTATION

TO SOLVE a particular problem, computers (classical or quantum) follow a precise set of instructions—an algorithm. Computer scientists quantify the efficiency of an algorithm according to how rapidly its running time increases when it is given ever larger inputs to work on. For example, using the algorithm taught in elementary school, one can multiply two n-digit numbers in a time that grows like the number of digits squared, n^2. In contrast, the fastest-known method for the reverse operation—factoring an n-digit integer into prime numbers—takes a time that grows exponentially, roughly as 2^n. That is considered inefficient.

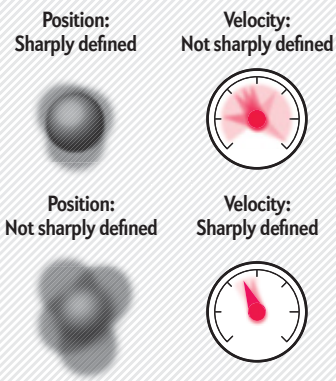
By providing qualitatively new logic gates, quantum mechanics makes new algorithms possible. One of the most impressive examples is for factoring. A quantum algorithm discovered in 1994 by Peter

Supposed Limits to Quantum Computing—and How to Break Them

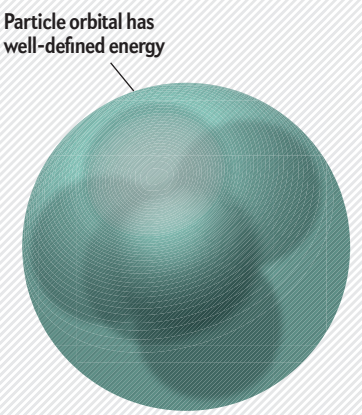
Quantum mechanics is often portrayed as the ultimate obstacle to the miniaturization of electronics. Fortunately, it is no such thing. Physicists have learned to work around the barriers they used to worry about. In fact, it is at the quantum level that computers will reach their true potential, achieving a power far beyond that of ordinary machines.

Uncertainty Principle

PROBLEM: The famous Heisenberg uncertainty principle limits the precision of certain measurements. If you pin down the position of a particle exactly, it will start moving with a range of different velocities simultaneously; if you measure its velocity exactly, you likewise force its position to spread out uncontrollably. Therefore, these properties are unreliable ways to store information.

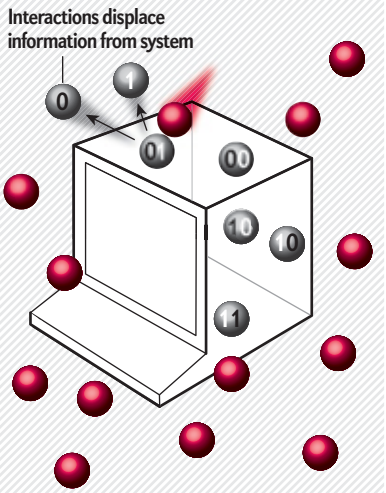


SOLUTION: Not all quantum measurements are subject to this limitation. In situations where position and velocity are uncertain, other properties such as energy may be perfectly well defined. In situations where energy is uncertain, some other variables may be suitable.

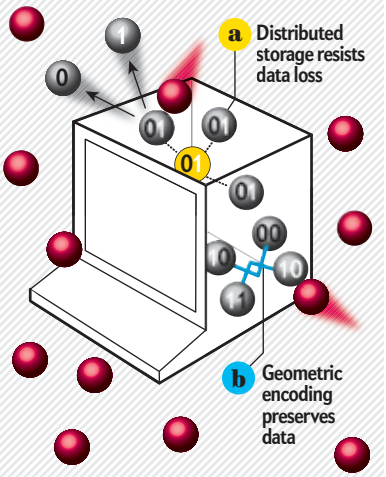


Decoherence

PROBLEM: The particles that make up a computer interact with the surroundings, so that information spreads out, spoiling quantum computations.



SOLUTION: Error-correction procedures can compensate for decoherence long enough to complete a computation. For instance, physicists can spread quantum information over multiple particles **a** or encode it in a geometric form that is naturally resistant to noise **b**.



Illustrations by Jen Christiansen

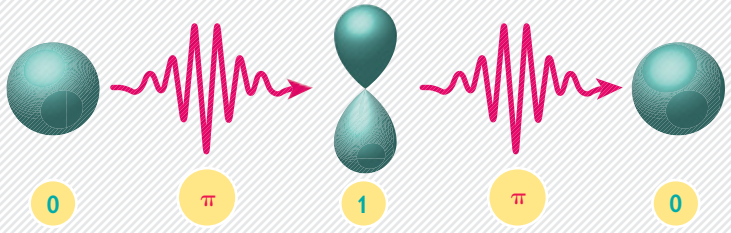
QUANTUM LOGIC

Impossible … NOT!

Quantum computers not only can do anything a classical computer can but also can perform operations outside the scope of classical logic. In this example, two energy states of an electron in an atom represent the 0 and 1 of a computer bit. In both states, the electron has no specific position and velocity: it is spread out over spherical and oval regions called orbitals, and its velocity takes a range of different values simultaneously. Nevertheless, the two states have different energies, and it is the energy that determines the bit value.

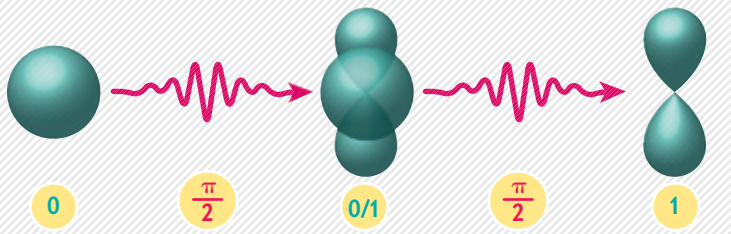
Ordinary NOT

To perform the most basic computational operation, NOT, which inverts the value of a bit, physicists shine pulses of light of appropriate frequency, duration and intensity—known as π-pulses—on the atom. If the electron begins in the 0 state, it will end up in the 1, and vice versa.



Square Root of NOT

The same procedure can be modified to perform a seemingly impossible computational operation: the square root of NOT. A so-called $\pi/2$-pulse, with a lesser amplitude or shorter duration than the π-pulse, sends the electron from the 0 or 1 state into a combination, or superposition, of both states. A second $\pi/2$-pulse then bumps the electron into either the 1 state (if it started as 0) or the 0 state (if it started as 1). This and other new operations give quantum computers their immense power.



Shor, then at Bell Laboratories, can factor n-digit numbers in a series of steps that grows only as n^2. For other problems, such as searching a long list, quantum computers offer less dramatic but nonetheless significant advantages. To be sure, not all quantum algorithms are so efficient; many are no faster than their classical counterparts [see "The Limits of Quantum Computers," by Scott Aaronson; Scientific American, March 2008].

Most likely, the first practical applications of general-purpose quantum computers will not be factorization but the simulation of other quantum systems—a task that takes an exponentially long time with classical computers. Quantum simulations may have a tremendous impact in fields such as the discovery of new drugs and the development of new materials.

Skeptics of the practicality of quantum computing cite the arduous problem of stringing together quantum logic gates. Apart from the technical difficulties of working at single-atom and single-photon scales, the main problem is that of preventing the surrounding environment from spoiling the computation. This process, called decoherence, is often presented as a fundamental limit to quantum computation. It is not. Quantum theory itself provides the means of correcting errors caused by decoherence. If the sources of error satisfy certain assumptions that can plausibly be met by ingenious designers—for instance, that the random errors occur independently on each of the qubits and that the logic gates are sufficiently accurate—then quantum computers can be made fault-tolerant. They can operate reliably for arbitrarily long durations.

BEYOND CONVENTIONAL MATHEMATICAL KNOWLEDGE

THE STORY of the "impossible" logic gates illustrates a startling fact about the physics of computation. When we improve our knowledge about physical reality, we sometimes improve our knowledge of the abstract realms of logic and mathematics, too. Quantum mechanics will transform these realms as surely as it already has transformed physics and engineering.

The reason is that although mathematical *truths* are independent of physics, we acquire *knowledge* of them through physical processes, and which ones we can know depends on what the laws of physics are. A mathematical proof is a sequence of logical operations. So what is provable and not provable depends on what logical operations (such as NOT) the laws of physics allow us to implement. These operations must be so simple, physically, that we know, without further proof, what it means to perform them, and that judgment is rooted in our knowledge of the physical world. By expanding our repertoire of such elementary computations to include ones such as the square root of NOT, quantum physics will allow mathematicians to poke their heads through a barrier previously assumed to exist in the world of pure abstractions. They will be able to see, and to prove, truths there that would otherwise remain hidden forever.

For example, suppose the answer to some unsolved mathematical puzzle depends on knowing the factors of some particular enormous integer N—so enormous that even if all the matter in the universe were made into classical computers that then ran for the age of the universe, they would still not be able to factor it. A quantum computer could do so quickly. When mathematicians publish the solution, they will have to state the factors at the outset, as if pulled out of a magician's hat: "Here are two integers whose product is N." No

amount of paper could ever suffice to detail how they had obtained those factors.

In this way, a quantum computer would supply the essential key that solves the mathematical puzzle. Without that key, which no classical process could realistically provide, the result would never be known. Some mathematicians already consider their subject an empirical science, obtaining its results not only by careful reasoning but also by experiments [see "The Death of Proof," by John Horgan; Scientific American, October 1993]. Quantum physics takes that approach to a new level and makes it compulsory.

BEYOND BAD PHILOSOPHY

IF QUANTUM MECHANICS allows new kinds of computation, why did physicists ever worry that the theory would limit scientific progress? The answer goes back to the formative days of the theory.

Erwin Schrödinger, who discovered quantum theory's defining equation, once warned a lecture audience that what he was about to say might be considered insane. He went on to explain that when his famous equation describes different histories of a particle, those are "not alternatives but all really happen simultaneously." Eminent scientists going off the rails is not unknown, but this 1933 Nobelist was merely making what should have been a modest claim: that the equation for which he had been awarded the prize was a true description of the facts. Schrödinger felt the need to be defensive not because he had interpreted his equation irrationally but precisely because he had not.

How could such an apparently innocuous claim ever have been considered outlandish? It was because the majority of physicists had succumbed to bad philosophy: philosophical doctrines that actively hindered the acquisition of other knowledge. Philosophy and fundamental physics are so closely connected—despite numerous claims to the contrary from both fields—that when the philosophical mainstream took a steep nosedive during the first decades of the 20th century, it dragged parts of physics down with it.

The culprits were doctrines such as logical positivism ("If it's not verifiable by experiment, it's meaningless"), instrumentalism ("If the predictions work, why worry about what brings them about?") and philosophical relativism ("Statements can't be objectively true or false, only legitimized or delegitimized by a particular culture"). The damage was done by what they had in common: denial of realism, the commonsense philosophical position that the physical world exists and that the methods of science can glean knowledge about it.

It was in that philosophical atmosphere that physicist Niels Bohr developed an influential interpretation of quantum theory that denied the possibility of speaking of phenomena as existing objectively. One was not permitted to ask what values physical variables had while not being observed (such as halfway through a quantum computation). Physicists who, by the nature of their calling, could not help wanting to ask, tried not to. Most of them went on to train their students not to. The most advanced theory in the most fundamental of the sciences was deemed to be stridently contradicting the very existence of truth, explanation and physical reality.

Not every philosopher abandoned realism. Bertrand Russell and Karl Popper were notable exceptions. Not every physicist did, either. Albert Einstein and David Bohm bucked the trend, and Hugh Everett proposed that physical quantities really do take on more than one value at once (the view we ourselves endorse). On the whole, however, philosophers were uninterested in reality, and although physicists went on using quantum theory to study other areas of physics, research on the nature of quantum processes themselves lost its way.

Things have been gradually improving for a couple of decades, and it has been physics that is dragging philosophy back on track. People want to understand reality, no matter how loudly they may deny that. We are finally sailing past the supposed limits that bad philosophy once taught us to resign ourselves to.

What if the theory is eventually refuted—if some deeper limitation foils the attempt to build a scalable quantum computer? We would be thrilled to see that happen. Such an outcome is by far the most desired one. Not only would it lead to a revision of our fundamental knowledge about physics, we would expect it to provide even more fascinating types of computation. For if something stops quantum mechanics, we shall expect to have an exciting new whatever-stops-quantum-mechanics theory, followed by exciting new whatever-stops-quantum-computers computers. One way or another, there will be no limits on knowledge or progress. SA

CORBIS

FLAMMARION ENGRAVING: This famous 19th-century wood engraving (first printed in black and white) poses the question: Is knowledge bounded, or can we always poke our head into the beyond?

MORE TO EXPLORE

The Fabric of Reality: The Science of Parallel Universes—and Its Implications. David Deutsch. Penguin, 1998.

The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation. Dirk Bouwmeester, Artur Ekert and Anton Zeilinger. Springer, 2000.

Quanta, Ciphers and Computers. Artur Ekert in *The New Physics*. Edited by Gordon Fraser. Cambridge University Press, 2006.

The Beginning of Infinity: Explanations That Transform the World. David Deutsch. Penguin, 2011.

The Emergent Multiverse: Quantum Theory according to the Everett Interpretation. David Wallace. Oxford University Press, 2012.

SCIENTIFIC AMERICAN ONLINE

Hear the authors dispel myths about quantum limits at ScientificAmerican.com/sep2012/quantum-myths