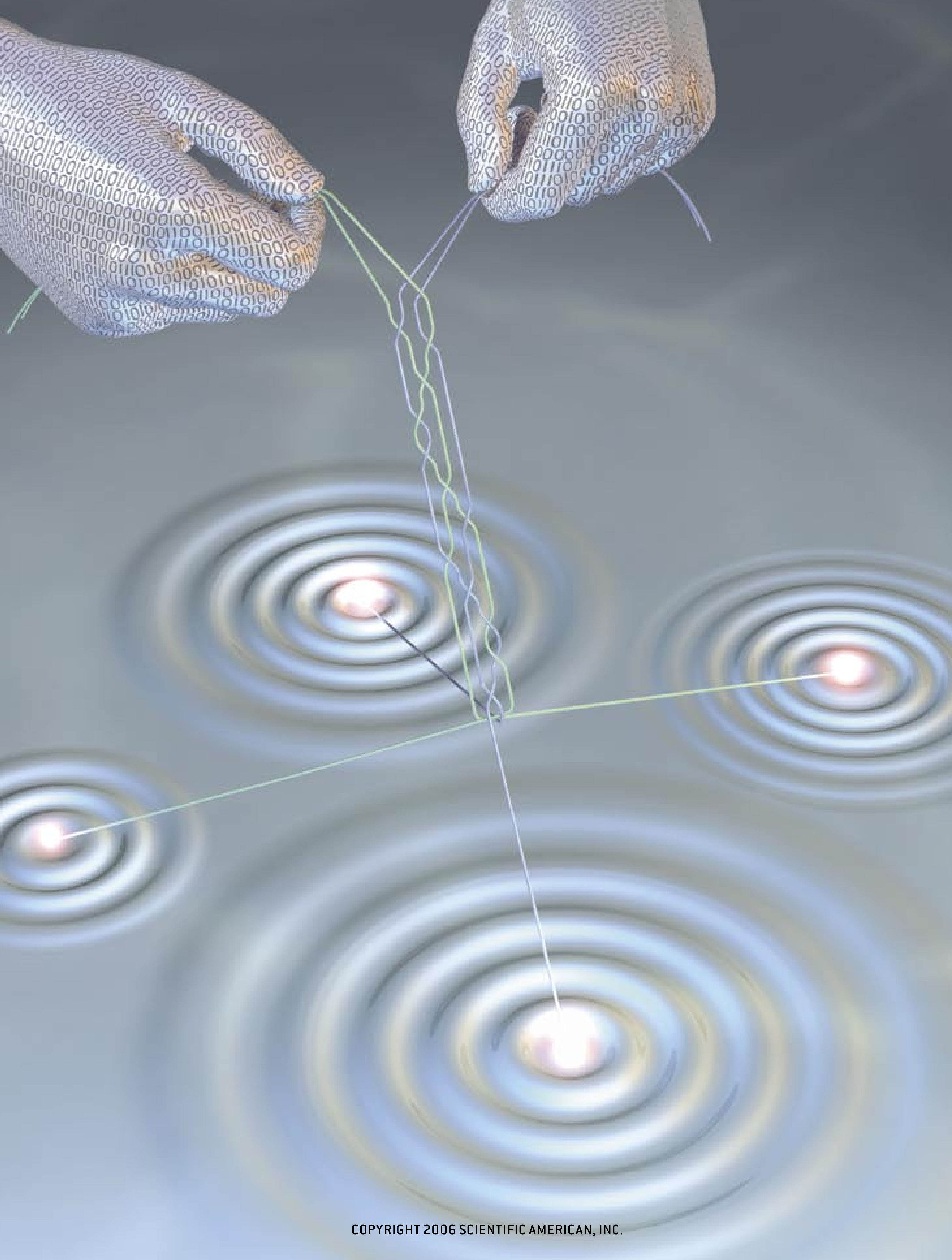


BY BRAIDING WORLD LINES (trajectories) of special particles, one can perform a quantum computation that is impossible for any ordinary (classical) computer. The particles live in a fluid known as a two-dimensional electron gas.

Computing with Quantum Knots

A machine based on bizarre particles called anyons that represents a calculation as a set of braids in spacetime might be a shortcut to practical quantum computation

By Graham P. Collins

Quantum computers promise to perform calculations believed to be impossible for ordinary computers. Some of those calculations are of great real-world importance. For example, certain widely used encryption methods could be cracked given a computer capable of breaking a large number into its component factors within a reasonable length of time. Virtually all encryption methods used for highly sensitive data are vulnerable to one quantum algorithm or another.

The extra power of a quantum computer comes about because it operates on information represented as qubits, or quantum bits, instead of bits. An ordinary classical bit can be either a 0 or a 1, and standard microchip architectures enforce that dichotomy rigorously. A qubit, in contrast, can be in a so-called superposition state, which entails proportions of 0 and 1 coexisting together. One can think of the possible qubit states as points on a sphere. The north pole is a classical 1, the south pole a 0, and all the points in between are all the possible superpositions of 0 and 1 [see "Rules for a Complex Quantum World," by Michael A. Nielsen; Scientific American, November 2002]. The freedom that qubits have to roam across the entire sphere helps to give quantum computers their unique capabilities.

Unfortunately, quantum computers seem to be extremely difficult to build. The qubits are typically expressed as certain quantum properties of trapped particles, such as individual atomic ions or electrons. But their superposition states are ex-

GEORGE RETSECK

ceedingly fragile and can be spoiled by the tiniest stray interactions with the ambient environment, which includes all the material making up the computer itself. If qubits are not carefully isolated from their surroundings, such disturbances will introduce errors into the computation.

Most schemes to design a quantum computer therefore focus on finding ways to minimize the interactions of the qubits with the environment. Researchers know that if the error rate can be reduced to around one error in every 10,000 steps, then error-correction procedures can be implemented to compensate for decay of individual qubits. Constructing a functional machine that has a large number of qubits isolated well enough to have such a low error rate is a daunting task that physicists are far from achieving.

A few researchers are pursuing a very different way to build a quantum computer. In their approach the delicate quantum states depend on what are known as topological properties of a physical system. Topology is the mathematical study of properties that are unchanged when an object is smoothly deformed, by actions such as stretching, squashing and bending but not by cutting or joining. It embraces such subjects as knot theory. Small perturbations do not change a topological property. For example, a closed loop of string with a knot tied in it is topologically different from a closed loop with no knot [*see box on opposite page*]. The only way to change the closed loop into a closed loop plus knot is to cut the string, tie the knot and then reseal the ends of the string together. Similarly, the only way to convert a topological qubit to a different state is to subject it to some such violence. Small nudges from the environment will not do the trick.

At first sight, a topological quantum computer *does not seem much like a computer at all.*

At first sight, a topological quantum computer does not seem much like a computer at all. It works its calculations on braided strings—but not physical strings in the conventional sense. Rather, they are what physicists refer to as world lines, representations of particles as they move through time and space. (Imagine that the length of one of these strings represents a particle's movement through time and that its thickness represents the particle's physical dimensions.) Moreover, even the particles involved are unlike the electrons and protons that one might first imagine. They are instead quasiparticles—excitations in a two-dimensional electronic system that behave a lot like the particles and antiparticles of high-energy physics. And as a further complication, the quasiparticles are of a special type called anyons, which have the desired mathematical properties.

Here is a what a computation might look like: first, create pairs of anyons and place them along a line [*see box on page 60*]. Each anyon pair is rather like a particle and its corresponding antiparticle, created out of pure energy.

Next, move pairs of adjacent anyons around one another in a carefully determined sequence. Each anyon's world line forms a thread, and the movements of the anyons as they are swapped this way and that produce a braiding of all the threads. The quantum computation is encapsulated in the particular braid so formed. The final states of the anyons, which embody the result of the computation, are determined by the braid and not by any stray electric or magnetic interaction. And because the braid is topological—nudging the threads a little bit this way and that does not change the braiding—it is inherently protected from outside disturbances. The idea of using anyons to carry out computations in this fashion was proposed in 1997 by Alexei Y. Kitaev, now at Microsoft.

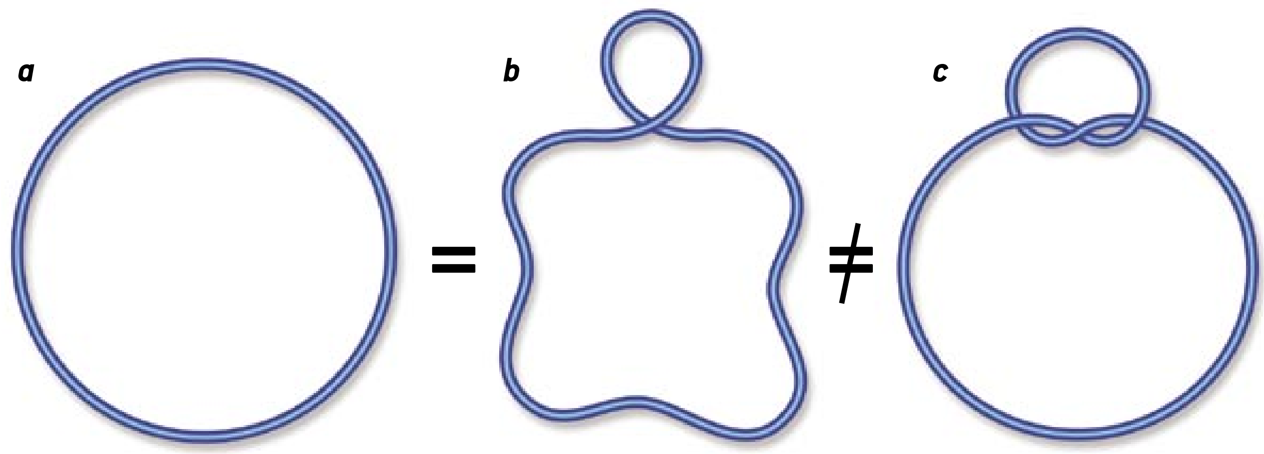
Michael H. Freedman, now at Microsoft, lectured at Harvard University in the fall of 1988 on the possibility of using quantum topology for computation. These ideas, published in a research paper in 1998, built on the discovery that certain mathematical quantities known as knot invariants were associated with the quantum physics of a two-dimensional surface evolving in time. If an instance of the physical system could be created and an appropriate measurement carried out, the knot invariant would be approximately computed automatically instead of via an inconvenient-

Overview/*Quantum Braids*

- Quantum computers promise to greatly exceed the abilities of classical computers, but to function at all, they must have very low error rates. Achieving the required low error rates with conventional designs is far beyond current technological capabilities.
- An alternative design is the so-called topological quantum computer, which would use a radically different physical system to implement quantum computation. Topological properties are unchanged by small perturbations, leading to a built-in resistance to errors such as those caused by stray interactions with the surrounding environment.
- Topological quantum computing would make use of theoretically postulated excitations called anyons, bizarre particlelike structures that are possible in a two-dimensional world. Experiments have recently indicated that anyons exist in special planar semiconductor structures cooled to near absolute zero and immersed in strong magnetic fields.

TOPOLOGY AND KNOTS

Topology of a closed loop (*a*) is unaltered if the string is pushed around to form another shape (*b*) but is different from that of a closed loop with a knot tied in it (*c*). The knot cannot be formed just by moving around the string. Instead one must cut the string, tie the knot and rejoin the ends. Consequently, the topology of the loop is insensitive to perturbations that only push the string around.



ly long calculation on a conventional computer. Equally difficult problems of more real-world importance would have similar shortcuts.

Although it all sounds like wild theorizing quite removed from reality, recent experiments in a field known as fractional quantum Hall physics have put the anyon scheme on firmer footing. Further experiments have been proposed to carry out the rudiments of a topological quantum computation.

Anyons

AS PREVIOUSLY MENTIONED, a topological quantum computer braids world lines by swapping the positions of particles. How particles behave when swapped is one of the many ways that quantum physics differs fundamentally from classical physics. In classical physics, if you have two electrons at locations A and B and you interchange their positions, the final state is the same as the initial state. Because the electrons are indistinguishable, so, too, are the initial and final states. Quantum mechanics is not so simple.

The difference arises because quantum mechanics describes the state of a particle with a quantity called the wave function, a wave in space that encapsulates all the properties of the particle—the probability of finding it at various locations, the probability of measuring it at various velocities, and so on. For example, a particle is most likely to be found in a region where the wave function has a large amplitude.

A pair of electrons is described by a joint wave function, and when the two electrons are exchanged, the resulting joint wave function is minus one times the original. That changes peaks of the wave into troughs, and vice versa, but it has no effect on the amplitude of the oscillations. In fact, it does not change any measurable quantity of the two electrons considered by themselves.

What it does change is how the electrons might interfere with other electrons. Interference occurs when two waves are added together. When two waves interfere, the combination has a high amplitude where peaks of one align with peaks of the other ("constructive interference") and has a low amplitude where peaks align with troughs ("destructive interference"). Multiplying one of the waves by a phase of minus one interchanges its peaks and troughs and thus changes constructive interference, a bright spot, to destructive interference, a dark spot.

It is not just electrons that pick up a factor of minus one in this way but also protons, neutrons and in general any particle of a class called fermions. Bosons, the other chief class of particles, have wave functions that are unchanged when two particles are swapped. You might say that their wave functions are multiplied by a factor of plus one.

Deep mathematical reasons require that quantum particles in three dimensions must be either fermions or bosons. In two dimensions, another possibility arises: the factor might be a complex phase. A complex phase can be thought of as an angle. Zero degrees corresponds to the number one; 180 degrees is minus one. Angles in-between are complex numbers. For example, 90 degrees corresponds to *i,* the square root of minus one. As with a factor of minus one, multiplying a wave function by a phase has absolutely no effect on the measured properties of the individual particle, because all that matters for those properties are the amplitudes of the oscillations of the wave. Nevertheless, the phase can change how two complex waves interfere.

Particles that pick up a complex phase on being swapped are called anyons because *any* complex phase might appear, not just a phase of plus or minus one. Particles of a given species, however, always pick up the same phase.

Electrons in Flatland

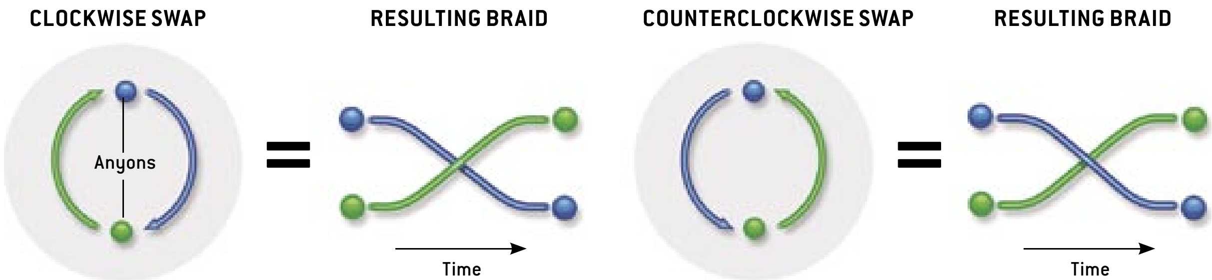
ANYONS EXIST ONLY in a two-dimensional world. How can we produce pairs of them for topological computing when we live in three dimensions? The

GEORGE RETSECK

HOW TOPOLOGICAL QUANTUM COMPUTING WORKS

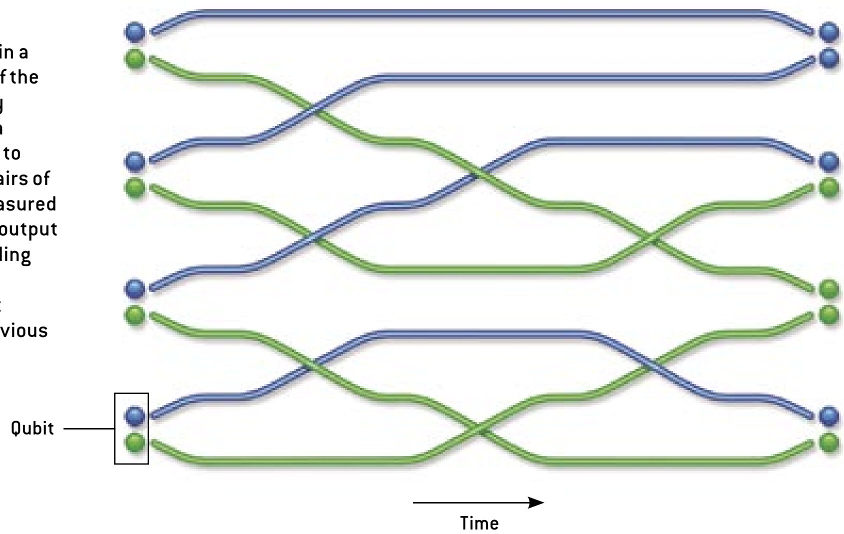
BRAIDING

Just two basic moves in a plane—a clockwise swap and a counterclockwise swap—generate all the possible braidings of the world lines (trajectories through spacetime) of a set of anyons.

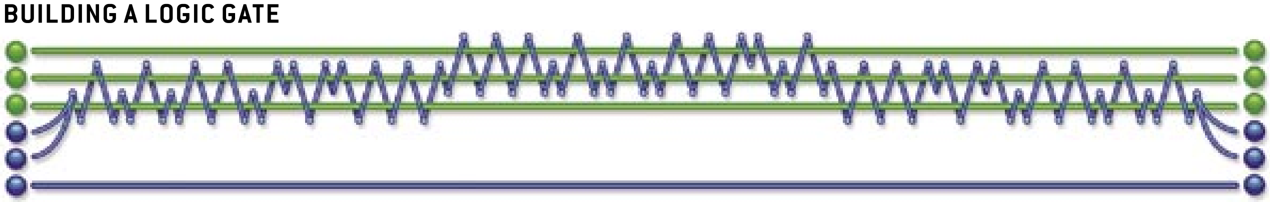


COMPUTING

First, pairs of anyons are created and lined up in a row to represent the qubits, or quantum bits, of the computation. The anyons are moved around by swapping the positions of adjacent anyons in a particular sequence. These moves correspond to operations performed on the qubits. Finally, pairs of adjacent anyons are brought together and measured to produce the output of the computation. The output depends on the topology of the particular braiding produced by those manipulations. Small disturbances of the anyons do not change that topology, which makes the computation impervious to normal sources of errors.



BUILDING A LOGIC GATE



A logic gate known as a CNOT gate is produced by this complicated braiding of six anyons. A CNOT gate takes two input qubits and produces two output qubits. Those qubits are represented by triplets (*green* and *blue*) of so-called Fibonacci anyons. The particular style of braiding—leaving one triplet in place and moving two anyons of the other triplet around its anyons—simplified the calculations involved in designing the gate. This braiding produces a CNOT gate that is accurate to about 10^{-3}.

GEORGE RETSECK

answer lies in the flatland realm of quasiparticles. Two slabs of gallium arsenide semiconductor can be carefully engineered to accommodate a "gas" of electrons at their interface. The electrons move freely in the two dimensions of the interface but are constrained from moving in the third dimension, which would take them off the interface. Physicists have intensely studied such systems of electrons, called two-dimensional electron gases, particularly when the systems are immersed in high transverse magnetic fields at extremely low temperatures, because of the unusual quantum properties exhibited under these conditions.

For example, in the fractional quantum Hall effect, excitations in the electron gas behave like particles having a fraction of the charge of the electron. Other excitations carry units of the magnetic flux around with them as though the flux were an integral part of the particle. In 2005 Vladimir J. Goldman, Fernando E. Camino and Wei Zhou of Stony Brook University claimed to have direct experimental confirmation that quasiparticles occurring in the fractional quantum Hall state are anyons, a crucial first step in the topological approach to quantum computation. Some researchers, however, still seek independent lines of evidence for the quasiparticles' anyonic nature because certain nonquantum effects could conceivably produce the results seen by Goldman and his colleagues.

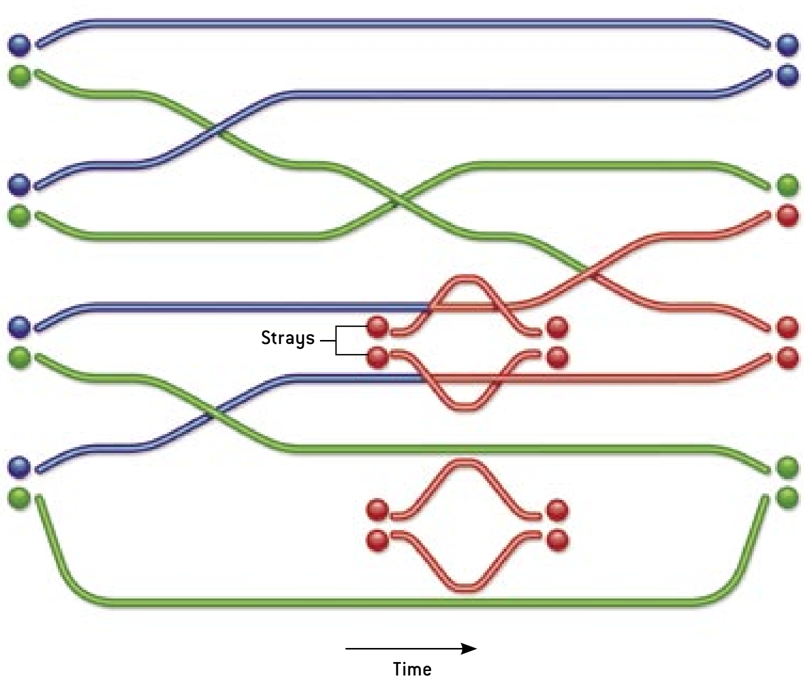
In two dimensions, an important new issue arises in the swapping of two particles: Do the particles follow clockwise tracks or counterclockwise tracks as they are interchanged? The phase picked up by the wave function depends on that property. The two alternative paths are topologically distinct, because the experimenter cannot continuously deform the clockwise paths into counterclockwise paths without crossing the paths and having the particles collide somewhere.

To build a topological quantum computer requires one additional complication: the anyons must be what is called nonabelian. This property means that the order in which particles are swapped is important. Imagine that you have three identical anyons in a row, at positions A, B and C. First swap the anyons at positions A and B. Next swap the anyons now located at B and C. The result will be the original wave function modified by some factor. Suppose instead that the anyons at B and C are swapped first, followed by swapping those at A and B. If the result is the wave function multiplied by the same factor as before, the anyons are called abelian. If the factors differ depending on the order of the swapping, they are nonabelian anyons. (The nonabelian property arises because for these anyons, the factor that multiplies the wave function is a matrix of numbers, and the result of multiplying two matrices depends on the order in which they are multiplied.)

The experiment by Goldman's team involved abelian anyons. Nevertheless, theorists have strong reason to believe that certain fractional quantum Hall quasiparticles are indeed nonabelian. Experiments have been proposed to settle that question. One was suggested by Freedman, along with Sankar Das Sarma of the University of Maryland at College Park and Chetan Nayak of Microsoft, with important refinements proposed by Ady Stern of the Weizmann Institute in Israel and Bertrand Halperin of Harvard University; the second was presented by Kitaev, Parsa Bonderson of the California Institute of Technology and Kirill Shtengel, now at the University of California, Riverside.

PREVENTING RANDOM ERRORS

Errors will occur in a topological computation if thermal fluctuations generate a stray pair of anyons that intertwine with the braid of the computation before they self-annihilate. Those strays will then corrupt (*red lines*) the computation. The probability of this interference drops exponentially with the distance that the anyons travel, however. The error rate can be minimized by keeping the computation anyons sufficiently far apart (*bottom pair*).



GEORGE RETSECK

Braids and Gates

ONCE YOU HAVE nonabelian anyons, you can generate a physical representation of what is called the braid group. This mathematical structure describes all the ways that a given row of threads can be braided together. Any braid can be built out of a series of elementary operations in which two adjacent threads are moved, by either a clockwise or a counterclockwise motion. Every possible sequence of anyon manipulations corresponds to a braid, and vice versa. Also corresponding to each braid is a very complicated matrix, the result of combining all the individual matrices of every anyon exchange.

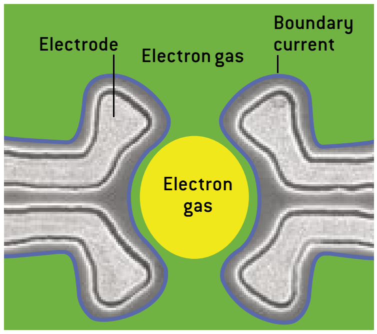
Now we have all the elements in place to see how these braids correspond to a quantum computation. In a conventional computer, the state of the computer is represented by the combined state of all its bits—the particular sequence of 0s and 1s in its register. Similarly, a quantum computer is represented by the combined state of all its qubits. In a topological quantum computer, the qubits may be represented by groups of anyons.

In a quantum computer, the process of going from the initial state of all the qubits to the final state is described by a matrix that multiplies the joint wave function of all the qubits. The similarity to what happens in a topological quantum computer is obvious: in that case, the matrix is the one associated with the particular braid corresponding to the sequence of anyon manipulations. Thus, we have verified that the operations car-

TOPOLOGICAL ERRORS

ANYON DETECTOR

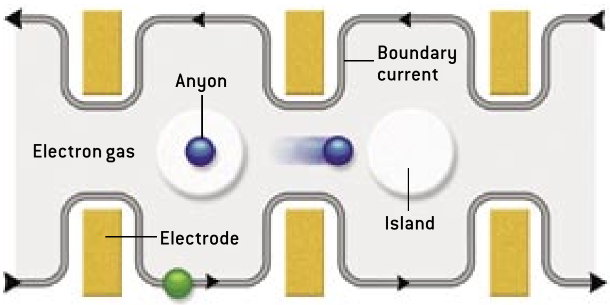
The device in this colorized micrograph was used by Vladimir J. Goldman and his co-workers to demonstrate that certain quasiparticles (excitations in the quantum Hall state) behave as anyons. The device was cooled to 10 millikelvins and put in a strong magnetic field. A two-dimensional electron gas formed around the four electrodes, with different types of quasiparticles present in the yellow and green areas. Characteristics of the current flowing along the boundary confirmed that the quasiparticles in the yellow island were anyonic.



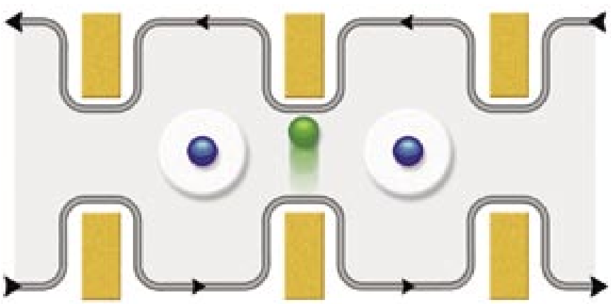
NOT GATE

This proposed anyonic NOT gate is based on a fractional quantum Hall state involving anyons having one-quarter the charge of an electron. Electrodes induce two islands on which anyons can be trapped. Current flows along the boundary but under the right conditions can also tunnel across the narrow isthmuses.

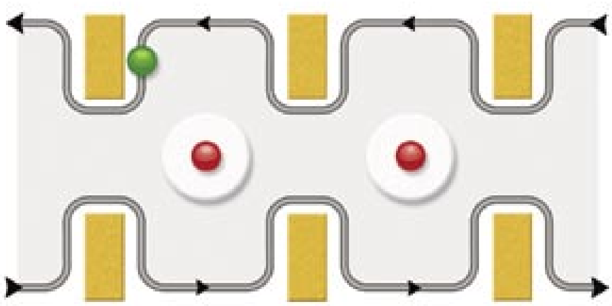
1 Initialize the gate by putting two anyons (*blue*) on one island and then applying voltages to transfer one anyon to the other island. This pair of anyons represents the qubit in its initial state, which can be determined by measuring the current flow along the neighboring boundary.



2 To flip the qubit (the NOT operation), apply voltages to induce one anyon from the boundary (*green*) to tunnel across the device.



3 The passage of this anyon changes the phase relation of the two anyons so that the qubit's value is flipped to the opposite state (*red*).



ried out on the anyons result in a quantum computation.

Another important feature must be confirmed: Can our topological quantum computer perform *any* computation that a conventional quantum computer can? Freedman, working with Michael Larsen of Indiana University and Zhenghan Wang, now at Microsoft, proved in 2002 that a topological quantum computer can indeed simulate any computation of a standard quantum computer, but with one catch: the simulation is approximate. Yet given any desired accuracy, such as one part in 10^4, a braid can be found that will simulate the required computation to that accuracy. The finer the accuracy required, the greater the number of twists in the braid. Fortunately, the number of twists required increases very slowly, so it is not too difficult to achieve very high accuracy. The proof does not, however, indicate *how* to determine which actual braid corresponds to a computation—that depends on the specific design of topological quantum computer, in particular the species of anyons employed and their relation to elementary qubits.

The problem of finding braids for doing specific computations was tackled in 2005 by Nicholas E. Bonesteel of Florida State University, along with colleagues there and at Lucent Technologies's Bell Laboratories. The team showed explicitly how to construct a so-called controlled NOT (or CNOT) gate to an accuracy of two parts in 10^3 by braiding six anyons. A CNOT gate takes two inputs: a control bit and a target bit. If the control bit is 1, it changes the target bit from 0 to 1, or vice versa. Otherwise the bits are unaltered. Acting on qubits, any computation can be built from a network of CNOT gates and one other operation—the multiplication of individual qubits by a complex phase. This result serves as another confirmation that topological quantum computers can perform any quantum computation.

Quantum computers can perform feats believed to be impossible for classical computers. Is it possible that a topological computer is more powerful than a conventional quantum computer? An-

GEORGE RETSECK (*illustration*); FROM F. E. CAMINO ET AL. IN *PHYSICAL REVIEW LETTERS*, VOL. 95; 2005 (*micrograph*) other theorem, proved by Freedman, Kitaev and Wang, shows that is not the case. They demonstrated that the operation of a topological quantum computer can be simulated efficiently to arbitrary accuracy on a conventional quantum computer, meaning that anything that a topological quantum computer can compute a conventional quantum computer can also compute. This result suggests a general theorem: any sufficiently advanced computation system that makes use of quantum resources has exactly the same computational abilities. (An analogous thesis for classical computing was proposed by Alonzo Church and Alan Turing in the 1930s.)

Particles In, Answers Out

I HAVE GLOSSED OVER two processes that are crucial to building a practical topological quantum computer: the initialization of the qubits before the start of the computation and the readout of the answer at the end.

The initialization step involves generating quasiparticle pairs, and the problem is knowing what species of quasiparticle has been created. The basic procedure is to pass test anyons around the generated pairs and then measure how the test anyons have been altered by that process, which depends on the species of the anyons that they have passed. (If a test anyon is altered, it will no longer be cleanly annihilated with its partner.) Anyon pairs not of the required type would be discarded.

The readout step also involves measuring anyon states. While the anyons are widely separated, that measurement is impossible: the anyons must be brought together in pairs to be measured. Roughly speaking, it is like checking to see if the pairs annihilate cleanly, like true antiparticles, or if they leave behind residues of charge and flux, which reveals how their states have been altered by braiding from the exact antiparticle relation in which they began their lives.

Also, it is not true that a topological computer is totally immune to errors. The main source of error is thermal fluctuations in the substrate material, which can generate an extra pair of anyons. Both the anyons then intertwine themselves with the braid of the computation, and finally the pair annihilates again [*see box on page 61*]. Fortunately, the thermal generation process is suppressed at the low temperature at which a topological computer would operate. Furthermore, the probability of the entire bad process occurring decreases exponentially as the distance traveled by the interlopers increases. Thus, one can achieve any required degree of accuracy by building a sufficiently large computer and keeping the working anyons far enough apart as they are braided.

The trio estimated that the error rate for their *NOT gate would be 10^{-30} or less.*

Topological quantum computing remains in its infancy. The basic working elements, nonabelian anyons, have not yet been demonstrated to exist, and the simplest of logic gates has yet to be built. The previously mentioned experiment of Freedman, Das Sarma and Nayak would achieve both those goals—if the anyons involved do turn out to be nonabelian, as expected, the device would carry out the logical NOT operation on the qubit state. The trio estimated that the error rate for the process would be 10^{-30} or less. Such a tiny error rate occurs because the probability of errors is exponentially suppressed as the temperature is lowered and the length scale increased. That exponential factor is the essential contribution of topology, and it has no analogue in the more traditional approaches to quantum computing.

The promise of extraordinarily low error rates—many orders of magnitude lower than those achieved by any other quantum computation scheme to date—is what makes topological quantum computing so attractive. Also, the technologies involved in making fractional quantum Hall devices are mature, being precisely those of the microchip industry; the only catch is that the devices have to operate at extremely low temperatures—on the order of millikelvins—for the magical quasiparticles to be stable.

If nonabelian anyons actually exist, topological quantum computers could well leapfrog conventional quantum computer designs in the race to scale up from individual qubits and logic gates to fully fledged machines more deserving of the name "computer." Carrying out calculations with quantum knots and braids, a scheme that began as an esoteric alternative, could become the standard way to implement practical, error-free quantum computation. SA

Graham P. Collins is a staff writer and editor, with a Ph.D. in physics from Stony Brook University. He wishes to thank Michael H. Freedman, the director of Project Q at Microsoft, for contributions in the preparation of this article.

MORE TO EXPLORE

Topologically Protected Qubits from a Possible Non-Abelian Fractional Quantum Hall State. Sankar Das Sarma, Michael Freedman and Chetan Nayak in *Physical Review Letters,* Vol. 94, pages 166802-1–168802-4; April 29, 2005.

Devices Based on the Fractional Quantum Hall Effect May Fulfill the Promise of Quantum Computing. Charles Day in *Physics Today,* Vol. 58, pages 21–24; October 2005.

Anyon There? David Lindley in *Physical Review Focus,* Vol. 16, Story 14; November 2, 2005. http://focus.aps.org/story/v16/st14

Topological Quantum Computation. John Preskill. Lecture notes available at www.theory.caltech.edu/~preskill/ph219/topological.pdf