Isaac Chuang

Quantum Information

Joining the Foundations of Physics and Computer Science

Why should physics have anything to do with the ability to solve mathematical problems? Indeed, until recently, physics and computer science were divorced at their foundations by a fundamental thesis, that algorithms—procedures for solving mathematical problems—could be distinguished *independent* of the physical world. The thesis holds that problems are, among other things, either *easy* or *hard* to solve, and such distinctions persist no matter what the physical nature of the computational machinery is, be it mechanical, electrical, optical or any other. Astonishingly, however, discoveries in the last decade showed this equivalence does not extend to information processors which utilize quantum physics. By utilizing non-classical states of matter, quantum-mechanical machines can easily solve certain problems which are hard for classical processors. Moreover, this capability can exist even in the presence of imperfections and noise.

This reunion of the two fields has generated significant surprises for physics and computer science. Here, I try to describe the ideas underlying this new scientific area, and how current experiments are racing to develop access to this new realm, known as QUANTUM INFORMATION.

Easy and Hard—Cryptography and Factoring

The ease or difficulty of solving mathematical problems might seem a bit esoteric, but, in fact, it is immediately relevant to everyday modern life. In particular, the security of most bank transactions, including the integrity of ATM machines, hinges upon the apparently enormous difficulty of one mathematical problem. How this is accomplished is simple to understand if you've ever played with a puzzle box. Just as carpenters design wooden boxes that open only when sliders are operated in the right sequence, and just as watchmakers build intricate mechanical locks for safes, modern cryptographers craft mathematical problems which are hard to solve without the right key. This key is a password, a string of digits transmitted over electronic networks, which authenticates identities between sender and receiver and encrypts data between buyer and seller. Today, such puzzles safeguard electronic documents, secret communications and financial transactions, including most web-based electronic commerce.

Nearly all such cryptography is based on the difficulty of one mathematical problem: finding the prime factors of an integer. What two numbers, when multiplied, give 91? It is easy to verify that 7313 =91, but finding these factors is a task so time-consuming for large numbers that it is deemed impractical. For example, what are the factors of 1207? Or of 12433159? Modern applications use numbers with more than 310 decimal digits, which are believed to require at least billions of years to factor. Thus, I could secretly choose two prime numbers and anonymously advertise their product in the *New York Times*. Years later, I could authoritatively establish myself as the author of the advertisement by revealing the secret factors. Other methods allow data to be encrypted using prime numbers; today, the importance of prime numbers is such that a U.S. Patent[1] has even been granted for a cryptosystem using two specific primes.

The confidence in factoring as a good cryptographic problem rests on two observations. First, it has a long history. Euclid studied the properties of prime numbers in the days of the Greeks. Indeed, the fact that any positive integer can be

> “Nearly all such cryptography is based on the difficulty of one mathematical problem: finding the prime factors of an integer.”

uniquely represented as a product of prime numbers is the fundamental theorem of arithmetic.

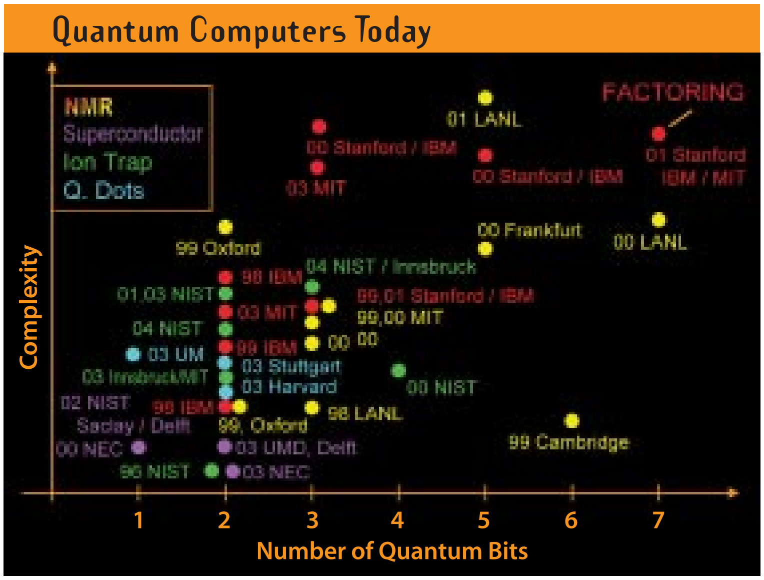

Figure 1

Graph giving some perspective on the state of some (but not all!) current quantum computer implementations, in terms of complexity of task accomplished plotted versus number of quantum bits ("qubits") realized.

Second, it is a fundamental tenet of computer science, known as the Modern Church-Turing thesis, that a hard mathematical problem remains hard no matter the physical nature of a machine used to solve it. No lock, after all, is perfectly secure; MIT undergraduates are notorious for their expertise at appearing behind apparently locked doors (and for authoring the "MIT Guide to Lock Picking," floating around the internet). And one is always wary of new technologies which break locks; for example, a mechanical lock can be X-rayed and the pins measured, to reproduce a master key. However, according to the Modern Church-Turing thesis, independent of the laws of physics, no better computing technology exists that can factor numbers much faster than electronic machines.

At this point, physics re-enters the story. In 1984, to great surprise and acclaim around the world, Peter Shor[2] announced his discovery of an algorithm to easily factor integers, using a computing machine based on quantum physics. This was astonishing! If such a machine could be built, it would jeopardize the most widely used modern cryptosystem. And other hard mathematical problems might also be easily solved. But what is a quantum computer, and is it realistic?

The Quantum Computer

All computing machines must be realized as physical devices that obey the laws of physics. Indeed, the first computers were mechanical machines, which essentially used Newtonian mechanics to solve mathematical problems. During the last century, these were replaced by electronic machines, with semiconductor devices employing electromagnetism and charge transport (Maxwell's and Boltzmann's equations) for representing information and performing computations. Moreover, for the past forty years, the number of transistor switches per square inch in the most important semiconductor, silicon, has been doubling roughly every 18 months—a phenomenon often referred to as Moore's Law. If this trend continues unabated, by 2015 transistors will be the size of single atoms and molecules. At that length scale, the classical laws of physics give way to quantum mechanics. That is the realm in which quantum computers operate.

The unique properties of quantum states of matter give rise to the additional computational capabilities of quantum computers. Single atoms can represent information in the form of zeros and ones, for example, as ground and excited states of atoms. But quantum physics allows additional superposition states, that are simultaneously partly ground and partly excited states. These are still "digital," in that, when measured, the atom can be found to be in only one of the two states, but before the measurement they can be in both at once.

Even stranger is the fact that two atoms can simultaneously be in a linked kind of superposition state, known as ENTANGLEMENT. For example, the two can be prepared in a superposition of both atoms being excited, and both atoms being in their ground states. This is a uniquely quantum state which has no classical analogue; when measured, both atoms are always found to be in the same state, which reflects a classical correlation, but this correlation persists beyond what is possible classically.

Using such superpositions and entanglement, a quantum computer can in a sense evaluate a mathematical function simultaneously on all possible input values. The multiple simultaneous computational pathways can then be interfered to obtain the desired result. Shor's quantum factoring algorithm cleverly causes constructive interference to occur such that the desired result, the factors of an integer, are amplified and successfully output after a short number of instructions. These include many of the usual computer programming instructions, such as addition, multiplication and boolean logic, but there are also new "quantum gates," such as the Hadamard gate, a kind of "square root of NOT" gate that transforms a bit from zero to an equal superposition of zero and one. Shor's algorithm can factor an L digit integer using approximately L^3 instructions, a tremendous improvement over the approximately $2^{L^{1/3}}$ required by the best known classical algorithm.

Beyond quantum factoring, new algorithms have recently been discovered, giving provable exponential speedups between classical and quantum. Notably, Edward Farhi[3], Jeffrey Goldstone[4], and collaborators showed that there exist tree structures that quantum processors can walk through easily, but classical processors find hard to traverse.

These and other results have overturned the Church-Turing thesis, at the foundations of computer science, which views algorithms as existing completely outside of the world of physics. Such a picture cannot hold when computers operating using quantum mechanics can easily perform tasks that computers solely utilizing classical mechanics and electrodynamics cannot. For computer science, this has been a great surprise that is slowly but surely gaining broad acceptance. For physics, there is delight in realizing that quantum mechanics will now be taught to aspiring new computer science students.

> "Even stranger is the fact that two atoms can simultaneously be in a linked kind of superposition state, known as ENTANGLEMENT."

Reduction to Practice

Will you ever be able to buy a quantum information processor at your local computer store? After all, many models of computation have come and gone; only those which are physically realistic, and realizable, are interesting. Over the past decade since Shor's discovery, a race has been developing to reduce these theories

continues on page 44

continued from page 29

to practice and to understand whether or not a large-scale quantum computer is possible in principle. A wide variety of physical systems (*see Figure 1, p. 28*) have been considered as candidate implementations, including single photons and atoms, Cooper pairs in superconducting metallic boxes, phases in Josephson junctions, electrons floating on liquid helium, nitrogen vacancies in diamond, trapped ions and nuclear spins. Among these, nuclear spins in molecules, controlled with magnetic resonance techniques, have been used to demonstrate Shor's factoring algorithm.

Current systems have been limited to just a handful of quantum bits, but future quantum information processing systems, with many more quantum bits, and even more complex sequences of operations, are widely expected to be realized. Recently, several groups around the world showed that superconductor qubit realizations could remain in superposition states for up to several hundred nanoseconds. Especially promising are atomic systems with cold, trapped ions and neutral atoms, because they are particularly well understood, cleanly controlled using pulsed laser excitations and accessible at time scales within reach of laboratory equipment. Recent ion trap experiments have demonstrated simple two, three and four qubit computations and manipulations, including quantum teleporation.

From Quantum Information to New Physics

Perhaps an even greater surprise than the discovery of fast quantum algorithms is the realization that such algorithms can retain their speed even in the presence of imperfections and fundamental noise sources. Quantum states, in particular superpositions and entangled states, are actually well known for their fragility; when measured, a wavefunction collapses, and nearly any interaction with an environment leads to a partial measurement of the state. This effect, known as *decoherence*, makes quantum systems evolve rapidly towards stable, classical states. For example, an excited atom is unstable; it inevitably decays by spontaneous emission to reach its ground state. Unchecked, decoherence prohibits quantum computers from functioning well, or for very long.

However, it turns out that techniques from the theory of information, originating in Claude Shannon's[5] seminal study of communication channels in 1948, allow information to be protected against errors, and these *error correction* techniques extend to protect quantum information as well.

More importantly, we now understand how reliable quantum circuits can be constructed from faulty quantum gates. Early in the days of computation, John von Neumann[6] drew upon biology to deal with the unreliability of vacuum tube transistors; he developed a theory of how reliable automata could operate even with faulty organs, as long as their failure probability was below a certain, constant threshold. His theory is, by and large, unemployed in modern digital computers, because of the high degree of reliability of metal-oxide semiconductor field effect transistors in silicon. But von Neumann's theories of fault tolerance generalize beautifully to the quantum world, and are fundamentally why digital quantum computers can conceivably work reliably despite decoherence.

These results, drawn from the dawn of computer science, hold fascinating implications for the world of physics. They imply that a sufficiently well-engineered quantum system can stay in entangled superposition states indefinitely, requiring only occasional correction. The scheme works much like a refrigerator, but what is being reduced is not the kinetic energy of the air in the refrigerator, but the entropy of a quantum state.

Borrowing an analogy from Wolfgang Ketterle[7], let me observe that just as imaginary citizens of the sun would be amazed by ice cream given the discovery of refrigeration, I have no doubt that in the future, we will be thrilled by the properties of long-lived, pure, entangled quantum states, "cold" preserved and manipulated by fault-tolerant quantum processors. Already, many new connections have emerged. For example, entangled states are useful for precision time keeping, and for increasing the accessible precision of certain measurements. And communicating entangled states allows secret information to be shared between parties.

Quantum computation offers the potential for quickly solving certain mathematical problems important in modern cryptosystems. Less immediately, but even more fundamentally, quantum information brings new ideas from computer science to physics, and from physics to computer science. I am certain this is a rich quest upon which we have only just begun.

ENDNOTES

1. U.S. Patent number 5,373,360.
2. Peter W. Shor, Morss Professor of Applied Mathematics, MIT.
3. Edward Farhi, Professor of Physics and Director, MIT Center for Theoretical Physics.
4. Jeffrey Goldstone, Cecil and Ida Green Professor of Physics, MIT.
5. MIT Professor Emeritus Claude E. Shannon (1916–2001), known as the "father of modern digital communications and information theory." [MIT News Office, February 27, 2001.]
6. John von Neumann (1903–1957), Professor of Mathematics, The Institute for Advanced Study, Princeton University.
7. Wolfgang Ketterle, John D. MacArthur Professor of Physics, MIT, and 2001 Nobel Laureate.

ISAAC CHUANG, *Associate Professor of Physics and Associate Professor of Media Arts and Sciences in the MIT Center for Bits and Atoms, is a pioneer in the field of quantum information science. His experimental realization of two, three, five and seven quantum bit quantum computers using nuclear spins in molecules provided the first laboratory demonstrations of many important quantum algorithms, including Shor's quantum factoring algorithm. The error correction, algorithmic cooling and entanglement manipulation techniques he developed provide new ways to obtain complete quantum control over light and matter, and lay a foundation for possible large-scale quantum information processing systems.*

Chuang came to MIT in 2000 from IBM, where he was a research staff member. He received his doctorate in Electrical Engineering from Stanford University, where he was a Hertz Foundation Fellow. Chuang also holds one master and two bachelors degrees, in Physics and Electrical Engineering, from MIT, and was a postdoctoral fellow at Los Alamos National Laboratory and the University of California at Berkeley. He is the author, together with Michael Nielsen, of the textbook Quantum Computation and Quantum Information.