Physics Today

Quantum Information and Computation

Charles H. Bennett

Citation: Physics Today **48**(10), 24 (1995); doi: 10.1063/1.881452
View online: http://dx.doi.org/10.1063/1.881452
View Table of Contents:
http://scitation.aip.org/content/aip/magazine/physicstoday/48/10?ver=pdfcov
Published by the AIP Publishing

Quantum Information and Computation

A new quantum theory of communication and computation is emerging, in which the stuff transmitted or processed is not classical information, but arbitrary superpositions of quantum states.

Charles H. Bennett

Theoretical computer scientists, like their counterparts in physics, suffer and benefit from a high level of intellectual machismo. They believe they have some of the biggest brains around, which they need to think about some of the hardest problems. Like mathematicians, they prove theorems and doubt the seriousness of those who don't. Lately, however, theoretical computer scientists have sought the help of physicists in understanding quantum mechanics, a hard part of physics which they now believe has great significance for their own field.

Until recently, classical notions have sufficed. A conventional digital computer operates with bits—the Boolean states 0 and 1—and after each computation step the computer has a definite, exactly measurable state. Similarly, classical information theory considers transmissions conveying classical states, such as sequences of characters, each character having its own frequency of occurrence in a given context. In contrast to this, quantum information processing involves quantum states. The state of a quantum computer is described by a wavefunction or a state in a Hilbert space, and quantum information theory considers the transmission of quantum states from source to receiver.

Fundamental properties of quantum systems now seen to be relevant to information processing include:

▷ Superposition: A quantum computer can exist in an arbitrary complex linear combination of classical Boolean states, which evolve in parallel according to a unitary transformation.

▷ Interference: Parallel computation paths in the superposition, like paths of a particle through an interferometer, can reinforce or cancel one another, depending on their relative phase.

▷ Entanglement: Some definite states of a complete quantum system do not correspond to definite states of its parts.

▷ Nonclonability and uncertainty: An unknown quantum state cannot be accurately copied (cloned) nor can it be observed without being disturbed.

Quantum information processing exhibits some startling differences from the classical case. States can be transmitted by "quantum teleportation," a process that disembodies the exact quantum state of a particle into classical data and Einstein–Podolsky–Rosen (EPR) correlations, and then uses these ingredients to reincarnate the state in another particle which has never been anywhere near the first particle. Cryptographic keys can be distributed by quantum means, with near-perfect security against undetected eavesdropping. Quantum computers, meanwhile, are theoretically capable of solving certain problems, such as the factoring of large numbers, in dramatically fewer steps than any known algorithm on a classical computer. (Cryptography schemes in use throughout the world depend on the difficulty of factoring for their security.)

Charles Bennett *is an IBM Fellow at the Thomas J. Watson Research Center in Yorktown Heights, New York.*

Qubits

To illustrate the new results, it is sufficient to consider operations on and pairwise interactions between quantum systems of the simplest sort: two-state systems or "qubits."[1] Examples include the polarization of a photon or a spin-½ particle, the relative phase and intensity of a single photon in two arms of an interferometer, or an arbitrary superposition of two atomic states. The classical Boolean states, 0 and 1, can be represented by a fixed pair of orthogonal states of the qubit (say, $|0\rangle = |\leftrightarrow\rangle$, $|1\rangle = |\updownarrow\rangle$), but a qubit can also exist in superpositions such as $|\nearrow\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|\nwarrow\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Moreover, a pair of qubits can exist in entangled states such as the singlet state $\Psi^- = (|01\rangle - |10\rangle)/\sqrt{2}$, in which neither qubit by itself has a definite state. More generally, a string of n qubits can exist in any state of the form

$$\Psi = \sum_{x=00\ldots0}^{11\ldots1} c_x |x\rangle$$

where the c_x are complex numbers and the index x ranges over all 2^n classical values of an n-bit string. Quantum data processing consists of applying a sequence of unitary transformations to the state vector Ψ.

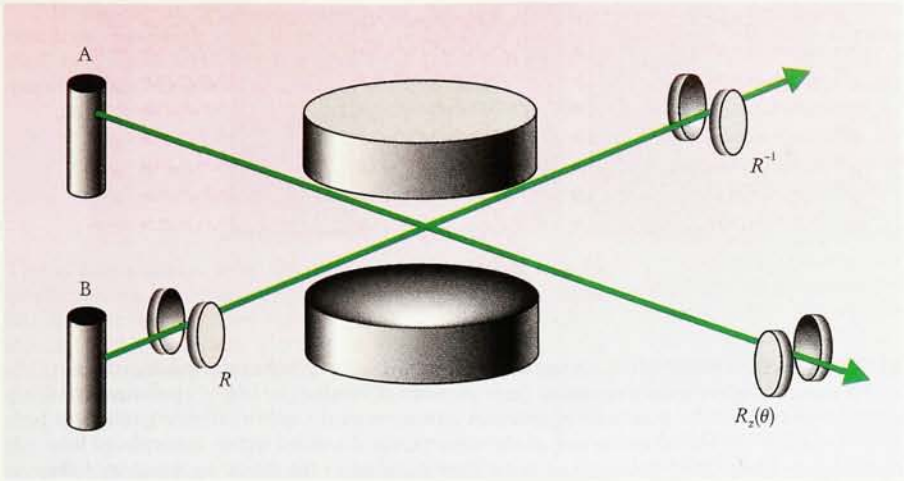
Some quantum logic operations are simply extensions of classical Boolean operations to superpositions of input states, for example NOT, represented by the unitary matrix

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

which flips the Boolean state of a single bit, and the controlled-NOT or exclusive-OR (XOR), which flips the second of two bits if and only if the first is 1. Others, such as the unitary operation represented by the 2×2 matrix

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

which corresponds to a 45° rotation of the polarization,



UNIVERSAL QUANTUM LOGIC GATE, as realized with high-finesse microwave cavities and two-state atoms. All possible quantum computations can be built up with a network of such gates. Passing atom $|A\rangle$ through the empty cavity on resonance transfers the atom's state, $|A\rangle = c_1|g\rangle + c_2|e\rangle$, to the photon occupancy $c_1|0\rangle + c_2|1\rangle$ of the cavity. Passing atom $|B\rangle$ through the Ramsey zones (R, R^{-1}) and the cavity (off resonance) changes its state to the exclusive-OR (XOR) of the initial states $|A\rangle \oplus |B\rangle$. The original state $|A\rangle$ can now be transferred back to an atom initially in the ground state, $|g\rangle$, passing along beam A. More general output states can be obtained by adjusting the atom–cavity interactions and adding another Ramsey zone, $R_z(\theta)$, which introduces a phase shift. (Adapted from refs. 4 and 15.) FIGURE 1.

are intrinsically nonclassical, because they transform Boolean states into superpositions.

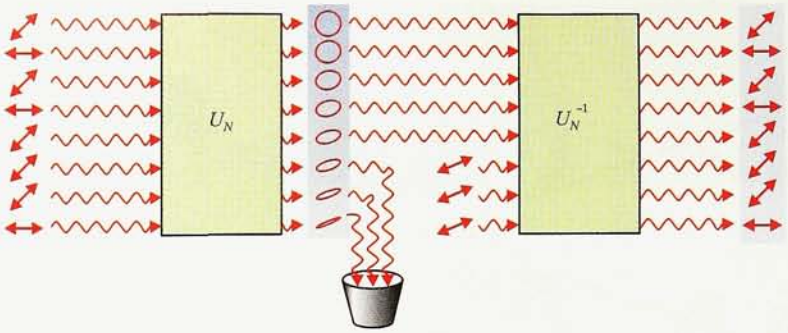
The XOR operation illustrates why classical data can be cloned but quantum superpositions cannot. If the XOR is applied to Boolean data in which the second qubit is 0 and the first is 0 or 1, the first qubit is unchanged while the second becomes a copy of it: $U_{\text{XOR}}|x, 0\rangle = |x, x\rangle$ for $x = 0$ or 1. In terms of the standard polarizations, $U_{\text{XOR}}|\leftrightarrow, \leftrightarrow\rangle = |\leftrightarrow, \leftrightarrow\rangle$ and $U_{\text{XOR}}|\updownarrow, \leftrightarrow\rangle = |\updownarrow, \updownarrow\rangle$. One might naively suppose that the XOR operation could also be used to copy superpositions of the two Boolean states, such as $|\nearrow\rangle$, so that $U_{\text{XOR}}|\nearrow, \leftrightarrow\rangle$ would yield $|\nearrow, \nearrow\rangle$, but this is not so. The unitarity of quantum evolution demands that a superposition of input states evolves to a corresponding superposition of outputs. Thus $U_{\text{XOR}}|\nearrow, \leftrightarrow\rangle = (|\leftrightarrow, \leftrightarrow\rangle + |\updownarrow, \updownarrow\rangle)/\sqrt{2}$, an entangled state in which neither output qubit by itself has definite polarization.

More complicated quantum information processing can be analyzed into elementary steps using diagrams similar to those used in classical computer logic. These diagrams consist of logic blocks or gates, where the processing is performed, and wires, which carry information forward from one stage of processing to the next. In classical processing, the wires carry bits and the gates perform deterministic (or occasionally stochastic) Boolean operations on them. In quantum information processing, the wires carry qubits and the gates perform unitary operations. (It has recently been shown that one- and two-qubit gates are sufficient to generate all such operations.[2–4]) Our diagrams will also include measurement steps, which generate classical outputs from quantum inputs, and preparation steps, in which a classical input specifies which of several unitary transformations is to be applied. Despite the concrete-sounding names, these gates and wires are to be thought of abstractly, as representing whatever physical apparatus is used to bring the qubits into controlled interaction, and to store and transport them between interactions. Figure 1 shows a physical realization of a two-qubit gate using high-finesse microwave cavities and two-state atoms.

Quantum data compression

Classical information theory characterizes the channel resources required for the transmission of classical data, asymptotically reliable transmission being possible if and only if the channel capacity exceeds the source entropy. There is also a well-developed theory of the optimum use of quantum channels to carry classical information. These notions have recently been further generalized by considering the classical and quantum channel resources needed to deliver *quantum* states accurately from a source to a receiver. In general, a quantum information source may be defined as a set of quantum states $\{\psi_i\}$ emitted with respective probabilities $\{p_i\}$. If the ψ_j are mutually orthogonal, no quantum channel resources are needed; all the information can be extracted by a measurement at the source, transmitted as classical information to the receiver, and used there to reconstruct the source state exactly. On the other hand, if the source states are nonorthogonal, for example $|\leftrightarrow\rangle$ and $|\nearrow\rangle$, they cannot be measured without being disturbed, and whatever procedure is used to transmit them faithfully to the receiver cannot also leave a faithful copy behind with the sender, because that would violate the no-cloning theorem. Indeed, since nonorthogonal source states cannot be distinguished reliably even by the sender, one may wonder what it means to transmit them reliably. Benjamin Schumacher[1,5] defined the *fidelity* of quantum transmission as the expectation of $|\langle\psi_i|\psi_i'\rangle|^2$ over channel inputs ψ_i and outputs ψ_i'. Fidelity is the expectation for the channel output to pass a test for being the same as the input, conducted by someone who knows what the input was.

Because of the fragility of nonorthogonal states, it might appear that the only way to transmit them faithfully is not to interact with them at all, but merely to let them pass undisturbed from sender to receiver. In this case, no quantum data compression would be possible. Schumacher has shown,[1,5] however, that quantum data-processing operations can be used to compress signals from any redundant quantum source and later regenerate them



QUANTUM DATA COMPRESSION. A unitary operation U_N on N unknown qubits from a known nonorthogonal source ensemble (here photons of random $|\leftrightarrow\rangle$ or $|\nearrow\rangle$ polarization) concentrates most of the quantum information into some of the qubits, allowing others to be safely discarded. At the receiving end of the channel, the discarded qubits are replaced by standard ones (here, 22.5° polarized photons corresponding to the major eigenvector of the source's density matrix) and the unitary operation is undone, resulting in a very good, but slightly entangled, approximation to the original input state. (The blue tints indicate entanglement.) FIGURE 2

from the compressed representation with asymptotically perfect fidelity. The means of doing so is shown schematically in figure 2, for the source S emitting $|\leftrightarrow\rangle$ and $|\nearrow\rangle$ with equal probabilities.

This source has a peculiarly quantum kind of redundancy consisting not in unequal probabilities of its signals, nor in correlations between signals emitted at different times, but rather in the fact that the two signals are nonorthogonal, and thus not wholly distinct as physical states. The redundancy of this source is reflected in its density matrix, $\rho = \frac{1}{2}(|\leftrightarrow\rangle\langle\leftrightarrow| + |\nearrow\rangle\langle\nearrow|)$, which has two unequal eigenvalues, $\lambda_{max} = \cos^2(\pi/8) \approx 0.854$, and $\lambda_{min} = \sin^2(\pi/8) \approx 0.146$, with respective eigenvectors in the 22.5° and 112.5° polarization directions, giving the mixture a von Neumann entropy $H(\rho) = -\mathrm{Tr}(\rho \log_2 \rho) \approx 0.601$ bits per photon, or about 0.399 bits per photon less than if the two signal states had been orthogonal. To exploit the source's redundancy, a block of N photons from the source is unitarily transformed (by U_N) into a basis of products of eigenvectors of ρ, arranged in order of decreasing eigenvalue from λ_{max}^N to λ_{min}^N, and approximately $[1 - H(\rho)]N$ of the highest order photons are discarded. These photons contain little information, being polarized in the 22.5° direction with high probability. By contrast, the low-order photons, which are retained, contain almost all the information of the original state, and would appear almost entirely depolarized if examined individually.

At the receiving end of the channel, the discarded photons are replaced by pure 22.5° photons, and the unitary transformation U_N is undone, resulting in an almost pure output state that approximates the N-photon input state with fidelity approaching 1 in the limit of large N. The technique just described works for arbitary quantum sources, efficiently compressing them to a number of qubits approaching their von Neumann entropy with fidelity approaching 1 in the limit of large N. Of course, faithful transmission of nonorthogonal states requires that the encoding and decoding be performed in a coherent quantum fashion, by an apparatus that retains no information about which states have passed through.

Teleportation and superdense coding

Quantum data compression optimizes the use of one channel resource—transmitted qubits—but it is possible to transmit an unknown quantum state with perfect fidelity without sending any qubits at all, if the sender and receiver have at their disposal two other resources:

▷ the ability to send classical messages, and

▷ entanglement, in the form of maximally entangled EPR pairs of particles previously shared between sender and receiver.

In this process, known as quantum teleportation,[6] the sending of two classical message bits and the using up of the entanglement in one separated pair of EPR particles suffices to convey the state of an arbitary qubit from sender to receiver. (See figure 3.) In more detail, the sender (Alice) takes particle 1 whose unknown state ξ is to be teleported, and performs a joint measurement on it and particle 2, one member of the EPR pair. Particles 2 and 3 have been prepared beforehand in a maximally entangled EPR state, such as $\Phi_{23}^+ = (|\leftrightarrow\rangle_2|\leftrightarrow\rangle_3 + |\updownarrow\rangle_2|\updownarrow\rangle_3)/\sqrt{2}$. The measurement on particles 1 and 2 projects them onto the so-called Bell basis, consisting of $\Phi_{12}^\pm = (|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2 \pm |\updownarrow\rangle_1|\updownarrow\rangle_2)/\sqrt{2}$ and $\Psi_{12}^\pm = (|\leftrightarrow\rangle_1|\updownarrow\rangle_2 \pm |\updownarrow\rangle_1|\leftrightarrow\rangle_2)/\sqrt{2}$, four orthogonal maximally entangled states. The Bell measurement generates two bits of classical data, and leaves particle 3, now held by Bob, in a residual state which can be unitarily transformed into a replica of the original quantum state ξ, which has been destroyed. Bob performs this transformation by subjecting particle 3 to one of four unitary operations ($\mathbf{1}$, σ_z, σ_x or σ_y) according to which of the four outcomes (Φ^+, Φ^-, Ψ^+ or Ψ^-) was obtained in the Bell measurement conducted by Alice. Teleportation may be said to split the complete information in particle 1 into a classical part, carried by the two-bit message, and a purely quantum part, carried by the prior entanglement between particles 2 and 3. It avoids both cloning (the state ξ is destroyed in particle 1 by Alice before it is re-created in particle 3 by Bob) and faster-than-light communication (the two-bit classical message must arrive at Bob before the replica can be created).

A closely related effect is superdense coding, a scheme devised by Stephen Wiesner.[7] (See figure 3.) Here, Bob encodes a two-bit classical message by performing one of four unitary operations on one member of a previously shared EPR pair, thereby placing the pair as a whole into a corresponding one of the four Bell states. The treated particle is returned to Alice, who by measuring it jointly with the untreated particle can recover both bits of the classical message. Thus the full classical information capacity of the two particles is made available, even though only one is directly handled by the sender.

If the term "ebit" is introduced for the quantum resource consisting of a shared pair of maximally entangled two-state particles, the following reductions among quantum and classical channel resources hold:

$$\begin{aligned} 1 \text{ bit} &\leq 1 \text{ qubit} \\ 1 \text{ ebit} &\leq 1 \text{ qubit} \\ 1 \text{ qubit} &\leq 1 \text{ ebit} + 2 \text{ bits} \\ 2 \text{ bits} &\leq 1 \text{ ebit} + 1 \text{ qubit} \end{aligned} \tag{1}$$

The ≤ signs mean that the resource on the left can be implemented by consuming the resource(s) on the right, but not necessarily vice versa. Thus, the first line of (1) means that a classical bit can be transmitted given the ability to transmit a qubit (for example, by restricting the qubit to two orthogonal states). The second line means that an ebit of shared entanglement can be created given the ability to send a qubit (for example, by having one observer prepare an EPR pair and send half of it to the other observer). The third and fourth lines represent the more complicated resource substitutions involved in teleportation and superdense coding. Note that ebits are an undirected resource, shared symmetrically between two remote parties, while qubits and bits have a definite direction, passing *from* a sender *to* a receiver.

Fast quantum computation

The most exciting development in quantum information processing has been Peter Shor's discovery[8] of quantum algorithms—for integer factorization and the discrete logarithm—that run exponentially faster than the best known classical algorithms. These algorithms take classical inputs (such as the number to be factored) and yield classical outputs (the factors), but obtain their speedup by using quantum interference among computation paths during the intermediate steps.

The obvious, direct way of trying to apply quantum parallelism to factor a large number N (say, a 200-digit number with no small factors) would be to try in parallel to divide it by all numbers less than $\sqrt{N}$. A quantum computer could indeed be programmed to do this, and one (or a few) of the paths of the superposition would indeed "solve" the problem immediately; but there is no known way to amplify this success, on an exponentially small fraction of the computation paths, into a non-negligible probability of success for the computation as a whole. (Loosely speaking, attempts to read off the answer by measuring the computer's state would almost certainly yield one of the unsuccessful paths and hence no information about the factors.) Instead, Shor reduced the problem of factoring N to another problem—finding the period of a periodic function—and used quantum techniques to solve this latter problem. Since this is the heart of the new quantum algorithms, we describe it here, omitting the details of how it in turn leads to a solution of the factoring problem.

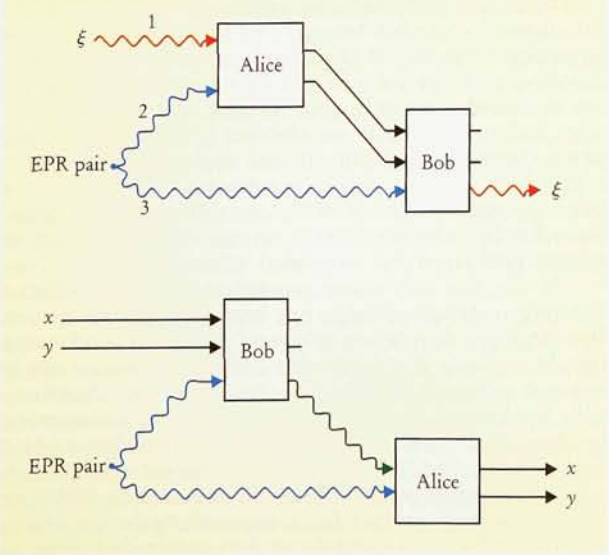
In brief, Shor's technique for finding the period of a periodic function consists of evaluating the function on a superposition of exponentially many arguments, computing a parallel Fourier transform on the superposition, then sampling the Fourier power spectrum to obtain the function's period.

In more detail (see figure 4), the quantum computer is prepared with two quantum registers, X and Y, each consisting of a string of qubits initialized to the Boolean value zero. The X register is used to hold arguments of the function f whose unknown period r is sought, and the Y register is used to store values of the function. The width w of the X register is chosen so that its number of possible Boolean states, $Q = 2^w$, is comfortably greater than the square of the anticipated period r. The Y register is made sufficiently wide to store any value of the function f. The initial state of the two quantum registers together is $|x, y\rangle = |0, 0\rangle$.

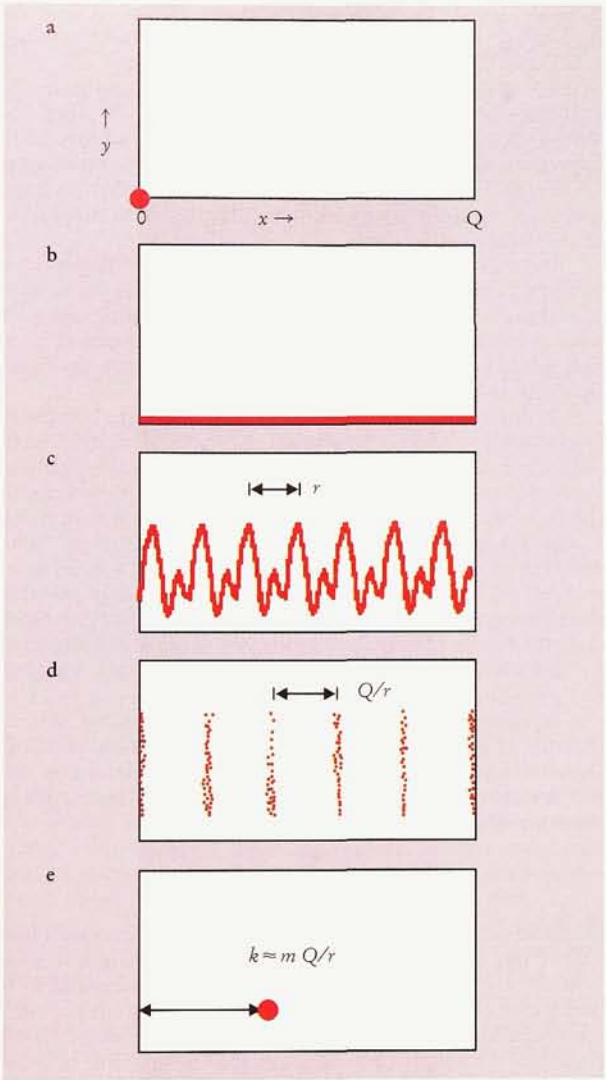
In the first stage of quantum computation, the X register is placed into a uniform superposition of all Q Boolean states. This can be done by performing a 45° rotation on each of its w qubits individually. The resulting superposed state,

$$\frac{1}{\sqrt{Q}} \sum_x |x, 0\rangle$$

is shown schematically in the figure as a horizontal band spread out over all possible x values but having a unique y value, $y = 0$. Next, a classical reversible computation is performed on all elements of the superposition in parallel, incrementing the Y register by f of the value in the X register. Although this computation is classical, it must be performed by a quantum computer, so that the above superposition of inputs is coherently transformed into the corresponding superposition of outputs. (For more on reversible computation, see the article by Rolf Landauer



QUANTUM TELEPORTATION AND SUPERDENSE CODING. Quantum teleportation (top) uses a two-bit classical message (solid lines) and an entangled EPR pair of particles to disembody an unknown quantum state ξ from one particle and reincarnate it in another. Quantum superdense coding (bottom) reliably transmits two classical bits (x,y) through an entangled pair of particles, even though only one member of the pair is handled by the sender. FIGURE 3



SHOR'S SUPERFAST QUANTUM FOURIER SAMPLING uses quantum interference to measure the period r of a periodic function f. The period may be exponentially greater than the number of qubits involved in the computation. **a:** The computer starts in the state $|x, y\rangle = |0, 0\rangle$. **b:** The x-register is put into a superposition of all possible values from 1 to $Q = 2^w$. **c:** The value $f(x)$ is computed in the y register simultaneously for all x values. **d:** A Fourier transform of the x register is performed. **e:** Measuring x yields a result k from which the period r can be deduced. FIGURE 4

in PHYSICS TODAY, May 1991, page 23.) The resulting output state is

$$\frac{1}{\sqrt{Q}} \sum_x |x, f(x)\rangle$$

and the schematic xy plane contains a graph of the periodic function f. (In the case of factoring, the function will not be continuous like the function in the figure.) Since the unknown period r is less than $\sqrt{Q}$, the graph includes at least $\sqrt{Q}$ complete periods. The graph ends with an incomplete period, except in the unlikely event that Q is exactly divisible by r.

In the next stage, a discrete Fourier transform is performed on the X register, resulting in the state

$$\frac{1}{Q} \sum_{x,k} e^{2\pi i k x/Q} |k, f(x)\rangle$$

This superposition includes terms with various y values, but the x values are strongly concentrated near multiples of the fundamental frequency Q/r. Finally, a single sample point in this Fourier power spectrum is obtained by classically measuring the state in the X register. The result, k, is an integer very close to some multiple of the fundamental frequency Q/r, typically so close that the desired r can be found unambiguously as the numerator of the closest rational approximation to Q/k with a denominator less than $\sqrt{Q}$.

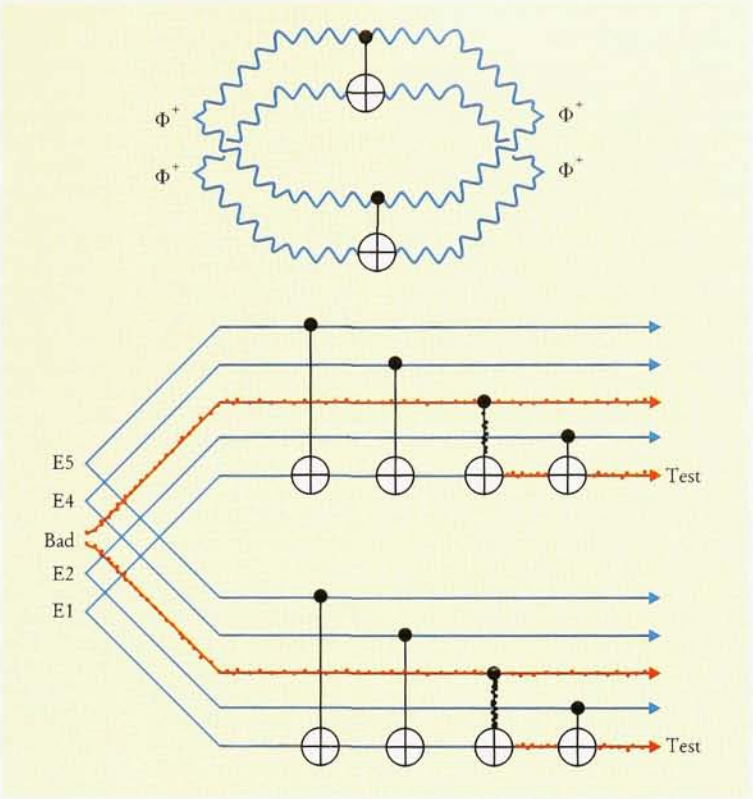
Each of the steps before the final measurement is unitary, and each can be economically implemented as an appropriate sequence of one- and two-qubit quantum operations of the kind considered earlier. In particular, the Fourier transform

$$\frac{1}{\sqrt{Q}} \sum_{x,k} |k, y\rangle\, e^{2\pi i k x/Q}\, \langle x, y|$$

is a transformation between orthonormal bases, implementable[9] by $O(w^2)$ XORs and rotations by angles of the form π, $\pi/2$, $\pi/4$, $\pi/8$, ...

The use of Fourier sampling to find an unknown period is analogous to the use of x-ray or neutron diffraction to measure the lattice constant of a crystal. This suggests that factoring might be reduced to an experiment in classical wave optics, which in turn could be simulated on an ordinary nonquantum computer. The critical difference is that a crystal's periodicity exists in real space, and therefore cannot be exponentially larger than the interatomic spacing or the wavelength of radiation used to measure the period. In quantum factoring, the period can be found efficiently even though it is exponentially large and exists only in an abstract space. If translated into a diffraction problem in real space, the factoring of a 200-digit number would correspond to measuring a lattice constant of about 10^{200} Å by diffracting 1-Å radiation off a 10^{400}-Å-wide crystal, an experiment that can be neither performed nor simulated efficiently.

So far, the only other natural problem for which a dramatic quantum speedup has been found is the discrete logarithm problem (given integers b, m and y, find x such that $b^x \bmod m = y$), a problem that, like factoring, can be reduced to period-finding. No fast quantum algorithms have been found for other famous search or optimization problems, such as the traveling salesman problem and the large class (called NP-complete) of problems equivalent to it. These problems, like the naive approach to factoring, can be cast as searches for a successful solution among exponentially many candidates; but unlike factoring, no



DISTILLING GOOD EPR PAIRS from mostly good ones. Top: Corresponding members of two EPR pairs of the Φ^+ type can be locally XORed together without disturbing the state of either pair. The symbol for the XOR gate indicates that for Boolean states (0s and 1s) the upper particle's state is unaltered while the lower particle is output in the XOR ($\oplus$) of the two input states. For superpositions the XOR can alter the state of both particles. Bottom: A "bad" (that is, random, non-EPR) pair contaminates the good pairs it interacts with, permitting bad pairs to be found efficiently without sacrificing all the good pairs. (For greater visual clarity, the qubits are denoted here by straight rather than wavy lines). FIGURE 5

way is known of transforming them into problems with a periodic structure amenable to detection by quantum interference.

Error, decoherence and eavesdropping

Both classical and quantum information are subject to errors during storage, transmission and processing. In a classical setting, techniques such as error-correcting codes and dissipative signal restoration (for example, circuits that restore distorted voltages toward their nominal digital values) have proved so effective at preventing or correcting errors that errors are no longer a major problem. The practical limits of classical digital computation are set by time and memory requirements, not by doubts about whether the results will be correct.

In quantum computers, as with classical analog computers, the space of legitimate states is continuous. There is thus no automatic way of detecting or correcting errors caused, for example, by slightly wrong initial conditions or slightly wrong parameters of one of the unitary transformations.

A far more serious and distinctively quantum kind of error is decoherence, the randomization of a quantum system's state that occurs when the system becomes entangled with its environment. (See the article by Wojciech Zurek, PHYSICS TODAY, October 1991, page 36.) Such entanglement is inevitable whenever

▷ a quantum computer attempts to reliably store or process nonorthogonal states, and

▷ the interaction with the environment allows some information about the computer's state to leak out into the environment.

If the environmental variables are then discarded or ignored, the computer's state will appear to have irreversibly decayed from its initial pure quantum superposition into a probabilistic classical mixture. Therefore, if quantum computations are to be performed in the laboratory, one must find or build systems that decohere slowly compared to the time required to do the computation. This will not be easy, as decoherence occurs on a time scale corresponding to the time required for significant information, even one bit, about the original quantum state to leak out into the environment. Most macroscopic systems decohere so rapidly as to make quantum interference effects practically unobservable.

The fragility of quantum information toward external interactions, which impedes the construction of quantum computers, is put to postive use in the art of quantum cryptography. The sender and receiver of a classical message as a rule cannot know whether it has been read en route by a third party. By contrast, with quantum information, eavesdropping and noise are not separate processes, but rather two consequences of entanglement between outside systems and the quantum data en route from sender to receiver. The technique of quantum cryptographic key distribution,[10] now in use over fiber-optic channels several kilometers long,[11] depends on having the sender and receiver engage in a circumspect public discussion of quantum data sent through an insecure quantum channel connecting them. The aim of the public discussion is to assess the noisiness of the quantum channel, infer from that an upper bound on the potential amount of eavesdropping, and, if this upper bound is not too great, use classical mathematical techniques to distill a body of certifiably secret shared classical data (a cryptographic key) from the sent and received versions of the quantum transmission. In other words, the technique uses classical post-processing to distill good (and secret) classical data from slightly noisy (and therefore potentially slightly nonsecret) quantum data. (See PHYSICS TODAY, November 1992, page 21.)

Similar techniques,[12] involving quantum post-processing of the quantum data, can be used to distill good entanglement from slightly noisy entanglement. (See fig-

ure 5.) Note first that if the quantum XOR operation is applied to respective members of two perfectly entangled Φ^+ pairs, the output is again two perfect Φ^+ pairs. But if either of the input Φ^+ states is replaced by a random unentangled pair of particles, the other is partly randomized, so that *neither* output pair remains a perfect Φ^+. The bottom part of figure 5 suggests how repeated XORs could be used to test a large batch of good Φ^+ pairs for the presence of a few bad ones. One of the pairs (say, $E1$) would be selected as target and the others successively XORed into it, the XORs as before being applied locally to corresponding members of each pair. If one of these pairs (say, $E3$) were bad, then $E1$ would have a significant chance of being spoiled. Therefore, if the two spins of the target pair were measured and found to exhibit correct Φ^+ correlations (say, giving identical outcomes for a $|\leftrightarrow\rangle$-vs-$|\updownarrow\rangle$ measurement), our confidence in the correctness of the remaining pairs $E2$, $E3$ and so on would be somewhat increased, even though the target pair $E1$ itself had been sacrificed. By repeated, systematic tests of this sort, a small yield of arbitrarily good EPR pairs could be distilled when as many as $\frac{2}{3}$ the original pairs have been depolarized.

An important achievement of classical information theory is the ability to transmit classical data reliably through a noisy channel. There is no evident direct way of doing the quantum analog of this, in other words of encoding an unknown quantum state so as to allow it to be recovered faithfully after transmission through a noisy quantum channel. (Schumacher's quantum data compression theorem, it will be recalled, deals with efficient quantum data transmission through a *noiseless* channel.) Nevertheless, the same goal can be achieved indirectly,[12] by combining teleportation with the entanglement purification procedure sketched above. Suppose Alice has an unknown quantum state ξ that she wishes to send to Bob, but only a noisy quantum channel to send it through. Instead of sending ξ directly, she uses the noisy channel to share a number of EPR pairs with Bob, then purifies the resulting noisy EPR pairs to obtain a smaller number of good ones. Finally, she uses one of the good EPR pairs, along with a classical message, to teleport the unknown state to Bob.

Experimental possibilities

Except for quantum cryptography, the above feats of quantum information processing require controlled, coherent interactions among quantum information carriers at some time between their initial preparation and final measurement. Quantum factoring is particularly demanding, requiring many thousands of coherent two-qubit operations to factor numbers that would not also be easy to factor by classical methods. The ability to perform long sequences of such operations, or even to store quantum data accurately, is, as noted above, threatened by errors, and especially by decoherence. William Unruh[13] has calculated rates of decoherence due to interactions with a thermal radiation field, and has estimated that the joint state of n quantum particles decoheres n times faster than that of a single particle, even when the particles are merely being used to store quantum data without processing it. Landauer[14] has noted some other obstacles to coherent quantum computation. Nevertheless, fairly complex manipulations of quantum states are routinely performed in experimental systems such as nuclear magnetic resonance and spectroscopy of atoms and ions, although not for explicit information processing purposes.

Among the more promising systems proposed for an actual quantum computer are excited electronic states of neutral atoms interacting with high-finesse microwave[15,4] or optical[16] cavities, nuclear spins[2] and trapped ions.[17] The goal in each case is to obtain a favorable ratio of decoherence time to switching time, that is, the time required to perform elementary unitary manipulations of the quantum data. In many of these systems, the ratio of decoherence time to switching time for a single information carrier is quite respectable. For example, nuclear spins can be manipulated in milliseconds, yet retain their phase coherence for minutes under favorable conditions. Perhaps the most difficult challenge facing designers of quantum information processing experiments is to achieve a strong, controlled interaction between quantum information carriers, for example between two nuclear spins brought into proximity by an atomic force microscope, or two atoms coupled through photon modes of a high-finesse cavity, while keeping these same carriers well enough isolated from their macroscopic environment to avoid rapid decoherence.

Recent rapid progress in laser cooling and thermal isolation, reflected for example in the achievement of a gaseous Bose–Einstein condensate (see PHYSICS TODAY, August, page 17), suggests that it will indeed be feasible to maintain such isolation long enough to perform at least a few steps of coherent quantum processing on at least a few qubits of quantum information. Even if such modest-sized quantum computations become feasible, it appears likely that error will remain a serious problem limiting the scale of computations that can be performed, not a problem that can be definitively solved for all practical purposes, as has been the case for classical computers.

I thank Gilles Brassard, Rolf Landauer, Artur Ekert, Sandu Popescu, Benjamin Schumacher, John Smolin, and especially David DiVincenzo and William K. Wootters for exciting collaborations, discussions of their own work and helpful advice.

References

1. B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
2. D. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
3. A. Barenco, D. Deutsch, A. Ekert, R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).
4. T. Sleator, H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
5. R. Jozsa, B. Schumacher, J. Modern Optics **41**, 2343 (1994).
6. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
7. C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
8. P. W. Shor, Proc. of the 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, Calif. (1994), p. 124. A. Ekert, R. Jozsa, "Shor's quantum algorithm for factorising numbers," preprint, Dept. of Mathematics and Statistics, Univ. of Plymouth, Plymouth, Devon, UK (1995).
9. D. Coppersmith, "An approximate Fourier transform useful in quantum factoring," IBM Research Report RC19642, T. J. Watson Research Center, Yorktown Heights, N.Y. (1994). R. Cleve, "A note on computing Fourier transforms by quantum programs," preprint, Dept. of Computer Science, Univ. of Calgary, Calgary, Alberta, Canada (1994).
10. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992).
11. For a review, see J. D. Franson, Opt. and Photonics News **6**, 30 (March 1995).
12. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W. K. Wootters, "Purification of Noisy Entanglement, and Faithful Teleportation via Noisy Channels," preprint, IBM T. J. Watson Research Center, Yorktown Heights, N.Y. (1995).
13. W. Unruh, Phys. Rev. A **51**, 992 (1995).
14. R. Landauer, Trans. R. Soc. London (to appear).
15. L. Davidovich, N. Zagury, M. Brune, J. M. Raimond, S. Haroche, Phys. Rev. A **50**, R895 (1994).
16. P. Berman, ed., *Cavity QED, Advances in Atomic, Molecular, and Optical Phys., Suppl. 2*, Academic, New York (1994).
17. J. I. Cirac, P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995). ■