Quantum Information

Luiz Davidovich

Abstract

The following article is based on the plenary address by Luiz Davidovich (Federal University of Rio de Janeiro), presented on April 14, 2004, at the 2004 MRS Spring Meeting in San Francisco. The field of quantum information is a discipline that aims to investigate methods for characterizing, transmitting, storing, compressing, and computationally utilizing the information carried by quantum states. It owes its rapid development over the last few years to several factors: the ability, developed in several laboratories, to control and measure simple microscopic systems; the discovery of fast quantum algorithms; and the recognition that Moore's law will soon lead to the single-atom limit of elementary computing gates. Cryptography and quantum computing are among the main applications in the field. They rely on the subtle and fundamental properties of the quantum world: the unavoidable disturbance associated with measurement, the superposition principle, and the nonlocal properties of entangled states. Progress in this area is intimately connected to a deep understanding of quantum physics: recent achievements include the experimental demonstration of teleportation and detailed investigations of the role of the environment in the quantum–classical transition. This article reviews basic concepts and recent developments in the field of quantum information, emphasizing the close ties between fundamental research and possible applications.

Keywords: *cryptography, decoherence, quantum computers, quantum information, teleportation.*

As ever greater numbers of bits are crammed into smaller and smaller volumes to increase the memory and computing capacity of digital computers, we must consider the ultimate end of such cramming. What happens when bits get so small that they consist of a single atom? At this scale, quantum effects become significant, and the life of a bit becomes much more complex. Instead of existing in either a 0 or a 1 state, a quantum bit, or "qubit," can exist in both states at the same time—a concept called "superposition." While such an indeterminate state would seem to rule out the use of qubits for practical computing purposes, scientists have shown that quantum computers consisting of only a few hundred atoms could perform massive parallel computations of great significance to the fields of cryptography, database searching, and modeling of complex real-world systems such as an ensemble of atoms undergoing a phase transition. Practical algorithms already exist to take advantage of quantum computing systems; what remains is to solve the problems of assembling a working quantum computer.

The following articles by Luiz Davidovich and Bruce E. Kane shed light upon the world of quantum information from two different angles. Davidovich discusses the theory of quantum computing in detail to show the possibilities of the technology, including encryption and teleportation of data. Through insightful explanations of basic concepts and lively examples of encrypted communications, he gives us an overview of the field.

Kane, on the other hand, looks at the materials challenges involved in implementing a quantum computing device. He shows that while solid-state qubits based on doped silicon are theoretically possible, their implementation may prove to be extremely challenging. The inherent variability of devices made by solid-state processing techniques may prevent the positioning of a single atom of phosphorus on a silicon lattice with the atomic-level precision necessary for quantum computation. Still, micropositioning or self-assembly techniques that have yet to be developed may solve this problem.

Together, these two articles provide the theoretical and practical bases for understanding possible materials solutions to the challenge of quantum computing.

—Eds.

Introduction

In 1952, Erwin Schrödinger, one of the founders of quantum mechanics, wrote in *The British Journal for the Philosophy of Science*:

> "One never realizes experiments with a single electron or an atom or a small molecule. In thought experiments, one assumes that sometimes this is possible; invariably, this leads to ridiculous consequences….One may say that one does not realize experiments with single particles, more than one raises ichthyosaurs in the zoo."[1]

Fifty years after this prediction, single electrons and atoms (see Figure 1) are being isolated and studied in several laboratories around the world.[2] New techniques, often known by the term quantum technology, allow the manipulation and control of these systems. This technology relies on the subtle properties of the quantum world to store and transmit information and to implement quantum algorithms that may lead to exponentially faster computation than is currently possible with classical machines.

Several motivations drive the development of this area of research. The control of single atoms and photons offers an interesting prospect for the investigation of fundamental aspects of quantum mechanics, involving, for instance, the behavior of microscopic systems under continuous monitoring and the properties of "entangled" states. These states exhibit one of the most subtle aspects of quantum mechanics: two systems that have interacted in the past remain correlated in such a way that, even though their global state is well-defined, the individual state of either system is undetermined. However, measurement of the state of one of the systems determines the state of the other one, even if the two systems are far apart.

To illustrate, suppose that "Alice" and "Bob" share two photons with entangled polarizations that are random but identical. When Alice measures the polarization of the photon in her possession to check if it is horizontal or vertical, there is a 50% chance for each result. The same is true for Bob's photon. However, entanglement assures that both photons will always be found with identical polarizations. Before measurement, each photon does not have a well-defined polarization. The global property specified by the entangled state implies that a measurement will find both photons with the same polarization.

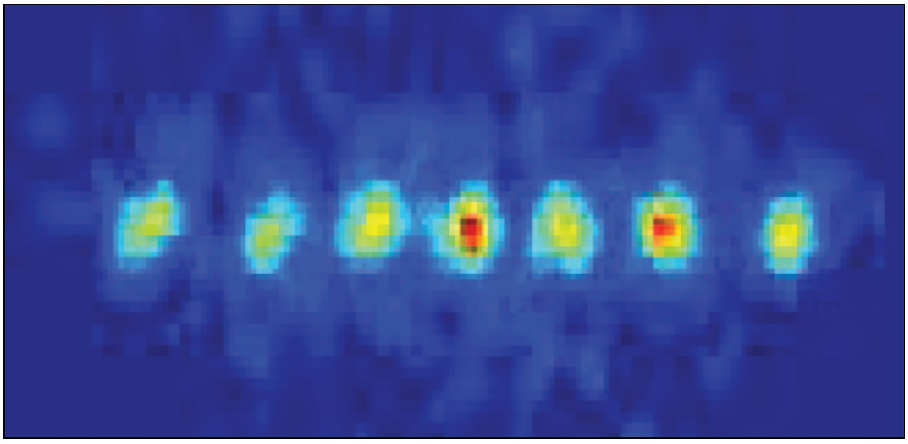

Figure 1. Optical photograph of seven ions in a harmonic trap built by Rainer Blatt's group at the University of Innsbruck. The average ion distance is 14 μm. The image was taken with a slow-scan-intensified CCD camera, which allows for exposure times as short as 5 ns with a repetition rate of up to 10 kHz. This frame is part of a video that can be found at http://heart-c704.uibk.ac.at/oscillating_ions.html. (Courtesy Rainer Blatt, University of Innsbruck.)

The property of entanglement has been known for a long time.[3] New insights on this intriguing quantum property have been obtained, however, in recent years.[4] They have led to the development of quantitative laws[4] and to the discovery of new communication schemes, like the teleportation of quantum states, which will be discussed later in this article.

Meanwhile, the exponential growth in the number of transistors in the central processing units of computers, as predicted by Gordon Moore in the 1960s, implies that the number of atoms needed to codify a single bit of information is cut in half in a period of approximately two years. This progression would lead us, around 2015, to a regime in which each bit of information will be stored in a single atom, which would imply the saturation of Moore's law (although, even before that point, the exponentially mounting costs of chip production may be a strong deterrent to continued progress along this line). As the single-atom limit is approached, it becomes natural to think of using the quantum properties of the atoms to implement new computational algorithms that would allow the increase of the processing speed, despite the saturation of Moore's law.

In 1994, Peter Shor, then a researcher at AT&T, found a quantum algorithm for the factorization of a number into prime factors that was much faster than the best classical algorithm known to date.[5] The time it takes a classical computer to factor a number increases exponentially with the length L of the number. This is the reason why factorization of large numbers is the basis of the RSA public key encrypting system, named after River, Shamir, and Adler, who invented this system in 1977. It is used, for instance, in Internet transactions. Shor demonstrated that a quantum computer—that is, a computer that employs the laws of quantum mechanics to implement its calculations—could factor a large number in a time that would increase only quadratically with the length L of the number, that is, as L^2. Therefore, building such a computer would realistically allow one to break encryptions based on factorization.

In 1997, Lov Grover showed that a quantum computer could make a database search with a quadratic gain in speed with respect to a classical computer search.[6]

Even before that, Paul Benioff[7] and Richard Feynman[8] in 1982, and David Deutsch[9] in 1985 had discussed the possibility of building a quantum mechanical computer. Recent contributions have proposed the use of quantum computers for the simulation of interesting physical systems, like an ensemble of atoms undergoing phase transitions, allowing in this case an exponential gain in the computation speed with respect to classical computers.

The interconnection between basic and applied research permeates the field of quantum information. The subtle properties of the quantum world have found new applications, like quantum cryptography, that go beyond the realm of quantum computers.

In the following, I will discuss some peculiar features of quantum mechanics and show their relevance for quantum computation and quantum cryptography.

Peculiarities of Quantum Information

Classical computers codify information by means of a sequence of bits in one of two states, 0 or 1. In quantum computers, this codification is made through quantum bits, or "qubits," that can be in a superposition of two states.

A qubit can be physically realized through, for instance, the spin of an electron or the polarization of a photon. For an electron, the "spin up" and "spin down" states correspond to the states 0 and 1, while other directions of the spin correspond to superpositions of these two states (in the same way that a vector in three-dimensional space can be written as a superposition of the basis vectors). For a single photon, the horizontal (H) and vertical (V) polarizations along a given set of axes would correspond to the states 0 and 1 of the qubit. Other directions of polarization would correspond to superpositions of these states. Since photons are never at rest, we refer to them as "flying" qubits.

Classical information is robust in the sense that it can be stored (for instance, a bit can be stored in a capacitor, which corresponds to the state 1 when charged and to the state 0 when discharged), read, and copied without being destroyed. These simple properties do not hold for quantum information.

In order to illustrate the special features of quantum information, let us consider a qubit based on the polarization of a single photon.

The polarization of light can be measured by polarizers: the intensity of the transmitted light depends on the orientation of the axis of the polarizer with respect to the direction of polarization of the light beam, maximum transmission being obtained when the axis of this measuring device is parallel to the polarization of the beam. For an arbitrary angle θ between the polarization of light and the axis of the polarizer, the corresponding transmitted intensity I_θ is given in terms of the maximum intensity I_0 by $I_\theta = I_0 \cos^2 \theta$ (this expression is known as Malus's law in classical optics). By rotating the polarizer, and measuring the intensity of the transmitted light, one is thus able to determine the direction of the polarization of the incident light. If the axis of the polarizer does not coincide with the direction of light polarization, this polarization is changed by the measurement: indeed, the emerging light becomes polarized along the polarizer's axis.

The peculiarities of quantum information come in when one considers what happens with single photons. These entities cannot be split: a single photon is either transmitted or absorbed. In this case, the orientation of the axis of the polarizer with respect to the polarization of the photon will determine the probability that the photon is

transmitted. For an ideal polarizer, a photon will certainly be transmitted if it is polarized along the axis of the polarizer, and it will not go through if its polarization is orthogonal to that axis. For polarizations forming an angle θ with the axis of the polarizer, the probability of transmission of each photon is given by $\cos^2\theta$. Thus, for an angle $\theta = 45°$, the photon has a 50% chance of being transmitted (since $\cos^2 45° = 1/2$).

Malus's law for classical light is recovered from these considerations: if one considers a large number of identical photons hitting the polarizer, the fraction of transmitted photons, and therefore the intensity of the transmitted beam, must be proportional to $\cos^2\theta$. In contrast, the transmission of an unpolarized light beam—for which the photons have random polarizations—does not depend on the orientation of the polarizer. Once a photon goes through, one knows its polarization after it is transmitted (it should be along the polarizer axis).

However, for a single entity, one does not have any way of finding out what its polarization was before it hit the polarizer. Indeed, if a photon goes through, this does not mean that its polarization was parallel to the axis of the polarizer: the photon has a probability of being transmitted for any polarization not orthogonal to that axis. This means that it is impossible to measure the polarization state of a single photon. Also, if we do not know *a priori* the direction of polarization of a photon, measurement along any other non-orthogonal direction changes the state of the photon. This unavoidable change in the state of a system upon measurement is an essential feature of quantum mechanics.

Furthermore, the state of a single photon cannot be copied. This is the so-called *no-cloning theorem*.[10] Note that if the state could be copied, one would be able to measure it, since one could then build a macroscopic photon beam and measure its polarization by changing the orientation of the axis of the polarizer and verifying for which orientation one would achieve maximum transmission.

This discussion may help one to understand the special role played by the superposition principle in quantum mechanics. When one says that the state of a photon with a 45° polarization is a superposition of two states corresponding to horizontal and vertical polarization, this is quite different from saying that we are not sure whether the photon has horizontal or vertical polarization, there being a 50% chance for each of these two orientations. This last statement, which corresponds to a classical probabilistic description, would imply a complete statistical uncertainty about the state of polarization of the photon (and, therefore, an unpolarized light beam). In contrast, the quantum superposition describes a polarized photon. In the quantum jargon, one says that these two cases correspond to a pure quantum state and a statistical mixture, respectively. The difference between them can be tested experimentally by changing the orientation of a polarizer placed in front of the beam and verifying whether the transmitted intensity changes or not.

In the same way, a collection of spin-1/2 particles in a superposition of the spin-up and the spin-down states is quite different from a statistical ensemble of particles with spin-up or spin-down, which could be described as a collection of classical bits in the states 0 or 1.

These features of quantum information have an interesting application in quantum cryptography, as will be shown in the following section.

Quantum Cryptography

The bottleneck of cryptography is the safe distribution of the cryptographic key. A quantum mechanical protocol for sending a key was proposed in 1984 by Charles Bennett and Giles Brassard.[11] Suppose a sender (Alice again) wants to transmit a cryptographic key to a receiver (Bob). They use, for this purpose, photons polarized along two non-orthogonal bases, forming an angle of 45° with respect to each other and randomly chosen for each photon. Then they follow these steps:

1. Alice sends to Bob a sequence of photons corresponding to the two non-orthogonal bases, randomly chosen. Note that Alice makes, for each photon she sends, two random choices: first she chooses the basis, and then the polarization of the photon in the chosen basis ("horizontal" or "vertical," with respect to the axes of the basis). She carefully writes down the choices made for each photon.
2. Bob measures the polarization of each photon he receives, randomly using either one of the bases. In order to do this, he makes a random choice of the orientation of the axis of a polarizer in his possession, making it parallel to the "horizontal" axis of one or the other of the bases. He then writes down in his notebook whether the photon was transmitted or not (corresponding, respectively, to the photon having, after transmission, "horizontal" or "vertical" polarization in Bob's basis). This does not allow Bob to infer the polarization of the photon sent by Alice. If, for instance, the photon is transmitted through his polarizer, this does not imply that its polarization was parallel to the axis of the polarizer before detection, since if Bob's basis is forming 45° with respect to the basis used by Alice, the photon has a probability of one-half of being transmitted, independently of whether it is a "horizontal" or "vertical" photon in Alice's basis.
3. Alice and Bob compare their choices of bases through a public channel, and keep only the results corresponding to identical choices (approximately half of the results). For this subset of the data, Alice and Bob should agree on the polarization of each photon ("horizontal" or "vertical" with respect to the common basis): their data are perfectly correlated. They end up, therefore, sharing a random sequence of bits HHVHVV…, which can be used as a key to code and decode messages through public channels.

If a third party ("Eve") intercepts the qubits, measures them, and resends them to Bob, she necessarily disturbs their correlations, since whenever she uses a basis different from the one used by Alice she changes the polarization of the photon. This can be perceived by Alice and Bob, by publicly comparing (and throwing away afterwards) a sample of their data.

Note that essential properties of quantum mechanics are involved in this protocol. Indeed, if Eve could replicate the state of a single photon, she would then be able to send it to Bob without him noticing that the information was read.

Quantum cryptography has been demonstrated by several groups.[12] On April 21, 2004, the Mayor of Vienna transferred money from City Hall to Bank Austria Creditanstalt over a fiber-optic cable using a quantum "key" made of single photons to ensure that the transfer was completely secure.[13] Several companies have developed quantum cryptography prototypes, and the first products are now commercially available.[14]

Other proposals for quantum communication have relied on even more subtle properties of quantum mechanics. This will be shown in the next section.

Entanglement and Teleportation

Entangled states of flying qubits (photons) can be produced by shining ultraviolet laser light on a nonlinear crystal. Under the appropriate conditions, each photon of the incoming light generates a pair of entangled photons, produced simultaneously (and, for this reason, called "twin" photons). These two photons have orthogonal polarizations and satisfy the typical properties of entangled states: when the polarization of each photon is measured to check if it is horizontally or vertically polarized, there is a 50% chance of each result. However, the two photons are always detected with orthogonal polarizations. Once produced, these photons fly

apart (keeping, however, their quantum correlation).

In 1993, Charles Bennett and co-workers[15] showed that entangled states could be used to transport the quantum state of one qubit to another qubit. This was called by them "teleportation." In this process, the state of the first qubit is changed, so that the no-cloning theorem is not violated.

Suppose Alice wants to transmit the quantum state of a qubit to Bob. She has two serious problems. First, if she has just one qubit, she cannot possibly measure its state (remember that the state of a single entity, like a photon, cannot be measured). So, she must send information which is unknown to her. Second, even if she somehow knows the state (for instance, she could have produced the state herself), in order to transmit it to Bob she needs an infinite number of bits (since an arbitrary state of polarization of a photon, or an arbitrary direction of the spin of an electron, is described by angles, which are continuous numbers, requiring in general an infinite number of bits to be specified).

Successful teleportation can, however, be achieved with only two bits of information, transmitted by classical means (for instance, a telephone line), by letting Alice and Bob share a "quantum communication channel" consisting of an entangled pair of particles: Alice keeps one of the particles (particle A) while Bob keeps the other one (particle B). Here we will specify that these particles are photons.

In order to transmit the polarization state of her photon (let us call it photon X), Alice makes measurements on the pair of photons in her possession, A and X. She cannot simply measure the state of X: the outcome of the measurement would be different from the original state of X, since the measurement changes the state of the photon. Instead, she measures global properties of the two photons A and X. For instance, she may determine that the two photons in her possession have orthogonal polarizations. It turns out that there are four possible results for the quantum relations between the pair of photons kept by Alice (which can be classified by two bits of classical information: 00, 01, 10, and 11; for details, see Reference 15). She transmits the outcome of her measurement (one of the four possibilities) to Bob. After receiving this message, Bob applies a transformation to his photon, which depends on the result obtained by Alice. Each of the four possible outcomes corresponds to one of four possible transformations. One of them is, for instance, rotating the polarization of the photon by 90° (which can be done by letting the photon pass through an optical device called a half-wavelength plate). In Reference 15 it is shown that, after the proper transformation, the state of photon B coincides precisely with the original state of photon X (which has been changed by Alice's measurement). The quantum state of Alice's qubit is thus transferred to Bob, without either Alice or Bob knowing it! This scheme is sketched in Figure 2.

The first proposal for an experimental realization of teleportation[16] was in the field of cavity quantum electrodynamics, which deals with the interaction between atoms and photons in cavities with very low losses (in the microwave domain, they are able to keep a photon inside for a time period of up to a fraction of a second).[17] In this case, the quantum channel is an entangled state that describes a single photon in one of two cavities and no photons in the other. The state does not specify, however, which of the two cavities contains the photon. This quantum channel allows the teleportation of the state of an atom crossing the first cavity to a second atom, going through the second cavity.

Experiments on teleportation have been done by several groups.[18]

The Basic Blocks and the Requirements for Quantum Computation

In 1995, it was shown by DiVincenzo and co-workers[19] that any quantum computation can be reduced to combinations of two basic blocks: (1) single-qubit operations (for instance, rotating the spin of an electron by letting it precess around a magnetic field, or rotating the polarization of a photon by letting it pass through a half-wavelength plate), and (2) a special kind of two-qubit operation called a "controlled-NOT" gate. This operation involves an interaction between two qubits: the state of the second qubit (the target) is changed if and only if the state of the first qubit (the control) is 1 (see Table I). Implementation of this gate in physical systems is less trivial than the realization of single-qubit operations. One must look for specific interactions between two physical qubits that would accomplish this result. For instance, using techniques of nuclear magnetic resonance, it is possible to tailor the interaction between two spins in such a way that, if the first spin is up, the other is reversed, while the two-spin state does not change if the first spin is down (see, for instance, Reference 2).

Other kinds of two-qubit gates may also be used as basic building blocks, instead of the controlled-NOT gate (see accompanying article by Kane in this issue). Useful calculations in a quantum computer, like those needed to factor large numbers, would typically involve thousands of qubits and an equally high number of single- and two-qubit operations.

This represents a challenge to physicists and materials scientists, that of finding systems and materials that would allow the realization of these gates, with minimal errors and losses, for a large number of qubits

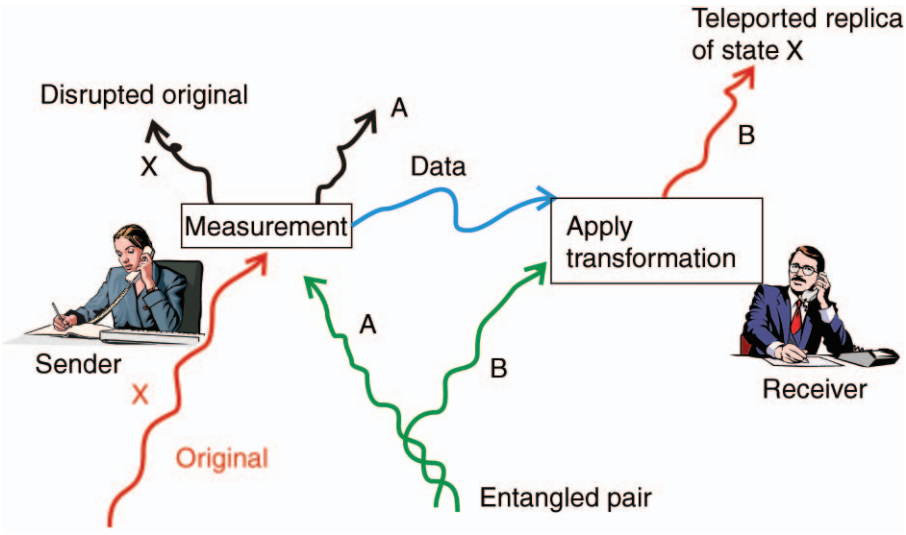

Figure 2. Quantum teleportation scheme (after Bennett[35]). A sender ("Alice") and a receiver ("Bob") share an entangled pair of qubits, marked A and B (green lines), used as a quantum communication channel. Alice makes two binary measurements on the pair (X,A) and sends the two bits of information to Bob, who then applies one out of four possible transformations (depending on the information he received from Alice) on his qubit, B, thus reproducing the state of qubit X.

Table I: Truth Table for the "Controlled-NOT" Gate.

Inputs		Outputs	
Control Qubit	Target Qubit	Control Qubit	Target Qubit
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Note: The state of the target qubit is changed if and only if the control bit is in state 1.

and operations. Suitable physical systems[20] would have to satisfy several requirements:
1. They should be scalable (that is, one should be able to increase the number of qubits without increasing exponentially the number of operations or resources needed to perform calculations), with well-characterized qubits. This means that they should contain a collection of two-level systems, like the ground and excited states of an atom, the two states of a spin-1/2 particle, or the horizontal and vertical polarization of a single photon. The requirement of scalability should be tested for each particular system. For instance, a proposal of quantum computation with photons interacting with optical elements must ensure that the number of mirrors, lenses, and detecting devices does not grow exponentially with the number of photons.
2. One should be able to initialize the state of the qubits by, for instance, putting all qubits in the 0 state at the start of the process.
3. Decoherence times should be much longer than the gate operation time. Decoherence times characterize the dynamics of any qubit—or more generally, any quantum system—in contact with its environment. The interaction of a quantum system with its environment transforms quantum superpositions into statistical mixtures, and qubits into classical bits, which implies that the quantum features of the system are lost.
4. They should allow the realization of a complete set of logic gates (for instance, operations on single qubits plus controlled-NOT gates).
5. They should allow individual measurement of the qubits.

One should also be able to convert stationary qubits to flying qubits, so that the results could be transported from one place to the other. The flying qubits should allow faithful transmission of the information.

Many systems have been proposed as possible devices for quantum computation, including trapped ions,[21] quantum dots,[22] Josephson junctions,[23] molecules in liquid solutions,[24] impurities in silicon,[25] and optical lattices.[26] Each of these systems has its own advantages and limitations.

Trapped ions offer the possibility of precise operations and easy measurement of the qubits, but may require a sophisticated, non-portable setup. In this case, the qubits correspond to two levels of the hyperfine structure of the ground state of the trapped ions. The long-lived nature of these states implies long decoherence times. Single-qubit operations are realized by applying laser fields to each ion, while two-qubit gates are produced by means of a collective vibration mode of the ions in the trap. Experiments demonstrating two-qubit gates have been realized recently.[27]

Molecules in liquid solutions, with their atomic spins manipulated through nuclear magnetic resonance techniques, have been used to demonstrate the factorization of the number 15 using Shor's algorithm,[24] but the signal-to-noise ratio decreases exponentially with the number of qubits.

Optical lattices have allowed the simulation of phase transitions for systems of spins,[26] but it is not known how an individual qubit could be addressed.

Josephson junctions allow the realization of robust qubits, but the demonstration of elementary gates lags behind other systems.

Quantum dots and impurities in silicon are certainly appealing to the semiconductor industry, and might lead to more portable systems. Advantages and limitations of these systems are discussed in the accompanying article by Kane in this issue.

A complete understanding of the scaling properties of these systems is far from being achieved and represents a considerable challenge for physics and materials science.

Decoherence, Quantum Computers, and the Quantum–Classical Limit

Fighting decoherence is a major concern in these implementations. As we have seen before, decoherence, which stems from the interaction between a qubit and its environment, transforms quantum superpositions into statistical mixtures. Therefore, under its action, quantum computers become classical.

Several strategies have been proposed to circumvent this obstacle, including quantum error correction,[28] decoherence-free subspaces,[29] and reservoir engineering.[30]

I concentrate here on quantum error correction, which is of more universal application than the other techniques. In classical computation, additional bits (like parity-checking bits) allow the correction of errors in strings of bits. In a similar way, quantum error correction relies on additional ancillary qubits. With a suitable sequence of quantum computations and measurements of these ancillary qubits, errors caused by decoherence can be detected and corrected. This procedure is successful as long as the decoherence time is 10^4-10^5 times larger than the time for the execution of an individual quantum gate.[31]

Decoherence is actually an important phenomenon in the emergence of the classical world from quantum mechanics.[32] It helps to explain why, while it is commonplace to have an atom in a superposition of two states, one does not see in the macroscopic world quantum superpositions of distinguishable states of the same object, like a body localized at two different positions at the same time or simultaneously alive and dead—the example known as Schrödinger's cat.[3] Decoherence transforms these superpositions into statistical mixtures within a very short time that decreases with the "macroscopicity" of the superposition.

The behavior of decoherence with the size of the system was investigated in the realm of cavity quantum electrodynamics.[33] A superposition of two distinguishable classical-like states (i.e., different phases) of the electromagnetic field in a cavity with very low losses is created by an atom that crosses the cavity, interacts with the field, and is detected afterwards. A second atom, sent through the same cavity, measures this state, allowing the differentiation between a quantum superposition and a statistical mixture of the two field states.

The study of the phenomenon of decoherence is therefore not only of practical importance, since it is a major obstacle for large-scale quantum computation, but it is also closely connected to fundamental questions of quantum mechanics.

Conclusions

Quantum information presents formidable challenges to physicists, mathematicians, computer and materials scientists, and engineers. It has the potential of leading to groundbreaking advances in sciences and engineering, including computation, communication, precision measurements,[34] and the foundational understanding of

quantum mechanics. The main aim of this field is to use quantum physics to dramatically enhance the acquisition, processing, and transmission of information.

Even though demonstrations of quantum cryptography and of quantum computing have already been implemented, we still have a long way to go before practical quantum computers are engineered. Major obstacles are the need to minimize the noise from the environment and of high precision in the realization of the elementary gates (error rate of $<0.01\%$). At present, it is not possible to assess whether these barriers are surmountable. It is not clear, either, which of the many systems being studied would lead the way in the realization of a quantum computer. However, in view of the high degree of experimental sophistication achieved in this field, it is quite reasonable to expect (as has been the case throughout the history of science) that we will witness in the future further and unexpected applications in this field.

Acknowledgments

This research is supported by the Brazilian agencies CNPq, CAPES, and FAPERJ, and the Brazilian Institute for Quantum Information.

References

1. E. Schrödinger, *Br. J. Philosophy Sci.* **3** (1952) p. 109.
2. See, for instance, *The Physics of Quantum Information*, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer, Berlin, 2000).
3. E. Schrödinger, *Naturw.* **23** (1935) pp. 807, 823, and 844. English translation by J.D. Trimmer, *Proc. Am. Phys. Soc*. **124** (1980) p. 3235; A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47** (1935) p. 777.
4. For a detailed review of this field, see, for instance, M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000), or the lecture notes by J. Preskill, available at http://www.theory.caltech.edu/people/preskill/ph229/ (accessed December 2004).
5. P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proc. 35nd Annu. Symp. on Foundations of Comp. Sci.* (IEEE Computer Society Press, 1994) p. 124; P.W. Shor, *SIAM J. Computing* **26** (1997) p. 1484.
6. L. Grover, *Phys. Rev. Lett.* **79** (1997) p. 325.
7. P. Benioff, *Phys. Rev. Lett.* **48** (1982) p. 1581.
8. R.P. Feynman, *Int. J. of Theor. Phys.* **21** (1982) p. 467; *Optics News* **11** (1985) p. 11.
9. D. Deutsch, *Proc. R. Soc. London, Ser. A* **400** (1985) p. 97.
10. W.K. Wootters and W.H. Zurek, *Nature* **299** (1982) p. 802.
11. C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing* (1984) p. 175.
12. For a review, see N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74** (2002) p. 145.
13. A. Poppe, A. Fedrizzi, R. Ursin, H.R. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, *Opt. Express* **12** (2004) p. 3865.
14. id Quantique SA home page, http://www.idquantique.com/; MagiQ Technologies home page, http://www.magiqtech.com/; NEC Corp. home page, http://www.nec.com/; Toshiba Research Europe Ltd. home page http://www.toshiba-europe.com/research/ (accessed December 2004).
15. C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, *Phys. Rev. Lett.* **70** (1993) p. 1895.
16. L. Davidovich, N. Zagury, M. Brune, J.M. Raimond, and S. Haroche, *Phys. Rev. A* **50** (1994) p. R895.
17. For reviews, see P. Berman, Ed., *Cavity Quantum Electrodynamics* (Academic Press, New York, 1994).
18. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Nature* **390** (1997) p. 575; D. Boschi, S. Branca, F. DeMartini, L. Hardy, and S. Popescu, *Phys. Rev. Lett.* **80** (1998) p. 1121; A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, *Science* **282** (1998) p. 706; M.A. Nielsen, E. Knill, and R. Laflamme, *Nature* **396** (1998) p. 52; I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, *Nature* **421** (2003) p. 509; M. Riebe, H. Häffner, C.F. Roos, W. Hänsel, J. Benhelm, G.P.T. Lancaster, T.W. Körber, C. Becher, F. Schmidt-Kaler, D.F.V. James, and R. Blatt, *Nature* **429** (2004) p. 734; M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D.J. Wineland, *Nature* **429** (2004) p. 737; R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, *Nature* **430** (2004) p. 849.
19. D.P. DiVincenzo, *Phys. Rev. A* **51** (1995) p. 1015; A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, *Phys. Rev. A* **52** (1995) p. 3457.
20. D.P. DiVincenzo, *Fortschritte der Physik* **48** (9–11) (2000) p. 771.
21. J.I. Cirac and P. Zoller, *Phys. Rev. Lett.* **74** (1995) p. 4091.
22. D. Loss and D.P. DiVincenzo, *Phys. Rev. A* **57** (1998) p. 120; A. Imamoglu, D.D. Awschalom, G. Burkard, D.P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, *Phys. Rev. Lett.* **83** (1999) p. 4204.
23. D.V. Averin, *J. Low Temp. Phys.* **118** (2000) p. 781; Y. Nakamura, Yu.A. Pashkin, and J.S. Tsai, *Nature* **398** (1999) p. 786; J.E. Mooij, T.P. Orlando, L. Levitov, L. Tian, C.H. van der Wal, and S. Lloyd, *Science* **285** (1999) p. 1036; I. Chiorescu, Y. Nakamura, C.J.P.M. Harmans, and J.E. Mooij, *Science* **299** (2003) p. 1869; Y. Makhlin, G. Schön, and A. Shnirman, *Nature* **398** (1999) p. 305; Y. Makhlin, G. Schön, and A. Shnirman, *Rev. Mod. Phys.* **73** (2001) p. 357.
24. N.A. Gershenfeld and I.L. Chuang, *Science* **275** (1997) 350; L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, *Nature* **414** (2001) p. 883.
25. B.E. Kane, *Nature* **393** (1998) p. 133.
26. D. Jaksch, C. Bruder, J.I. Cirac, C.W. Gardiner, and P. Zoller, *Phys. Rev. Lett.* **81** (1998) p. 3108; I.H. Deutsch, G.K. Brennen, and P.S. Jessen, *Fortschritte der Physik* **48** (2000) p. 925; M. Greiner, O. Mandel, T. Esslinger, T.W. Hänsch, and I. Bloch, *Nature* **415** (2002) p. 39.
27. F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G.P.T. Lancaster, T. Deuschle, C. Becher, C.F. Roos, J. Eschner, and R. Blatt, *Nature* **422** (2003) p. 408; D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W.M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D.J. Wineland, *Nature* **422** (2003) p. 412.
28. P.W. Shor, *Phys. Rev. A* **52** (1995) p. R2493; A.M. Steane, *Phys. Rev. Lett.* **77** (1996) p. 793; R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, *Phys. Rev. Lett.* **77** (1996) p. 198.
29. D.A. Lidar, I.L. Chuang, and K.B. Whaley, *Phys. Rev. Lett.* **81** (1998) p. 2594.
30. A.R.R. Carvalho, P. Milman, R.L. de Matos Filho, and L. Davidovich, *Phys. Rev. Lett.* **86** (2001) p. 4988.
31. See, for instance, J. Preskill, *Proc. R. Soc. London, Ser. A* **454** (1998) p. 384; E. Knill, R. Laflamme, and W.H. Zurek, *Science* **279** (1998) p. 342; and D. Aharonov, in *Annu. Rev. Comput. Phys. VI,* edited by D. Stauffer (World Scientific, Singapore, 1999).
32. For a review, see W.H. Zurek, *Rev. Mod. Phys.* **75** (2003) p. 715.
33. L. Davidovich, M. Brune, J.M. Raimond, and S. Haroche, *Phys. Rev. A* **53** (1996) p. 1295; M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J.M. Raimond, and S. Haroche, *Phys. Rev. Lett.* **77** (1996) p. 4887.
34. D. Leibfried, M.D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W.M. Itano, J.D. Jost, C. Langer, and D.J. Wineland, *Science* **304** (2004) p. 1476.
35. C.H. Bennett, seminar presentation. A similar diagram can be found at http://www.research.ibm.com/quantuminfo/teleportation/ (accessed December 2004).

Luiz Davidovich *is a professor of physics at the Federal University of Rio de Janeiro, Brazil. His research interests are in quantum optics and quantum information, including laser theory; the analysis of the role of decoherence in the quantum–classical limit; and proposals for the measurement of quantum states and the realization of quantum logic operations. He received an undergraduate degree in physics (1968) at the Pontifical Catholic University in Rio de Janeiro, and a PhD degree in physics (1975) from the University of Rochester, N.Y.*

Davidovich is a member of the Brazilian Academy of Sciences and the Third World Academy of Sciences (TWAS). He received the 2001 Physics Award from TWAS and the Grand Cross of Scientific Merit from the Brazilian government. He has been a visiting scientist at many institutions in the United States and Europe and is the author of around 100 scientific papers.

Davidovich can be reached by e-mail at ldavid@if.ufrj.br.