The Computer Journal Advance Access published June 27, 2007

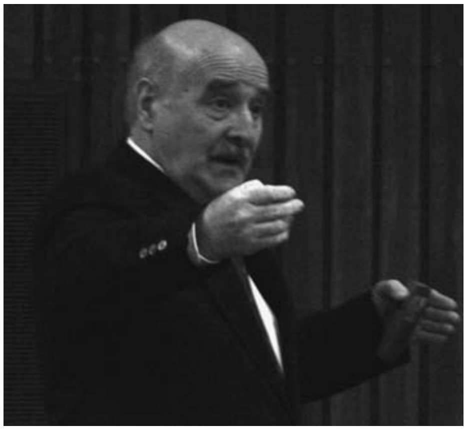
doi:10.1093/comjnl/bxm017

Quantum Information: A Glimpse At the Strange and Intriguing Future Of Information

Dan C. Marinescu* and Gabriela M. Marinescu

School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816, USA
**Corresponding author: dcm@cs.ucf.edu*

The Annual Boole Lecture was established and is sponsored by the Boole Center for Research in Informatics, the Cork Constraint Computation Center, the Department of Computer Science and the School of Mathematics, Applied Mathematics and Statistics, at University College Cork. The series is named in honor of George Boole (picture below), the first professor of Mathematics at UCC, whose seminal work on logic in the mid-1800s is central to modern digital computing. To mark this great contribution, leaders in the field of computing and mathematics are invited to talk to the general public on directions in science, on past achievements and on visions for the future.



Quantum and biological information processing could revolutionize computing and communication in the third millennium. In the 2007 Boole Lecture, we discussed the necessity to explore alternative paradigms for computing and communication and presented some striking features of quantum information processing and provided some insights into quantum parallelism as well as quantum communication and teleportation.

Keywords: Information; quantum information; qubit; entanglement; decoherence; density operator; polarization; spin; pure and mixed States; EPR experiment

1. INTRODUCTION

In our time, the research required to comprehend the more subtle aspects of the laws of nature and to use them for the good of mankind is very costly. The society will be willing to allocate the necessary resources for research only if the gap between the forefront of science and the level of scientific knowledge of the average individual narrows down. The purpose of Boole Lecture is to make scientific knowledge accessible to larger groups of individuals. In the 2007 Boole Lecture, we discussed the necessity to explore alternative paradigms for computing and communication and presented some striking features of quantum information processing and provided some insights into quantum parallelism as well as quantum communication and teleportation.

Quantum mechanics and information theory were developed by Heisenberg [1] in the mid-1920s and, respectively, by Shannon in the late 1940s [2]. Quantum mechanics had a profound influence on our understanding of nature and on our ability to exploit this understanding for the good of mankind. Information theory provided the foundation for the unprecedented development of communication and computing systems we have witnessed in the second half of the 20th century. The integration of quantum mechanics and information theory promises to provide an even deeper understanding of fundamental properties of nature and, at the same time, support new and exciting applications.

During the last few decades of the 20th century, the world witnessed the development in rapid succession of microprocessors, high-speed optical communication, high density storage technologies, followed by the widespread use of sensors. We are able to collect enormous volumes of information, process that information at high speed, transmit the information through high-bandwidth channels, store it on digital media and share it using the world wide web. Thus, the full cycle at the heart of information revolution was closed (Fig. 1), and this revolution became a reality that profoundly affects our daily life.

Now, at the beginning of the 21st first century, information processing is faced with new challenges: heat dissipation, leakage and other physical phenomena limit our ability to build increasingly smaller and faster solid-state devices; we have a hard time to ensure security of our communication; we are overwhelmed by the volume of information we are bombarded with, and it is increasingly more difficult to extract useful information from the ocean of information garbage.

For many years we have enjoyed Moore's law which states that the number of transistors on a chip doubles every 18 months, but an exponential growth cannot be sustained indefinitely; sooner or later one will hit a wall. The heat generated by densely packed solid-state devices in a sphere of radius R is proportional to the volume, thus to R^3; the heat can be removed trough the surface of the sphere, proportional to R^2. In 1992, Ralph Merkle from Xerox PARC calculated that a computer operating at room temperature with a clock rate of 1 GHz and 10^{18} gates packed in a volume of about 1 cm^3 would dissipate 3 MW of power. Leakage because of electromagnetic radiation, as well as power dissipation, limits also the speed of microprocessors. While we may still be able to increase the number of transistors on a chip according to Moore's law for a few more years, we are going to see microprocessors with multiple cores running at current clock rates rather than microprocessors with a higher clock rate.

The inquiring human mind is now searching for revolutionary means to overcome the limitations of computing and communication systems based upon the laws of classical physics; DNA computing and quantum information processing are the most promising avenues explored nowadays.

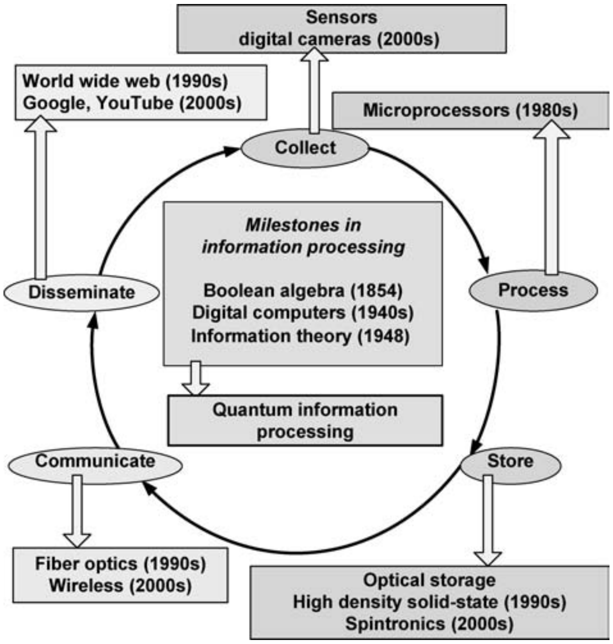


FIGURE 1. Our ability to collect, process, store, communicate and disseminate information has increased considerably during the last two decades of the 20th century. The 1980s was the decade of microprocessors; advances in solid-state technologies allowed Intel to increase the number of transistors on a chip from about 29×10^3 (8086) to 3.1×10^6 (Pentium) and to decrease the cost of the a microprocessor considerably. In 1990s, we have seen major breakthroughs in optical storage, high density solid-state storage technologies, fiber optics communication and the widespread acceptance of the word wide web. The first decade of the 21 century is the decade of sensors and rapid information dissemination.

Quantum information, information stored as the state of atomic or subatomic particles provides a glimpse of hope to overcome some of the limitations we mentioned. Yet, the strange world of atomic or sub-atomic particles is governed by quantum mechanics, a highly abstract and often counterintuitive mathematical model of the physical world.

The marriage of quantum physics with computing and communication cannot be a marriage of convenience, but one of necessity; we have to overcome immensely difficult technological problems and provide answers to fundamental questions regarding our understanding of nature. Quantum information has special properties: the state of a quantum system cannot be measured or copied without disturbing it; a quantum state can be *entangled*, two entangled systems have a definite global state, though neither has a state of its own; we cannot reliably distinguish non-orthogonal states of a quantum system. *Decoherence*, the randomization of the internal state of a quantum computer because of interactions with the environment, is a major problem in quantum information processing; fault-tolerant quantum computing requires many more years of research.

Bennett and Shor summarized the main differences between classical and quantum information [3]: "classical information can be copied freely, but can only be transmitted forward in time to a receiver in the sender's forward light cone. Entanglement, by contrast cannot be copied, but can connect any two points in space–time. Conventional data-processing operations destroy entanglement, but quantum operations can create it, preserve it and use it for various purposes, notably speeding up certain computations and assisting in the transmission of classical data or intact quantum states (teleportation) from a sender to a receiver."

The payoff of mastering quantum information could equally be astounding: in quantum systems an exponential increase in parallelism requires only a linear increase in the amount of space needed, thus, in principle, a quantum computer will be able to solve problems that cannot be solved with today's computers [4, 5]. Reversible quantum computers avoid logically irreversible operations and can, in principle, dissipate arbitrarily little energy for each logic operation. Eavesdropping on a quantum communication channel can be detected with very high probability. Quantum information theory allows us to design algorithms for quantum teleportation and for quantum key distribution.

2. INFORMATION

Once asked 'what is time,' Richard Feynman answered: 'time is what happens when nothing else happens.' Unfortunately, history did not record Feynman's answer to the question 'what is information' and thus we do not have a crisp, witty and insightful answer to a question central to the 21st century science.

Indeed, the questions 'what is information' and 'what is its relationship with the physical world' become more important as we try to better understand physical phenomena at quantum scale and the behavior of biological systems. von Weizšacker's answer, 'information is what is understood,' implies that information has a sender and a receiver who have a common understanding of the representation and the means to convey information using some properties of the physical systems [6]. He adds, 'Information has no absolute meaning; it exists relatively between two semantic levels' [7].

Like matter and energy, information is a primitive concept, thus it is rather difficult to rigorously define it. While matter and energy preoccupied the minds of philosophers starting with Leucippus and Democritus several hundred years before our era and later preoccupied the minds of many generations of natural scientists, information *per se* became a subject of serious investigation only after significant technological developments in communication in the late 1940s. Earlier, in the 1930s, Leo Szilard was concerned with the relation between information and energy and in 1960s Rolf Landauer formulated his principle[1], which relates information with thermodynamic entropy.

The concept of 'information' was brought to the forefront of science and engineering by Shannon who created Information Theory in the context of a statistical theory of communication. Shannon introduced the concept of *entropy* as a measure of information and developed the theoretical foundation of coding theory. Shannon's statistical theory of communication presented in 1948 was essential for the development of modern communication systems [8].

Informally, we all know that information abstracts properties of and allows us to distinguish objects/entities/phenomena/thoughts. Information is a common denominator for the very diverse contents of our material and spiritual world. There is a common expression of information as strings of bits, regardless of the objects/entities/processes/thoughts it describes. Moreover, these bits are independent of their physical embodiment. Information can be expressed using pebbles on the beach, mechanical relays, electronic circuits and even atomic and subatomic particles.

Information is transformed using logic operations. Gates implement logic operations and allow for automatic processing of information. The *usefulness of information* increases if the physical embodiments of bits and gates become smaller and we need less energy to process, store and transmit information. This justifies our interest in quantum information.

Evolution requires the ability to make decisions and a basic property of living matter is the capacity to distinguish objects and entities in order to make such decisions; a virus is able to distinguish the cells it can attach to an animal can distinguish a mate from a predator. Intelligent behavior requires the ability to distinguish concepts, ideas; scientists can distinguish the results of an experiment as well as the hypothesis each result confirms or rejects.

The concept of *distinguishability* provides a strong bond between quantum mechanics and information theory as each is concerned with the ability to distinguish information: quantum information embodied by quantum states in the case of the former, and classical information as generated by different physical processes of the later.

Quantum mechanics and information theory are both founded in non-determinism. Indeed, information theory was developed as a statistical theory of communication and non-determinism is a fundamental tenet of quantum mechanics. But there are fundamental differences between the role played by nondeterminism in information theory and in quantum mechanics.

In his book 'An Investigation of the Laws of Thought', Boole expresses the view that classical probabilities reflect lack of knowledge: "probability is expectation founded upon partial knowledge. A perfect acquaintance with all the circumstances affecting the occurrence of an event would change expectation into certainty, and leave neither room nor demand for a theory of probabilities" [9].

[1] *Landauer's Principle:* when a computer erases a bit of information the thermodynamic entropy of the environment increases by at least k_B In 2, k_B—Boltzmann's constant.

In stark contrast with information theory and classical physics where probabilities reflect lack of knowledge, the nondeterminism of quantum mechanics reflects our inability to precisely know the state of atomic or subatomic particles. The nondeterminism of quantum mechanics required the development of quantum information theory. If a deterministic model would be consistent with the experimental evidence regarding the behavior of atomic and subatomic particles, as quantum mechanics is, then classical information theory would be sufficient to study the information encoded as the state of quantum systems.

Mathematical models of the physical world describe the state and the dynamics of physical systems and any such description must consider the concept of information either explicitly or implicitly. Quantum mechanics is a mathematical model of the physical world developed in the mid-1920s to explain the behavior of atomic and subatomic particles, at a time when one could only dream about the practical applications of quantum effects for storing, processing and transmission of information. It took almost six decades, until in 1982, Feynman envisioned the idea of a quantum computer, a physical device which takes the advantage of the 'weird' behavior of quantum systems to process information. Feynman conjectured that only a quantum computer would be able to carry out an 'exact simulation' of a physical system [10].

There is little wonder that information is not a central concept in quantum mechanics, or that Information Theory, as developed by Shannon, is not concerned with the behavior of atomic and subatomic particles capable of carrying information. The milestones that mark the inception of the information age happened in the second half of the 20th century: the transistor was invented by William Shockley, John Bardeen and Walter Brattain, just before Christmas in 1947; the first commercial computer, UNIVAC I became operational in 1951; the DNA double helix strucrure was discovered by Sir Francis Harry Compton Crick and James Dewey Watson in 1953; the first microprocessor, the 4004, was produced by Intel in 1971.

There is no doubt that information plays an increasingly important role in our society. As we are exposed to an outpouring of information it becomes increasingly more difficult to discriminate useful information from noise, to extract information from apparently random data, to control complex systems with information distributed among a large set of actors, e.g. computer networks.

Information also plays a critical role in our understanding of nature. This revelation was brought to us by quantum mechanics, by our desire to use quantum information, and by our quest to understand biological systems. Fundamental questions on how accurately we can model the physical reality and what are the limitations in our knowledge about the surrounding universe do not have a clear and unambiguous answer.

Nowadays, some believe that the focus of Information Theory should migrate from the communication channel to the recipient of information, from communication to the consequences of receiving information. Indeed, in many instances the timeliness of information is important; the context of the information and the goals of the recipient of information (whether a human or a machine) affect the usefulness of information.

In spite of the significant progress made during the past half century, there are profound questions that still remain to be answered unequivocally by a unified information theory. Some believe that information has three aspects: (i) a syntactic aspect—the relationship between the symbols of the alphabet used to construct a message, (ii) a semantic aspect—the meaning of the message and (iii) a pragmatic aspect—the actions taken by the parties involved in the exchange. Shannon's theory does not cover the semantic aspect of information and cannot describe quantum and biological information [11] that, most certainly, will play a critical role in the third millennium.

3. QUBITS

A *quantum bit* or *qubit* is an elementary quantum object used to store information. For now we view a qubit as a mathematical abstraction and we hint to possible physical implementations of this abstract object.

Aqubit's state $|\psi\rangle$ is a vector in a two-dimensional complex vector space. In this space, a vector has two components and the projections of the vector on a basis of the vector space are complex numbers. We use Dirac notations to represent a vector $|\psi\rangle$ as

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{1}$$

with α_0 and α_1 complex numbers and with $|0\rangle$ and $|1\rangle$ the vectors forming an orthonormal basis for this two-dimensional vector space [12].

A classical bit can be in one of two states, 0 or 1. Thus, we can represent the state of a bit as $b = a_1 0 + a_2 1$, which has exactly two forma: either $a_1 = 1$ and $a_2 = 0$ and the value of the bit is $b = 0$, or $a_1 = 0$ and $a_2 = 1$ and the value of the bit is $b = 1$.

In contrast, the state of a qubit can be represented by $|\psi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle$, where $|0\rangle$ and $|1\rangle$ is an orthonormal pair of basis vectors, called *computational basis states*. The only restriction on the coefficients are that (i) α_0 and α_1 are complex numbers and (ii) $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Such a state is called a *superposition* of the basis vectors.

When we observe or measure a classical bit we determine its state with a probability of 1; the bit is either in state 0 or in state 1 and the result of a measurement is strictly deterministic. On the other hand, when we observe or measure the state of a qubit we get the result:

$$\begin{aligned} &|0\rangle \quad \text{with probability } |\alpha_0|^2, \\ &|1\rangle \quad \text{with probability } |\alpha_1|^2. \end{aligned} \tag{2}$$

For these statements to be true we need the vector length, or the *norm of the vector* to be equal to one, otherwise the probabilities do not sum to unity. This means that

$$|\alpha_0|^2 + |\alpha_1|^2 = \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 = 1 \tag{3}$$

with α_i^*, $i = 0, 1$ the complex conjugate of α_i.

We say that a qubit is in a superposition state until we measure it. For example, a qubit can be in state

$$\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \tag{4}$$

and a measurement of the qubit yields the result $|0\rangle$ with probability 1/4 and $|1\rangle$ with probability 3/4.

The superposition and the effect of the measurement of a quantum state (the state of the qubit) really mean that there is *hidden information* that is preserved in a *closed quantum system* until it is forced to reveal itself to an external observer. We say that the system is closed until it interacts with the outside world, e.g. until we perform an observation of the system.

Two physical systems leading to the simplest possible embodiments of a qubit are:

(1) the *electron* with two independent *spin* values, $\pm 1/2$, and
(2) the *photon*, with two independent *polarizations*, say *horizontal* and *vertical* (in case of linear polarization), or *right hand* and *left hand* (in case of circular polarization).

The *spin* is an intrinsic angular momentum[2] of a quantum particle, related to an intrinsic rotation about an arbitrary direction.

There are two classes of quantum particles, those with spin value a multiple of one-half, called *fermions*, and those with spin value a multiple of one, called *bosons*. The spin quantum number of fermions can be $s = +1/2$, $s = -1/2$, or an odd multiple of $s = \pm 1/2$. The spin quantum number of bosons can be $s = +1$, $s = -1$, $s = 0$ or a multiple of ± 1. The spin of a quantum particle can be observed as an interaction of the intrinsic angular momentum of the particle with an external magnetic field $\boldsymbol{B}$.

One embodiment of a qubit is the spin state of a particle with spin one-half, such as the electron[3]. 'Spin' does not correspond to any property in classical mechanics. Classical mechanics operates with the concept of an 'angular momentum' arising from a rotation around a well-defined axis of a body. A quantum particle such as the electron is not a 'body' in the classical sense and does not have a defined axis of rotation. The electron is characterized by a charge, which has a non-stationary spatial distribution. The variation in time of this charge distribution can be associated with an intrinsic rotation of the electron about directions randomly oriented in space.

The observable associated with the electron intrinsic rotation is the intrinsic angular momentum, also called the *spin angular momentum* of the electron. The 'spin' is the quantum number characterizing the intrinsic angular momentum of the electron. The electron spin is found to have either the value $+1/2$ or $-1/2$ along the measurement axis, regardless of what that axis is (see Fig. 2a).

The qubit states $|0\rangle$ and $|1\rangle$ correspond to the spin up $|\uparrow\rangle$ and spin down $|\downarrow\rangle$ states along a chosen axis such as the z-axis. It is convenient to represent the spin states as orthogonal unit vectors

$$|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{5}$$

A *photon* is another important two-state quantum system used to embody a qubit. A photon can have two independent polarizations and systems using the polarization of a photon to encode binary information have been used in real-life experiments.

Photons differ from the spin one-half electrons in two ways: (i) they are massless and (ii) they have spin one. A photon is characterized by its vector momentum (the vector momentum determines the frequency) and its polarization. In the classical theory, light is described as having an electric field that oscillates. The electric field can oscillate vertically, in a plane perpendicular to the direction of propagation, the z-axis, and then we say that the light is *x-polarized*, as in Fig. 3a. The electric field can oscillate horizontally in a plane perpendicular to the direction of propagation, and then we say the light is *y-polarized* as shown in Fig. 3b.

If the electric field has an arbitrary orientation in the xy-plane, then it will have x and y components. If these components are out of phase by 90°, the electric field rotates and the light is *elliptically polarized.* When the x and y components are equal and out of phase by 90°, the light is *circularly polarized.* Circularly polarized light can be *right-hand* polarized or *left-hand* polarized, depending on which way it propagates along the z-direction.

If we look at the individual photons participating in the 'light', we cannot talk about an electric field associated with

[2] The intrinsic angular momentum of a quantum particle should be distinguished from its orbital momentum.

[3] The protons and the neutrons are other particles with spin 1/2.

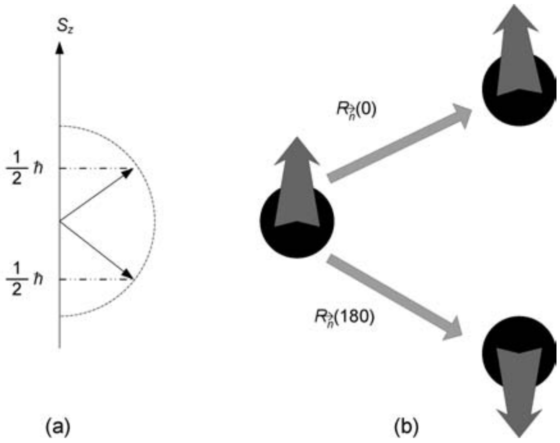


FIGURE 2. The spin of the electron. (a) Electrons and other particles (fermions) have intrinsic angular momentum characterized by the spin quantum number 1/2. (b) There are two rotation operators; the first keeps the spin unchanged, and the second flips the spin to an orthogonal state.

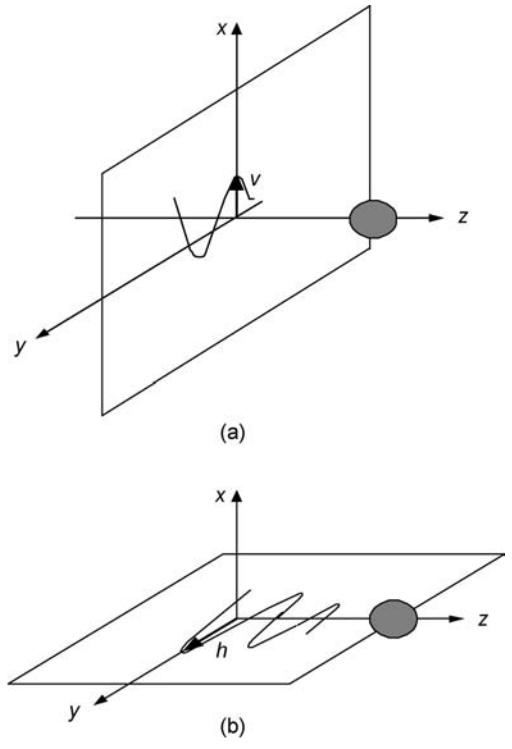


FIGURE 3. Linear photon polarization. (a) Vertical polarization, the polarization vector, *v* along the *x*-axis. (b) Horizontal polarization, the polarization vector, *h* along the *y*-axis.

a single photon, but a single photon must have a property as the analog of the classical phenomenon of polarization.

From the point of view of polarization, a photon can be described as a two-state system; a photon can be in state $|h\rangle$ or in state $|v\rangle$. All photons in a classically *y*-polarized beam of light are said to be in polarization state $|h\rangle$ and, similarly, all photons in a classically *x*-polarized beam of light are said to be in polarization state $|v\rangle$. The states $|h\rangle$ and $|v\rangle$ can be used as basis states to describe the polarization of a photon (in a linearly polarized beam of light) with given momentum oriented along the *z*-direction.

Actually, light contains photons in these two states of polarization. If we use a polarization filter (or polarization analyzer) and set its axis to let *y*-polarized light pass, then all photons in the state $|v\rangle$ will be absorbed in the filter and only the photons in state $|h\rangle$ will pass through. If the axis of the polarization filter is set to let *x*-polarized light pass, then all photons in state $|h\rangle$ will be absorbed and only photons in state $|v\rangle$ will pass through.

The question is how to use the hidden information captured by the state of a qubit. Now we discuss why quantum information can be exploited to compute faster and to communicate more securely.

4. QUANTUM PARALLELISM AND QUANTUM ALGORITHMS

In 1985, Deutsch recognized that a quantum computer has capabilities well beyond a classical computer and suggested that such capabilities can be exploited by cleverly crafted algorithms. Deutsch realized that a quantum computer can evaluate a function *f*(*x*) for many values of *x* simultaneously and called this strikingly new feature *quantum parallelism* [13].

Assume that the input vector $|x\rangle$ is in a superposition state and can be expressed as a linear combination of 2^m vectors forming an orthonormal basis in $\mathcal{H}^m$. The gate array performs a linear transformation. Henceforth, the transformation is applied to all basis vectors used to express the input superposition simultaneously, and it generates a superposition of results. In other words, the values of the function *f*(*x*) for the 2^m possible values of its argument *x* are computed simultaneously. This effect is called quantum parallelism and shows that quantum computers can provide an exponentially increasing computational space in a linearly increasing physical space.

Quantum parallelism allows us to construct the entire truth table of a quantum gate array having 2^n entries in one at once. In a classical system, we can compute the truth table in one time step with 2^n gate arrays running in parallel, or we need 2^n time steps with a single-gate array.

Quantum parallelism is best illustrated by the solution to the so-called 'Deutsch's problem'. Consider a black box characterized by a transfer function that maps a single input bit *x* into an output, *f*(*x*). The transformation performed by the black box, *f*(*x*), is a general function and might not be invertible. We assume that it takes the same amount of time, *T*, to carry out each of the four possible mappings performed by the transfer function $f(x)$ of the black box:

$$f(0) = 0 \quad f(0) = 1 \quad f(1) = 0 \quad f(1) = 1. \tag{6}$$

The problem posed is to distinguish if $f(0) = f(1)$ or $f(0) \neq f(1)$.

Using a classical computer one alternative is to compute sequentially $f(0)$ and $f(1)$ and then compare the results (see Fig. 4a) with a total time $2T$. A classical parallel solution is illustrated in Fig. 4b, where we feed 0 as input to one of the replicas of the black box and 1 to the other and then compare the partial results. In this case, we obtain the answer after time T.

Consider now a quantum computer with a transfer function U_f that takes as input two qubits $|x\rangle$ (control) and $|y\rangle$ (target) and two outputs, $|x\rangle$ and $|y\rangle \oplus f(x)\rangle$. We have the choice of selecting the states of the two qubits $|x\rangle$ and $|y\rangle$. First, let us choose for the second qubit the state $|y\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$.

We know that $|0\rangle \oplus f(x)\rangle = |f(x)\rangle$ with $\oplus$ the XOR operation. Thus:

$$|y\rangle \oplus |f(x)\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus |f(x)\rangle \tag{7}$$

or

$$|y\rangle \oplus |f(x)\rangle = \frac{1}{\sqrt{2}}(|f(x)\rangle - |1\rangle \oplus f(x)\rangle). \tag{8}$$

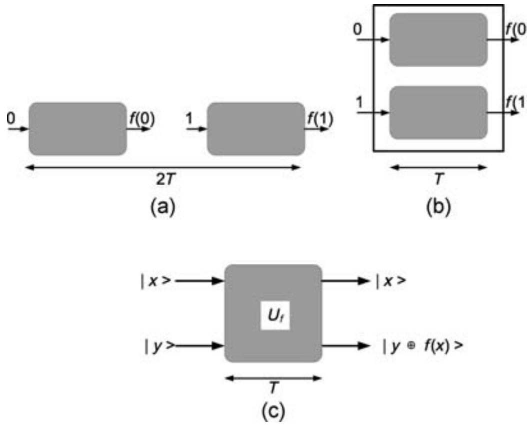


FIGURE 4. Classical and quantum parallelism. (a) Sequential solution to Deutsch's problem using a classical computer. (b) A parallel solution to Deutsch's problem using a classical computer. (c) The quantum black box with a transfer function U_f. It evaluates $f(0)$ and $f(1)$ simultaneously.

But $|1\rangle \oplus f(x)\rangle$ is equal to 0 when $f(x) = 1$ and it is equal to 1 when $f(x) = 0$ thus:

$$|1\rangle \oplus |f(x)\rangle = (-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{9}$$

The quantum black box performs the following transformation of the two qubits:

$$\begin{aligned}&\left[|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \xrightarrow{U_f} \\ &\left[|x\rangle \otimes (-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right].\end{aligned} \tag{10}$$

In these expressions, $|x\rangle \otimes |y\rangle$ denotes the tensor product of the two vectors and U_f is the transfer function of the quantum circuit. Let us now assume that the first qubit is in state $|x\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$. The transformation performed by the black box is:

$$\begin{aligned}&\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \xrightarrow{U_f} \\ &\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right].\end{aligned} \tag{11}$$

The procedure described above can be generalized for a function $f(x)$ where x is an n-tuple and can take any of the 2^n values. Aquantum black box allows us to compute at once the entire table giving all possible 2^N values of the function $f(x)$. The transfer function would then be:

$$[|x\rangle \otimes |0\rangle] \xrightarrow{U_f} [|x\rangle \otimes |f(x)\rangle]. \tag{12}$$

We select as control input a qubit in the state:

$$|x\rangle = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes n} = \frac{1}{\sqrt{2}}\sum_{x=0}^{2^n-1}|x\rangle. \tag{13}$$

We compute $f(x)$ only once and generate a state that encodes global properties of $f(x)$:

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{2^n-1}|x\rangle \otimes |f(x)\rangle. \tag{14}$$

The truly amazing result is that we compute the entire table of 2^n values at once regardless of the value of n. This gives a totally different meaning to the concept of *massive parallelism*. But, as always, there is a catch; unfortunately, as soon as we perform one measurement of state we can only recover one entry in the table. This parallelism is not very useful as such, we must discover clever ways of using it.

How similar are, at least conceptually, quantum and classical computers and, respectively, quantum and classical algorithms? In a quantum computer, the logic circuits and the time steps are essentially classical. Nevertheless, the qubits, the bits the quantum circuits operate on, can be in a superposition state; that's why we can simultaneously carry out multiple computations on the same computer, and that is ultimately the source of the immense power of quantum computers.

Quantum, as well as classical algorithms, start from an initial state and then cause a set of state transformations of the quantum, respectively, of the classical physical device, which eventually lead to the desired result. Indeed, the first step for any quantum computation is to initialize the system to a state that we can easily prepare; then we carry out a sequence of unitary transformations that cause the system to evolve toward a state which provides the answer to the computational problem.

A quantum operation is a rotation of the state $|\psi\rangle$ in an N-dimensional Hilbert space. Thus, the ultimate challenge is to build up powerful N-dimensional rotations as sequences of one- and two-dimensional rotations.

For any quantum algorithm there are multiple paths leading from the initial to the final state and there is a degree of interference among these paths. The amplitude of the final state, thus the probability of reaching the desired final state depends upon the interference among these paths. This justifies the common belief that quantum algorithms are very sensitive to perturbations and one has to be extremely careful when choosing the transformations the quantum system is subjected to.

A computational problem is considered tractable if an algorithm to solve it in a number of steps and requiring storage space polynomial in the size of the input exists. There are classically intractable problems, such as the Travelling Salesman Problem, which are proven to be in the complexity class *non-deterministic polynomial* ($\mathcal{NP}$).

In 1994, Shor found a polynomial time algorithm for the factorization of n-bit numbers on quantum computers [14]. Shor's algorithm reduces the factoring problem to the problem of finding the period of a function, but uses quantum parallelism to find a superposition of all values of the function in one step. Then the algorithm calculates the Quantum Fourier Transform of the function, which sets the amplitudes into multiples of the fundamental frequency, the reciprocal of the period. To factor an integer, the algorithm measures the period of the function. Shor's discovery generated a wave of enthusiasm for quantum computing, for two major reasons: the intrinsic intellectual beauty of the algorithm and the fact that efficient integer factorization is a very important practical problem. The security of widely used cryptographic protocols is based upon the conjectured difficulty of the factorization of large integers.

In 1996, Grover described a quantum algorithm for searching an unsorted database containing N items in a time of order $\sqrt{N}$ while on a classical computer the search requires a time of order N [15]. The speed-up of Grover's algorithm is achieved by exploiting both quantum parallelism and the fact that, according to quantum theory, a probability is the square of an amplitude. Bennett *et al.* [16] and Zalka [17] showed that Grover's algorithm is optimal. No classical or quantum algorithm can solve this problem faster than time of order $\sqrt{N}$.

Preskill called Grover's algorithm for searching an unsorted database 'perhaps the most important new development' in quantum complexity. "If quantum computers are being used 100 years from now, I would guess they will be used to run Grover's algorithm or something like it," Preskill says.

Grover's search algorithm can be applied directly to a wide range of problems, see for example [18]. Even problems not generally regarded as searching problems can be reformulated to take advantage of quantum parallelism and entanglement, and lead to algorithms which show a square root speed-up over their classical counterparts [19].

The main idea of the quantum search algorithm is to rotate the state vector in a two-dimensional Hilbert space defined by an initial and a final (target) state vector. The algorithm is iterative and each iteration causes the same amount of rotation.

5. HOW MUCH INFORMATION CAN WE ACQUIRE ABOUT A QUANTUM STATE?

The answer to this question forces us to quantify the uncertainty associated with a quantum state. It turns out that we have to distinguish between two types of quantum states, pure and mixed (impure) states, and that the density operator allows us to make this distinction.

We can acquire maximal knowledge about pure states. Whenever we can only attribute probabilities to possible states, or when we are allowed to observe only a subsystem of a composed system, we cannot acquire maximum information about the entire quantum system and we say that the system is in a mixed state.

In [20], we focused our discussion on *pure states*, which are described by Dirac's `ket` and `bra` vectors, or wave functions in a Hilbert space of the corresponding dimension. The evolution of a closed quantum system can be completely described as a unitary transformation of pure states in a Hilbert space. Pure states are characterized by maximal knowledge or minimal ignorance; in principle there is nothing more to be learned about the quantum system [3]. Pure states are represented as points on the *Bloch sphere*.

Mixed states are used to describe:

(1) Ensembles, or statistical mixtures of pure states. In this case the system can be in any of the pure states $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, ... with probabilities p_1, p_2, p_3, ...

(2) Composite systems. For example, consider the case when systems $\mathcal{A}$ and $\mathcal{B}$ are parts of a larger system, $\mathcal{AB}$ in an entangled pure state.

Mixed states require a *statistical characterization* provided by new concepts from *quantum statistical mechanics*, an extension of quantum mechanics. Mixed states are represented by points inside the *Bloch sphere*. For this reason it seems more accurate to talk about the *Bloch ball*.

The distinction between pure and mixed states is best described using the density operator, a positive semi-definite[4], self-adjoint operator with trace equal to unity. The density operator of a system in a pure state $|\psi\rangle$ is defined as:

$$\rho = |\psi\rangle\langle\psi|. \tag{15}$$

The density operator of the ensemble of pure states $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle \ldots$ with probabilities $p_1, p_2, p_3, \ldots$ is defined as:

$$\rho = \sum_{(i)} p_i |\psi_i\rangle\langle\psi_i|. \tag{16}$$

The density operator of an ensemble, ρ, captures only the information available to an observer who has the opportunities to examine infinitely many states of the ensemble. The entropy of a mixed state of non-orthogonal pure states, which are not mutually distinguishable, is given by von Neumann's expression [21]:

$$S(\rho) = -Tr(\rho) \times \log \rho. \tag{17}$$

When the pure states of the ensemble are orthogonal, they can be treated as classical states and then the entropy is given by the known Shannon expression:

$$H = -\sum_{(i)} p_i \times \log p_i. \tag{18}$$

We now turn our attention to composite systems. Composite systems are of interest in quantum information theory because quantum systems interact with one another and with the environment; such interactions affect the information encoded into the quantum state. For example, a system $\mathcal{A}$ in a pure state may interact with the environment; as a result of this interaction the state of the system may become a mixed state.

Let us consider a quantum system $\mathcal{C}$ consisting of two subsystems $\mathcal{A}$ and $\mathcal{B}$. The question we wish to explore is how to gather information about one of the subsystems, $\mathcal{A}$, from measurements performed on the composite system, $\mathcal{C} = \mathcal{AB}$ [3, 22]. The composite system may be in a product state $|\psi_\mathcal{C}\rangle = |\psi_\mathcal{A}\rangle \otimes |\psi_\mathcal{B}\rangle$ with $|\psi_\mathcal{A}\rangle$ the state of subsystem $\mathcal{A}$ and $|\psi_\mathcal{B}\rangle$ the state of subsystem $\mathcal{B}$, or in a state with some degree of entanglement between the two subsystems when $|\psi_\mathcal{C}\rangle \neq |\psi_\mathcal{A}\rangle \otimes |\psi_\mathcal{B}\rangle$ (Fig. 5).

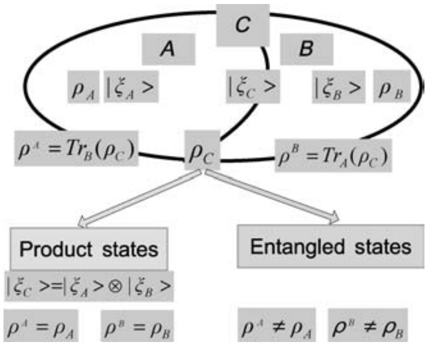


FIGURE 5. $\mathcal{C}$ is a composite system consisting of systems $\mathcal{A}$ and $\mathcal{B}$. The state and the density operators of the three systems are, respectively, $|\xi_\mathcal{C}\rangle$ and $\rho_\mathcal{C}$, $|\xi_\mathcal{A}\rangle$ and $\rho_\mathcal{A}$, $|\xi_\mathcal{B}\rangle$ and $\rho_\mathcal{B}$. The composite system can be either in a product state, or in an entangled state. $\mathcal{C}$ is in a product state if $|\xi_\mathcal{C}\rangle = |\xi_\mathcal{A}\rangle \otimes |\xi_\mathcal{B}\rangle$; in this case, the reduced density operators satisfy the equalities $\rho^\mathcal{A} = \rho_\mathcal{A}$ and $\rho^\mathcal{B} = \rho_\mathcal{B}$.

To characterize composite systems, we use the partial of the density matrix and the reduced density operator of a subsystem of a composite system. Let $\mathcal{C} = \mathcal{AB}$ be a composite system consisting of two subsystems $\mathcal{A}$ and $\mathcal{B}$ described by the density operator $\rho_\mathcal{C}$. The *partial trace of $\rho_\mathcal{C}$ over system $\mathcal{B}$ is*:

$$\begin{aligned} Tr_\mathcal{B}[\rho_\mathcal{C}] &= Tr_\mathcal{B}[|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|] \\ &= |a_1\rangle\langle a_2| Tr_\mathcal{B}[|b_1\rangle\langle b_2|] = |a_1\rangle\langle a_2|\langle b_1|b_2\rangle \end{aligned} \tag{19}$$

with $|a_1\rangle$, $|a_2\rangle$ any two vectors in the state space of $\mathcal{A}$ and $|b_1\rangle$, $|b_2\rangle$ any two vectors in the state space of $\mathcal{B}$. The *reduced density operator of subsystem $\mathcal{A}$ is:*

$$\rho^\mathcal{A} = Tr_\mathcal{B}[\rho_\mathcal{C}]. \tag{20}$$

Let $\mathcal{C} = \mathcal{AB}$ be a composite system in a product state with $\rho_\mathcal{A}$ the density operator of subsystem $\mathcal{A}$, $\rho_\mathcal{B}$ the density operator of subsystem $\mathcal{B}$, and $\rho_\mathcal{C} = \rho_\mathcal{A} \otimes \rho_\mathcal{B}$. Then the reduced density operator of each subsystem is equal to the density operator of the subsystem:

$$\rho^\mathcal{A} = \rho_\mathcal{A} \quad \text{and} \quad \rho^\mathcal{B} = \rho_\mathcal{B}. \tag{21}$$

Indeed, the trace of the density operator of a system is equal to unity thus:

$$Tr_\mathcal{A}[\rho_\mathcal{A}] = 1 \quad \text{and} \quad Tr_\mathcal{B}[\rho_\mathcal{B}] = 1. \tag{22}$$

[4] An $n \times n$ symmetric matrix A is positive semi-definite if $\forall v \neq 0$ $v^\mathrm{T} Av \geq 0$; the eigenvalues of A are real and non-negative, the diagonal elements of A are non-negative and $TrA \geq 0$. The eigenvalues of a positive definite matrix are real and positive.

According to the definition of the reduced density operator:

$$\begin{aligned}\rho^{\mathcal{A}} &= Tr_{\mathcal{B}}[\rho_{\mathcal{C}}] = Tr_{\mathcal{B}}[\rho_{\mathcal{A}} \otimes \rho_{\mathcal{B}}] = \rho_{\mathcal{A}} Tr_{\mathcal{B}}[\rho_{\mathcal{B}}] = \rho_{\mathcal{A}}, \\ \rho^{\mathcal{B}} &= Tr_{\mathcal{A}}[\rho_{\mathcal{C}}] = Tr_{\mathcal{A}}[\rho_{\mathcal{A}} \otimes \rho_{\mathcal{B}}] = \rho_{\mathcal{B}} Tr_{\mathcal{A}}[\rho_{\mathcal{A}}] = \rho_{\mathcal{B}}.\end{aligned} \tag{23}$$

This result reflects also our intuition; if indeed both the density operator $\rho_{\mathcal{A}}$ and the reduced density operator $\rho^{\mathcal{A}}$ characterize the same state of the system $\mathcal{A}$, then the average of an observable should be the same regardless whether it is computed using $\rho_{\mathcal{A}}$, or $\rho^{\mathcal{A}}$. This is true only for product states; if the system is in an entangled state we expect that the interaction of the two subsystems will affect the outcome of a measurement in a more subtle manner.

Let $\mathcal{M}^{\mathcal{A}}$ be an observable of $\mathcal{A}$ and $\mathcal{M}^{\mathcal{C}}$ the corresponding observable of $\mathcal{A}$ but performed on $\mathcal{C} = \mathcal{AB}$. Let $I_{\mathcal{B}}$ be the identity matrix in the state space of $\mathcal{B}$ and $\rho_{\mathcal{A}}$ and $\rho_{\mathcal{C}}$ be the density operators for the two systems, respectively. Then:

$$\mathcal{M}^{\mathcal{C}} = \mathcal{M}^{\mathcal{A}} \otimes I_{\mathcal{B}}. \tag{24}$$

If $|\psi_{\mathcal{C}}\rangle$ is a pure state of the composite system $\mathcal{C} = \mathcal{AB}$ then the eigenvalues of the reduced density operators of the two component systems are identical. Thus, many properties of the two subsystems that are determined by the eigenvalues of the reduced density operators are the same for the two subsystems.

Pure states have a particular appeal for quantum information theory thus, a legitimate question is, if given a quantum system $\mathcal{A}$ in a mixed state can we identify another system $\mathcal{B}$ such that the composite system $\mathcal{C} = \mathcal{AB}$ is in a pure state. In this case $\mathcal{B}$, called a *reference system*, is only a mathematical construct without a physical support.

The density operator of $\mathcal{A}$, a subsystem of the composite system $\mathcal{AB}$, in the entangled pure state $|\psi_{\mathcal{AB}}\rangle$ is:

$$\rho = Tr_B|\psi_{AB}\rangle\langle\psi_{AB}|. \tag{25}$$

In this case, the density operator captures only the information available to an observer who has infinitely many opportunities to examine the subsystem $\mathcal{A}$ of the composite system $\mathcal{AB}$.

Consider now a quantum system in a mixed state. The Stern–Gerlach experiment (Fig. 6) illustrates the fact that a beam of silver atoms consists of a mix of atoms with two different spin values. The experimental setup uses a non-uniform magnetic field whose z-axis component is normal to the planar cap; the components of the magnetic field along x and y axis are negligible. The atomic beam entering the apparatus consists of a statistical mixture of silver atoms in spin states $|\uparrow\rangle$ and $|\downarrow\rangle$, which will be deflected upwards and, respectively, downwards following their spin interaction with the magnetic field. If the atomic beam consists of N particles, then the probability of an atom to have its spin up approaches the ratio $N^{\uparrow}/N$ for very large N; $N^{\uparrow}$ is the number of atoms deflected upwards.

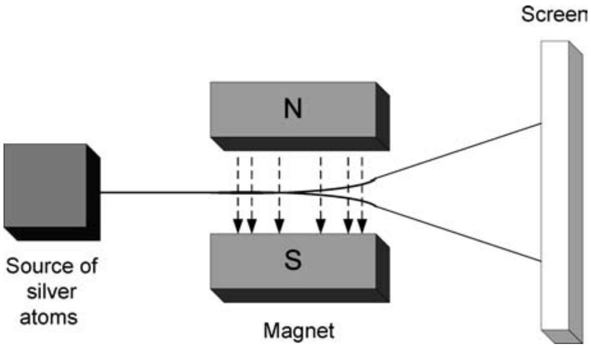


FIGURE 6. The silver atomic beam entering the apparatus used in the Stern–Gerlach experiment consists of a statistical mixture of atoms in spin states $|\uparrow\rangle$ and $|\downarrow\rangle$, which will be deflected upwards and, respectively, downwards.

The value of an observable cannot be predicted with certainty. Yet, we have to make a distinction between the probabilities associated with a pure state and the probabilities associated with impure states or statistical mixtures. For example, in case of spin one-half particles discussed above we have two possible spin states, $|\uparrow\rangle$ and $|\downarrow\rangle$; for any superposition state $|\psi\rangle = \alpha_0|\uparrow\rangle + \alpha_1|\downarrow\rangle$ the sum of the probabilities of the two possible states is 1, $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The $|\uparrow\rangle$ and $|\downarrow\rangle$ are pure states.

In our discussion of the Stern–Gerlach experiment, *a pure spin state* corresponds to a *completely polarized beam*, while a statistical mixture corresponds to either a *partially polarized beam* when the probabilities of possible states are unequal, or to an *unpolarized beam* if the probabilities of the states are equal.

6. MONOGAMY OF ENTANGLEMENT

Quantum systems have a unique property: a composite system can be in a pure state for which it is not possible to assign a definite state to each of its component sub-systems. This strong correlation of quantum states is called *entanglement*. Erwin Schrödinger discovered the phenomenon of entanglement[5] and in 1935 he made the following crucial observation: “Total knowledge of a composite system does not necessarily include maximal knowledge of all its parts, not even when these are fully separated from each other and at the moment are not influencing each other at all.” Entanglement plays a critical role in quantum computing and quantum communication; the concept of monogamy of entanglement justifies why quantum states cannot be cloned.

[5] Entanglement is the English translation of the German noun Verschränkung, the name used by Schrödinger to describe this phenomenon.

According to the postulates of quantum mechanics, the state of a composite system is a vector in the Hilbert space[6] obtained as a tensor product of the individual Hilbert spaces $\mathcal{H}_{n_1}, \mathcal{H}_{n_2} \dots \mathcal{H}_{n_k}$:

$$\mathcal{H}_{n_1 \times n_2 \cdots \times n_k} = \mathcal{H}_{n_1} \otimes \mathcal{H}_{n_2} \dots \otimes \mathcal{H}_{n_k}. \tag{26}$$

In this expression, the states of the component systems are represented by vectors in lower dimensional Hilbert spaces, $\mathcal{H}_{n_i}$, $1 \leq i \leq k$, respectively. For example, a quantum system consisting of two qubits is described using the orthonormal basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ by a vector in $\mathcal{H}_{2^2} = \mathcal{H}_2 \otimes \mathcal{H}_2$:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{27}$$

with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

Sometimes the state of a two-qubit system can be factored as the tensor product of the individual states of two qubits. For example, when $\alpha_{00} = \alpha_{10} = 1/2$ and $\alpha_{01} = \alpha_{11} = -i/2$ the state is:

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}[|00\rangle + i|01\rangle - |10\rangle - i|11\rangle] \\ &= \frac{1}{2}[|0\rangle \otimes (|0\rangle + i|1\rangle) - |1\rangle \otimes (|0\rangle + i|1\rangle)] \\ &= \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle + i|1\rangle) \\ &= |\psi_1\rangle \otimes |\psi_2\rangle. \end{aligned} \tag{28}$$

The individual states of the two qubits are well defined:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle). \tag{29}$$

This factorization is not always feasible. For example, consider a special state of a two-qubit system when:

$$\alpha_{00} = \alpha_{11} = 1/\sqrt{2}, \quad \alpha_{01} = \alpha_{10} = 0. \tag{30}$$

The state:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{31}$$

is called a *Bell state* and the pair of qubits is called an Einstein–Podolski–Rosen (EPR) *pair*. There are three other *Bell states*:

$$\begin{gathered} |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{gathered} \tag{32}$$

The Bell states form an orthonormal basis and can be distinguished from one another. The Bell states are *entangled* states; all four states are called *maximally entangled* states. The last one, $|\beta_{11}\rangle$ is called an *anti-correlated* state.

It can be shown that *the joint state of an EPR pair* (*a Bell state*) *is known exactly* (*it is a pure state*), *while the state of either qubit of the pair is not* (*it is a mixed state*).

Let us pick one of the Bell states, say $|\beta_{10}\rangle$, and compute its density operator, $\rho_{(\beta_{10})}$. Then we compute the density operator of one of the qubits of the EPR pair, say the second one, $\rho_{(\beta_{10},\text{second})}$. We expect that the traces of the two density operators satisfy the known relations for pure and, respectively, mixed states

$$Tr\left[\rho^2_{(\beta_{10})}\right] = 1 \quad Tr\left[\rho^2_{(\beta_{10},\text{second})}\right] < 1. \tag{33}$$

First, we compute the density operator of the pair:

$$\rho_{(\beta_{10})} = |\beta_{10}\rangle\langle\beta_{10}| = \frac{(|00\rangle - |11\rangle)}{\sqrt{2}}\frac{(\langle 00| - \langle 11|)}{\sqrt{2}}. \tag{34}$$

Then,

$$\rho_{(\beta_{10})} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \tag{35}$$

and

$$\rho^2_{(\beta_{10})} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}. \tag{36}$$

It follows that:

$$Tr\left[\rho^2_{(\beta_{10})}\right] = \frac{1}{2}(1 + 0 + 0 + 1) = 1. \tag{37}$$

[6] A Hilbert space is a vector space over the field of complex numbers with the distance defined as the inner product of two vectors.

We compute the reduced density operator and the partial trace for the second qubit of the EPR pair by tracing the first qubit

$$\begin{aligned}\rho_{(\beta_{10},\text{second})} &= Tr_{\text{first}}\Big[\rho_{\beta_{10}}\Big]\\ &= Tr_{\text{first}}\frac{[|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|]}{2}.\end{aligned} \tag{38}$$

Then

$$\rho_{(\beta_{10},\text{second})} = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{I}{2} \tag{39}$$

and

$$\rho^2_{(\beta_{10},\text{second})} = \frac{1}{4}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{4}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}. \tag{40}$$

It follows that

$$Tr\Big[\rho^2_{(\beta_{10},\text{second})}\Big] = \frac{1}{4}(1+1) = \frac{1}{2}. \tag{41}$$

To complete the proof of this proposition, we have to repeat the calculation for the first qubit of the β_{10} pair following the pattern presented above. Then we have to redo the calculations for the other three Bell states β_{00}, β_{01} and β_{11}.

The monogamy of entanglement is the deeper root of our inability to clone quantum states. Figure 7 illustrates why the monogamy of entanglement prevents quantum states to be cloned. Consider two maximally entangled quantum systems, $\mathcal{A}$ and $\mathcal{B}$. Assume that we have a quantum copy machine able to clone quantum states. If the input to this quantum copy machine is system $\mathcal{A}$, then the output will be the original, system $\mathcal{A}$, and a perfect replica of it, $\mathcal{A}'$. Thus, the quantum system $\mathcal{B}$ would end up being entangled with both systems $\mathcal{A}$ and $\mathcal{A}'$, in violation of the monogamy of entanglement. The dotted line represents the original entanglement of $\mathcal{B}$ with $\mathcal{A}$, and the solid lines the entanglement of $\mathcal{B}$ with $\mathcal{A}$ and its clone $\mathcal{A}'$. As we have seen earlier, the joint state of a maximally entangled pair system is a pure state, while individual particles are in mixed state; thus, the state of individual particles cannot be known with certainty and individual particles cannot be cloned.

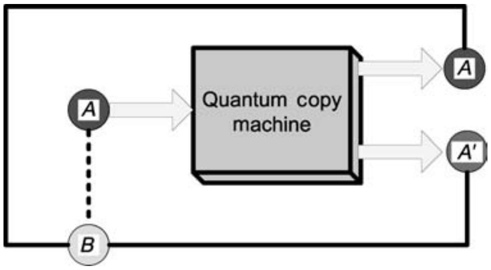


FIGURE 7. In violation of the monogamy of entanglement, a quantum copy machine would allow a quantum state $\mathcal{B}$ entangled with another quantum state $\mathcal{A}$ to end up entangled with the two copies of state $\mathcal{A}$.

One of the most intriguing properties of quantum information is the shareability of quantum correlations. While classical correlations can be shared among many parties, quantum correlations cannot be shared freely, quantum correlations of pure states are monogamous.

As we know from statistics, if two random variables X and Y are correlated, then X can also be correlated with any number of other random variables, Z, W, ... and Y can also be correlated with U, V, ... If two quantum systems $\mathcal{A}$ and $\mathcal{B}$ are in a maximally entangled pure state, then neither of them can be correlated with any other system in the universe.

There is a trade-off between the amount of entanglement of two qubits and the quantum correlation each of the two qubits could share with a third one. It is widely believed that if the two qubits are as much entangled with each other as it is possible they cannot be entangled or even classically correlated with another qubit.

Consider three qubits a, b, c such that the first two are in a maximally entangled pure state [23]:

$$|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}|0_a \otimes 0_b\rangle + \frac{1}{\sqrt{2}}|1_a \otimes 1_b\rangle \tag{42}$$

and the third is in state $|\psi_c\rangle$. There is no quantum state shared by the three qubits, such that when we remove the third qubit, c, we get the joint state of qubits a and b, $|\psi_{ab}\rangle$, and, at the same time, the three-qubit state does not change when we interchange qubits b and c, i.e. we entangle a with c instead of b. Thus, the joint state of the three qubits is:

$$|\psi_{abc}\rangle = |\psi_c\rangle \otimes \left[\frac{1}{\sqrt{2}}|0_a \otimes 0_b\rangle + \frac{1}{\sqrt{2}}|1_a \otimes 1_b\rangle\right]. \tag{43}$$

There is no symmetry, between qubits b and c, b is maximally entangled with a while c is not entangled with a.

The monogamy of entanglement has important consequences for quantum cryptography. If two parties, Alice and Bob share an entangled quantum state they can communicate securely.

The next question is if all entangled states are monogamous. For example, are entangled mixed states monogamous? Schumacher introduced the term *sharable quantum states* and Bennett *et al.* [24] gave an example of a mixed entangled state that is sharable rather than monogamous. Consider a noisy quantum channel shared by Alice, Bob and Eve; with probability 1/2 a qubit sent by Alice is transmitted unchanged to Bob and with probability 1/2 the qubit is intercepted by Eve and Bob gets a random qubit. When Alice sends to Bob half of a maximally entangled pair, the state shared by Alice and Bob is still entangled while the state shared by the three is always symmetric in respect to Eve and Bob, thus Eve is entangled with Alice as well.

7. EPR EXPERIMENT

EPR is the gedanken experiment proposed by Einstein, Podolsky and Rosen to show that the description of a quantum system by means of the wave function is incomplete. The EPR experiment led some physicists to the belief that the nondeterminism of quantum mechanics could be explained by the existence of 'hidden variables.'

If we knew the exact values of hidden variables, then we would have a fully deterministic view of the world [25]. A suggestive analogy was proposed by one of our students. He said: "Imagine that we are behind a wall that obscures the view of the other side where several machines throw tennis balls over the wall. The trajectory of each ball depends upon the setting of each machine; assuming that the tennis balls are identical and their weight and diameter are known and that there is no wind, the trajectory of each one is perfectly deterministic. Yet, to us the trajectory of a ball appears to be random. The nondeterminism is due to the lack of knowledge of the initial conditions for each trajectory, the hidden variables of this game."

The EPR argument is based upon the concept of 'element of physical reality' defined as follows: *if without in any way disturbing a system we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*

In his autobiography Einstein wrote [26]: "... the paradox forces us to relinquish one of the following two assertions: (i) the description by means of the wave function ψ is complete, (ii) the real states of spatially separated objects are independent of each other." Einstein concluded that the quantum mechanical description by means of the wave function is not complete, he had no doubts that the second assertion is true. Non-locality would violate one of the basic postulates of the Special Theory of Relativity[7].

We consider a composite system consisting of two particles, 'particle 1' and 'particle 2' prepared in such a state that their total momentum is close to zero and their relative distance is close to L, where L is much larger than the distance that allows the two particles to interact with each other. If we denote by γ a normalizable function with a very high and very narrow peak, and by x_1, x_2, p_1, p_2 the position and the momentum of the two particles, then the state of the system is described by an entangled wave function:

$$\psi = \gamma(x_1 - x_2 - L)\gamma(p_1 + p_2). \tag{44}$$

We do not know anything about the position of the particles or about their individual momenta, we only know that they are at distance L from one another and that the total momentum is equal to zero.

If we measure the position of the first particle, x_1, the wave function allows us to predict with certainty, x_2, the position of the second particle. It is easy to argue based upon EPR definition that x_2 corresponds to an element of the physical reality. Indeed, the measurements on the two systems do not affect each other because the distance L was chosen to be large enough to prevent such interactions. Thus, no change may take place in the second system as a result of the measurement performed in the first system.

We could have measured the momentum of the first particle, p_1, and then we would have been able to predict the momentum of the second one, p_2. Similar arguments indicate that p_2 corresponds to an element of the physical reality. Yet, Heisenberg's inequality precludes the simultaneous assignment of precise values to both the position, x_2 and the momentum, p_2 of the second particle because the two operators corresponding to the two measurements of observables do not commute.

In a simpler version of the EPR experiment suggested by Bohm (see [27]), a spin zero pion π^0 decays into an electron e^- and a positron e^+ both spin one-half particles. If a spin component of the electron, say S_z^e is measured when the two decay products are far apart and found to be $+\hbar/2$, then we can be sure that the S_z^p component of the positron spin will be found equal to $-\hbar/2$. We could have measured the other spin components of the electron, S_x^e and S_y^e, and then the spin components of the positron S_x^p and S_y^p would have also been predictable with certainty. Thus, the three spin components of the positron spin, S_x^p, S_y^p and S_z^p would have corresponded to 'elements of the physical reality' and that would have been in contradiction with quantum mechanics which says that at most one spin component of each particle may be definite.

The EPR conclusion is that the quantum mechanical description of the physical world by means of the weave function is incomplete, but the authors do not discuss whether a complete description really exists.

8. QUANTUM TELEPORTATION

In a science fiction context, teleportation means: making an object or person disintegrate in one place and have it

[7] Einstein's Special Theory of Relativity describes the motion of particles moving at close to the speed of light. The two basic postulates of special relativity are: (i) The speed of light is the same for all observers, no matter what their relative speeds. (ii) The laws of physics are the same in any inertial (that is, non-accelerated) frame of reference. This means that the laws of physics observed by a hypothetical observer traveling with a relativistic particle must be the same as those observed by an observer who is stationary in the laboratory.

reembodied as the same object or person somewhere else. In the context of quantum information theory, teleportation means [27]: “a way to scan out part of the information from an object A, which one wishes to teleport, while causing the remaining, unscanned, part of the information to pass, via the EPR effect, into another object C which has never been in contact with A. Later, by applying to C a treatment depending on the scanned-out information, it is possible to maneuver C into exactly the same state as A was in before it was scanned.” In this process, the original state is destroyed.

Communication over quantum channels involves the transport of quantum particles and could certainly benefit from the formalism described above. This formalism allows us to determine the state of system $\mathcal{A}$, namely the original quantum particle(s) prepared in a certain state $|\varphi_{\mathcal{A}}\rangle$ based upon observations performed on the composite system $\mathcal{AB}$ in state $|\varphi_{\mathcal{AB}}\rangle$.

Quantum teleportation means the transfer of quantum state from one particle to another [20]. In this process, one has to perform a measurement of one particle of a composite system.

Assume that Alice and Bob are given a pair of entangled particles called ‘particle 1’ and ‘particle 2’ in a maximally entangled state (Fig. 8):

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{45}$$

Then Bob takes ‘particle 2’ with him, while Alice keeps ‘particle 1’ with her. A third party, Eve, asks Alice to deliver a secret message to Bob. The message is encoded ins the state of ‘particle 3’:

$$|\psi_C\rangle = \alpha_0|0\rangle + \alpha_1|1. \tag{46}$$

Alice applies a CNOT gate to the pair, using the state of ‘particle 3’ as the control qubit and the state of ‘particle 1’ as the target qubit. When Alice performs a joint measurement of her two qubits, she gets the results $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, which correspond to classical information 00, 01, 10 and 11, respectively, with equal probability, $p = 1/4$. Alice then measures the state of ‘particle 1’ and sends over a classical communication channel the result of the measurement, ‘00’, ‘01’, ‘10’ or ‘11’. Then Bob applies one of the following four transformations to the state of ‘particle 2’. If he receives the string ‘00’ he applies the identity transformation, I. He applies X if he receives the string ‘01’, Z for ‘10’, and Y for ‘11’. As a result of this transformation, the state of ‘particle 2’ is identical to the state of ‘particle 3’.

It can be shown that *quantum teleportation does not allow an instantaneous exchange of information.* The state of Bob’s qubit after Alice’s measurement is not dependent upon the state of ‘particle 3’. No measurement performed by Bob after Alice’s measurement contains definite information about ‘particle 3’. Therefore, Alice needs to use a classical communication channel to transmit the result of her measurement to Bob; in fact, she cannot use teleportation to transmit information instantaneously to Bob.

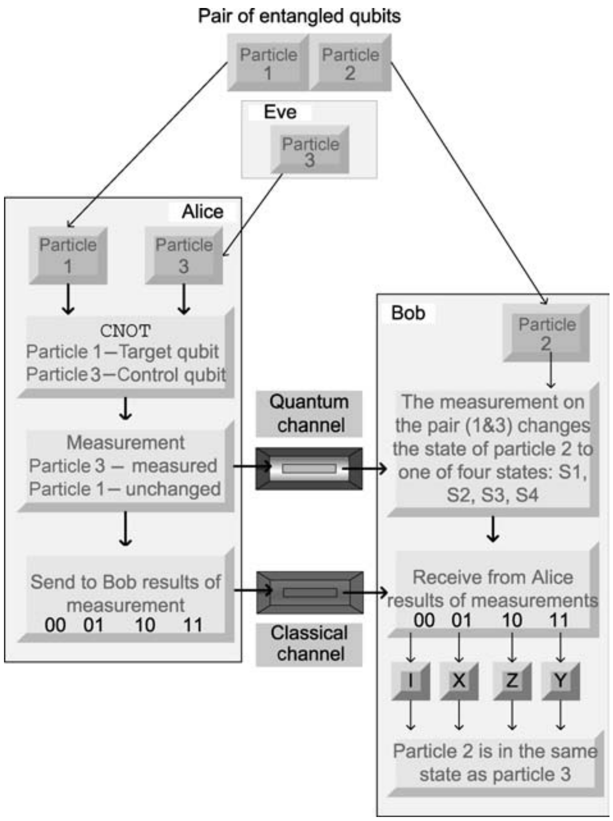


FIGURE 8. Schematics of quantum teleportation with maximally entangled particles. At the beginning of the experiment Eve’s particle is in state $|\psi_C\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$; the pair of particles shared by Alice and Bob are in a maximally entangled state $|\beta_{00}\rangle$. At the end of the experiment Bob’s half of the entangled pair is in state $|\psi_C\rangle$, while the state of Eve’s particle was affected by the quantum measurement and is no longer $|\psi_C\rangle$. The change of state of Bob’s particle does not occur instantaneously, Alice must use a classical communication channel to transmit the results of her measurement to Bob.

The state $|\zeta\rangle$ of the three particle systems after Alice performs her measurement is:

$$\begin{aligned}|\zeta\rangle = \frac{1}{2}[&|00\rangle(\alpha_0|0\rangle + \alpha_1|1\rangle)\\ &+ |01\rangle(\alpha_0|1\rangle) + \alpha_1|0\rangle) + |10\rangle(\alpha_0|0\rangle - \alpha_1|1\rangle)\\ &+ |11\rangle(\alpha_0|1\rangle - \alpha_1|0\rangle)].\end{aligned} \tag{47}$$

Indeed, the joint state of ‘particle 3’ and ‘particle 1’ is:

$$|\xi\rangle = |\psi_C\rangle \otimes |\beta_{00}\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} \tag{48}$$

or

$$|\xi\rangle = \left(\frac{1}{\sqrt{2}}\right)\Big(\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|100\rangle + \alpha_1|111\rangle\Big). \quad (49)$$

Alice applies a CNOT to the pair; she uses Eve's qubit as a control and her own as a target. She applies the $G_{\texttt{CNOT}} \otimes I$ transformation to the state $|\xi\rangle$.

$$|\kappa\rangle = (G_{\texttt{CNOT}} \otimes I)(|\xi\rangle) \quad (50)$$

$$G_{\texttt{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (51)$$

Thus:

$$|\kappa\rangle = \left(\frac{1}{\sqrt{2}}\right)\Big(\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|101\rangle + \alpha_1|110\rangle\Big). \quad (52)$$

Then Alice measures the first qubit (Eve's qubit) and leaves the second (the one entangled with Bob's qubit) untouched:

$$|\zeta\rangle = (H \otimes I \otimes I)|\kappa\rangle. \quad (53)$$

Thus:

$$|\zeta\rangle = \frac{1}{2}\Big[|00\rangle(\alpha_0|0\rangle + \alpha_1|1\rangle) + |01\rangle(\alpha_0|1\rangle) + \alpha_1|0\rangle) + |10\rangle(\alpha_0|0\rangle - \alpha_1|1\rangle) + |11\rangle(\alpha_0|1\rangle - \alpha_1|0\rangle)\Big]. \quad (54)$$

From this expression, it follows that when Alice performs a joint measurement of her two qubits, she gets one of the four equally probable results $|00\rangle$ or $|01\rangle$ or $|10\rangle$ or $|11\rangle$. As we already know, this measurement forces the pair of qubits to one of the four basis states, and transforms quantum information into classical one. Then, she sends Bob the result of her measurement, 00, 01, 10 or 11, over a classical communication channel. At the same time, the measurement performed by Alice forces the qubit in Bob's possession to change to one of four states:

(1) $|\eta_{00}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ when the result is 00.
(2) $|\eta_{01}\rangle = \alpha_0|1\rangle + \alpha_1|0\rangle$ when the result is 01.
(3) $|\eta_{10}\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle$ when the result is 10.
(4) $|\eta_{11}\rangle = \alpha_0|1\rangle - \alpha_1|0\rangle$ when the result is 11.

The density operator of state $|\zeta\rangle$ is:

$$\begin{aligned}\rho_{\mathcal{C}}(\zeta) &= \sum_{i=1}^{4} p_i\rho_i = \frac{1}{4}(\rho_0 + \rho_1 + \rho_2 + \rho_3) \\ &= \frac{1}{4}\big(|00\rangle\langle 00|[(\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0^*\langle 0| + \alpha_1^*\langle 1|)] \\ &\quad +|01\rangle\langle 01|[(\alpha_0|1\rangle + \alpha_1|0\rangle)(\alpha_0^*\langle 1| + \alpha_1^*\langle 0|)] \\ &\quad +|10\rangle\langle 10|[(\alpha_0|0\rangle - \alpha_1|1\rangle)(\alpha_0^*\langle 0| - \alpha_1^*\langle 1|)] \\ &\quad +|11\rangle\langle 11|[(\alpha_0|1\rangle - \alpha_1|0\rangle)(\alpha_0^*\langle 1| - \alpha_1^*\langle 0|)]\big).\end{aligned} \quad (55)$$

Bob's qubit is the second of the pair and the reduced density operator of Bob's qubit is:

$$\begin{aligned}\rho^{\mathcal{B}} &= Tr_{\mathcal{A}}\Big[\rho_{\mathcal{C}}(\zeta)] = \frac{1}{4}[(\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0^*\langle 0| \\ &\quad +\alpha_1^*\langle 1|) + (\alpha_0|1\rangle + \alpha_1|0\rangle)(\alpha_0^*\langle 1| + \alpha_1^*\langle 0|) \\ &\quad +(\alpha_0|0\rangle - \alpha_1|1\rangle)(\alpha_0^*\langle 0| - \alpha_1^*\langle 1|) \\ &\quad +(\alpha_0|1\rangle - \alpha_1|0\rangle)(\alpha_0^*\langle 0| - \alpha_1^*\langle 1|)\Big].\end{aligned} \quad (56)$$

Then,

$$\rho^{\mathcal{B}} = \frac{1}{4}\Big[|0\rangle\langle 0|2(|\alpha_0|^2 + |\alpha_1|^2) + |1\rangle\langle 1|2(|\alpha_0|^2 + |\alpha_1|^2)\Big] \quad (57)$$

But we know that $|\alpha_0|^2 + |\alpha_1|^2 = 1$ thus:

$$\rho^{\mathcal{B}} = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}I. \quad (58)$$

This confirms that the state of Bob's qubit after Alice's measurement, but before Bob has learned the measurement result, is $I/2$ and it is independent upon the state of 'particle 3', as stated earlier.

Note that Bob's qubit is in a mixed state. Indeed:

$$Tr\left[\left(\frac{I}{2}\right)^2\right] = \frac{1}{2} < 1. \quad (59)$$

This is a remarkable result, the state of the pair 'particle 1' and 'particle 2' is a pure state, it is known exactly, while state of 'particle 2' is a mixed state.

Needless to say that the teleportation gedanken experiment described in this section does not violate the 'no-cloning theorem.' The state of 'particle 3' has not been cloned, it has been altered in the measurement process and as a result

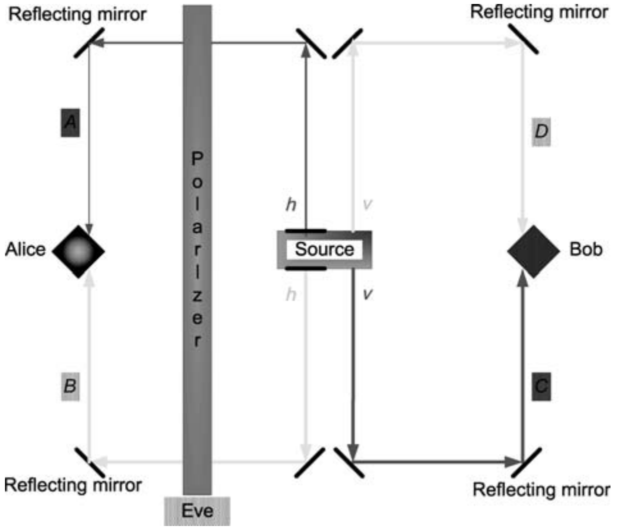


FIGURE 9. The teleportation experiment at University of Rome. The source generates a photon with horizontal polarization for Alice and one with vertical polarization for Bob. The entanglement is in the path selection. If Alice gets her photon via path *A*, then Bob gets his via path *C*; if Alice gets the photon via path *B* then Bob gets his via path *D*. Eve encodes her quantum information using a polarizer. Alice measures the polarization of the photon she receives and sends this classical information to Bob.

of teleportation 'particle 2' acquires the original state of 'particle 3.'

A demonstration of quantum teleportation was carried out in 1997 at the University of Rome by Francesco de Martini based upon an idea of Sandu Popescu and at about the same time at Innsbruck by Anton Zeilinger. In both experiments, the quantum state was teleported a few meters.

The experiment of de Martini is illustrated in Fig. 9 [28]. In this experiment, the information is double encoded into a single photon instead of two. The source generates two parametric downconverted[8] photons with opposite polarization, 'photon 1', with horizontal polarization, *h*, for Alice and 'photon 2', with vertical polarization, *v*, for Bob. The polarization entanglement of the two photons sent to Alice and Bob is converted into an entanglement of the paths followed by the two photons. A calcite crystal performs this conversion.

If 'photon 1' travels to Alice via path A then 'photon 2' travels to Bob via path *C*; if 'photon 1' travels via path *B*, then 'photon 2' travels via path *D*. Eve encodes her message in the polarization of the photon sent to Alice, 'photon 1.' Alice measures the polarization of the photon she receives from the source and sends the classical result to Bob. Finally, Bob performs the measurement suggested by Alice's result and he gets a photon with the polarization imposed by Eve.

In this experiment, the polarizer forces a certain polarization on 'photon 1' and because of the anti-correlation of 'photon 1' and 'photon 2' the latter is forced to an opposite polarization.

9. SUMMARY

In this paper, we overview quantum parallelism and quantum communication using entangled particles. In recent years, quantum computing and communication devices have been built. A 7 (seven) qubit liquid NMR quantum computer able to factor the integer 15 was built in late 1990s [29]. In February 2007, a Canadian company, D-Wave, demonstrated a 16 qubit quantum computer based on superconducting electronics and they announce plans to build a 1024 qubit quantum computer by the end of 2008. Also, applications of quantum cryptography seem ready for commercialization. In 2003, a successful quantum key distribution experiment over a distance of some 100 km has been announced.

Building quantum computing and communication devices faces tremendous technological and theoretical challenges. As Winston Churchill once said 'Success is the ability to go from failure to failure with no loss of enthusiasm.'

10. ACKNOWLEDGEMENTS

The Annual Boole Lecture Series in Informatics was established and is sponsored by the Boole Centre for Research in Informatics, the Cork Constraint Computation Centre, the Department of Computer Science and School of Mathematics, Applied Mathematics and Statistics. We are particulary indebted to our gracious hosts Dr. John P. Morrison Professor of Computer Science and Dr. Patrick Fitzpatrick, Dean of the College. The author wants to thank Professor Fionn Murtagh, the Editor in Chief of the Computer Journal, for his comments.

11. REFERENCES

[1] Heisenberg, W. (1933) The Development of Quantum Mechanics. *Nobel Lectures, Physics 1922–1942*, pp. 290–301.

[2] Shannon, C.E. (1949) Communication in the presence of noise. *Proc. IRE*, **37**, 10–21.

[3] Bennett, C.H. and Shor, P.W. (1998) Quantum information theory. *IEEE Trans. Inf. Theory*, **44**, 2724–2742.

[4] Feynman, R.P. (1986) Quantum mechanical computers. *Found. Phys.* **16**, 507–531.

[5] Feynman, R.P. (1996) *Lectures on Computation.* Addison-Wesley, Reading, MA.

[6] von Weizsäcker, C.F. (1971) Die Einheit der Natur (The Unity of Nature). (F. Zucker, ed.). Farrar, Straus, and Giroux.

[7] von Weizsäcker, C.F. and von Weizsäcker, E. (1972) Wiederaufname der begrifflichen Frage: Was ist Information?

[8] A parametric downconversion source uses a UV laser beam, which upon an interaction with a non-linear medium, a crystal of ammonium dihydrogen phosphate, generates two photons for one input photon.

(Revisting the fundamental question: what is information?). *Nova Acta Leopoldina*, **206**, 535–555.

[8] Shannon, C.E. and Weaver, W. (1963) *A Mathematical Theory of Communication.* University of Illinois Press, Urbana, IL.

[9] Boole, G. (1958) *An Investigation of the Laws of Thought*. Dover Publications, New Edition. ISBN-13: 978-0486600284.

[10] Feynman, R.P. (1982) Simulating physics with computers. *Int. J. Theoret. Phys.* **21**, 467–488.

[11] Küppers, B.O. (1990) *Information and the Origin of Life.* MIT Press, Cambridge, MA. ISBN 0-262-11141-X.

[12] Dirac, P.A.M. (1967) *The Principles of Quantum Mechanics* (4th edn). Clarendon Press, Oxford.

[13] Deutsch, D. (1985) Quantum theory, the church-turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, **400**, 97–117.

[14] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Log and Factoring. *Proc. 35 Annual Symp. Foundations of Computer Science*, pp. 124–134. IEEE Press, Piscataway, NJ.

[15] Grover, L.K. (1996) A fast quantum algorithm for database search. *Proc. ACM Symp. on Theory of Computing*, pp. 212–219. ACM Press, NY. See also updated version: http://arxiv.org/abs/quanth-ph/9605043.

[16] Bennett, C.H., Bernstein, E., Brassard, G. and Vazirani, U. (1997) Strengths and weaknesses of quantum computation. *SIAM J. Comput.*, **26**, 1510–1523.

[17] Zalka, C. (1999) *Grover's Quantum Searching Algorithm is Optimal. Phys. Rev. A*, **60**, 2746–2751.

[18] Furrow, B. (2006) *A panoply of quantum algorithms*. http://www.arxiv.org/abs/quant-ph/0606127.

[19] Lu, F. and Marinescu, D.C. (2005) An $R \parallel C_{\max}$ quantum scheduling algorithm. *Quantum Inf. Process.*, **6**, 159–178.

[20] Marinescu, D.C. and Marinescu, G.M. (2004) *Approaching Quantum Computing*. Prentice Hall, Upper Saddle River, NJ.

[21] von Neumann, J. (1955) *Mathematical Foundations of Quantum Mechanics.* (Trans. R.T. Bayer). Princeton University Press, Princeton, NJ.

[22] Nielsen, M.A. and Chuang, I.L. (2000) *Quantum Computing and Quantum Information.* Cambridge University Press.

[23] Terhal, B.M. (2004) *Is Entanglement Monogamous? IBM J. Res. Dev.*, **48**(1), 71–78.

[24] Bennett, C.H., DiVincenzo, D.P., Smolin, J.A. and Wooters, W.K. (1996) Mixed state entanglement and quantum error correction. *Phys. Rev. A*, **54**, 3824–3851.

[25] Bell, J.S. (1987) *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy.* Cambridge University Press, Cambridge.

[26] Einstein, A. (1949) *Albert Einstein, Philosopher–Scientist* (P.A. Schilpp, ed.), Autobiographical Notes in Library of Living Philosophers.

[27] Peres, A. (1995) *Quantum Theory: Concepts and Methods.* Kluwer Academic Press, Dordrecht, Boston, London.

[28] Brown, J. (1999) *The Quest for the Quantum Computer.* Simon and Schuster, New York, NY.

[29] Chuang, I.L., Vandersypen, L.M.K., Zhou, X., Leung, D.W. and Lloyd, S. (1998) Experimental realization of a quantum algorithm. *Nature*, **393**, 143–146.