QUANTUM COMPUTING AND COMMUNICATION

GABRIELA MOGOS

Quantum Information and Communication

Quantum Information and Communication

Gabriela Mogos

Prometeo researcher, Faculty of Informatics and Electronics, ESPOCH, Ecuador

Escuela Superior Politécnica de Chimborazo

Faculty of Informatics and Electronics

- 2015 -

ISBN: 978-9942-21-517

PUBLISHED BY PUBLISHER ESPOCH
www.espoch.com

First printing, October 2015

Contents

List of figures

Introduction

Quantum physics has had an enormous technological and societal impact. The importance of computers is such that is appropriate to say that we are now living in the *information age*. This information revolution became possible thanks to the invention of the transistor, that is, thanks to the synergy between computer science and quantum physics. Today, this synergy offers completely new opportunities and promises exciting advances in both fundamental science and technological application. We are referring here to the fact that quantum physics can be used to process and transmit information.

A quantum computer represents a radically different challenge: the aim is to build a machine based on quantum logic, that is, it processes the information and performs logic operations by exploiting the law of quantum physics.

The unit of quantum information is know as a qubit (the quantum counterpart of a classical bit) and a quantum computer may be viewed as a many-qubit system. A quantum computer is a system of many qubits, whose evolution can be controlled, and a quantum computation is a unitary transformation that acts on the many-qubit state describing the quantum computer.

The power of computers is due to typical quantum phenomena, such as the superposition of quantum states and entanglement. There is an inherent quantum parallelism associated with the superposition principle. In simple terms, a quantum computers can processes a large number of classical inputs in a single run. To be useful, quantum computers require the development of appropriate quantum software, that is, of efficient quantum algorithms.

In the 1980's Feynman suggested that a quantum computer based on quantum logic would be ideal for simulating quantum-physical systems and his ideas have spawned an active area of research in physics. In 1994, Peter Shor proposed a quantum algorithm that efficiently solves the prime-factorization problem: given a composite integer, find its prime factors. This is a central problem in computer science and it is conjectured, though not proven, that for a classical computer it is computationally difficult to find the

prime factors. Shor's algorithm efficiently solves the integer factorization problem and therefore it provides an exponential improvement in speed with respect to any known classical algorithm. Lov Grover has shown that quantum physics can also be useful for solving the problem of searching of a marked item in an unstructured database.

The technological challenge of realizing a quantum computer is very demanding: we need to be able to control the evolution of a large number of qubits for the time necessary to perform many quantum gates. Decoherence may be considered the ultimate obstacle to the practical realization of a quantum computer. Here the term decoherence denotes the decay of de quantum information stored in a quantum computer, due to the inevitable interaction of quantum computer with the environment. Such interaction affects the performance of a quantum computer, introducing errors into computation. Beside the problem of decoherence, we should also remark on the difficulty of finding new and efficient algorithms.

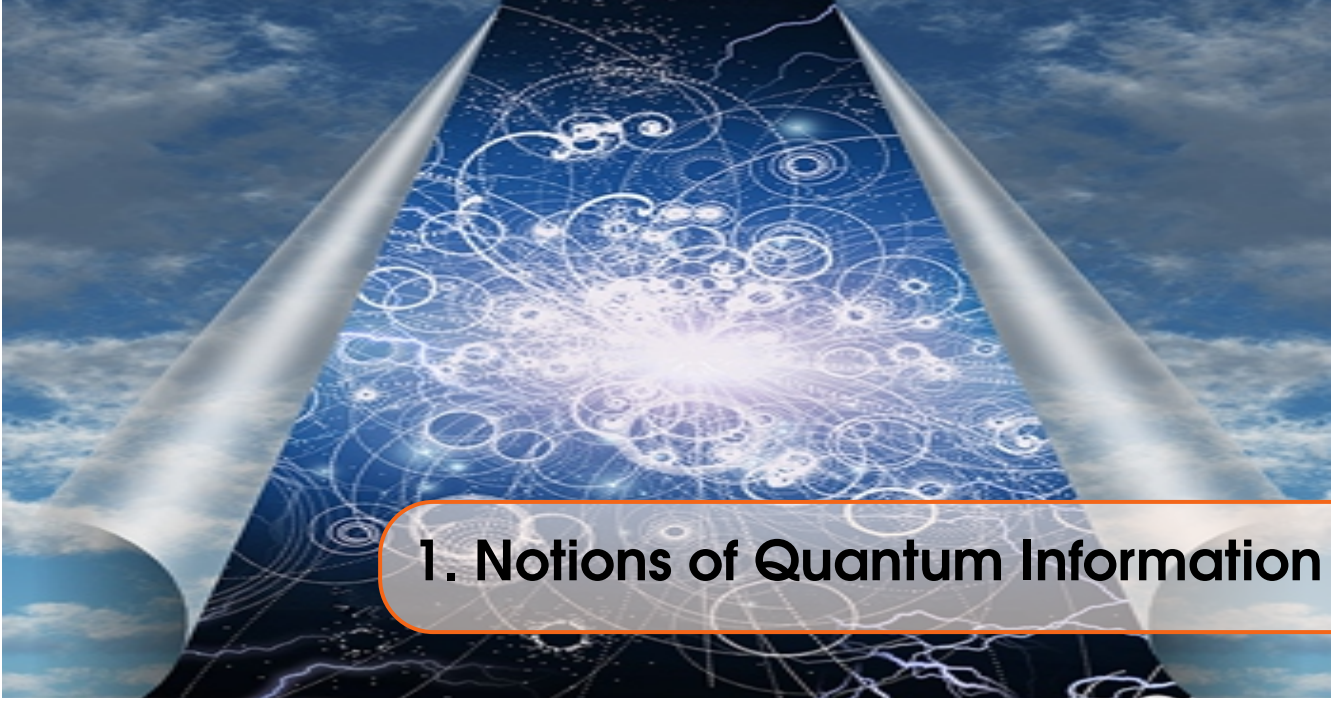
This book is support a courses in Quantum Information Theory, Quantum Computing and Quantum Cryptography and attempts to present the material in such way that it is accessible to advanced undergraduates and starting graduate students in Computer Science.

This book is an introduction to the field of quantum information. It is aimed at students who are new to the field and also at those who wish to make sense of the already bewildering and extensive literature. I have aimed to cover, in an introductory manner, what seem to me to be all of the most fundamental ideas in the field. The emphasis, throughout, is on theoretical aspects of the subject, not because these are the most important, but because it is only by understanding these that the true significance of practical developments can be appreciated.

This book is divided into three parts. The *Foundations of quantum physics* part provides a broad overview of the background material in physics and computer science necessary to understand quantum cryptography in depth. Chapter *Foundations of quantum physics* describes the fundamental elements needed to perform quantum computation, and present many elementary operations which may be used to develop more sophisticated applications of quantum computation; the quantum Fourier transform and how may be used to solve the factoring problems; the quantum search algorithm; the quantum error-correcting codes, etc.

The *Quantum Cryptography* part presents some procedures known as quantum cryptography or quantum key distribution, using quantum physics principles to enable provably secure distribution of private information, and methods of sharing the quantum secret. Four different protocols for quantum key distribution are presented in this chapter, together with the security level which can be reached by each protocol. It is presented the notion of quantum states entanglement, and also the modalities of their entanglement (partial or full entanglement).

Chapter *Quantum communication* covers thorough basic introduction to the quantum computing world and discusses quantum assisted computing and communications where we use the new paradigm to improve (assist) the performance of classical systems. Quantum computing and communications is one of the promising new fields at the dawn of the new millennium. This emerging topic has reach ed the age when not only physicists and mathematicians but engineers become more and more interested in it.



1. Notions of Quantum Information

1.1 Foundations of quantum physics

The formalism of quantum physics is based on a number of postulates. These postulates are in turn based on a wide range of experimental observations. In this chapter we present a formal discussion of these postulates, and how they can be used to extract quantitative information about microphysical systems. These postulates cannot be derived; they result from experiment. They represent the minimal set of assumptions needed to develop the theory of quantum mechanics. But how does one find out about the validity of these postulates?

Their validity cannot be determined directly; only an indirect inferential statement is possible. For this, one has to turn to the theory built upon these postulates: if the theory works, the postulates will be valid; otherwise they will make no sense. Quantum theory not only works, but works extremely well, and this represents its experimental justification. The accurate prediction power of quantum theory gives irrefutable evidence to the validity of the postulates upon which the theory is built.

1.1.1 The state space

The first postulate of the quantum physics delimitates the domain of development of quantum physics, which is the Hilbert space [46], linear algebra.

Postulate 1. To any isolated physical system is associated a complex vector space (Hilbert space), known as a *state space of the system*. The system is completely described by a *state vector*, which is a unit vector in the state space of the system. In order to describe the state vectors in quantum physics we use the *Dirac notation* [28] [29].

Quantum physics does not reveal, for a given physical system, neither the state space of the system, nor the state vector of the system.

1.1.2 Evolution of a quantum system

How does the state of a quantum system modify in time? This postulate gives indications about these changes.

Postulate 2. The evolution of a closed quantum system is described by a *unitary transformation*. If a quantum system at the time t_1 has the state $|\Psi\rangle$ and at the time t_2 the state $|\Psi'\rangle$, the relation can be written:

$$|\Psi'\rangle = U|\Psi\rangle$$

This postulate only applies to the closed systems, which means that it is available for the systems which do not interact with other systems [80]. Therefore, we can speak of an evolution of quantum systems in a continuous time. However, in reality things are different, and the systems interact among them. Thus, the postulate can be reformulated as it follows:

Postulate $2'$. The evolution in time of a closed quantum system is described by Schrödinger equation [81],

$$i\hbar\frac{d|\Psi\rangle}{dt} = H|\Psi\rangle$$

where $\hbar$ is a physical constant, called Planck's constant reduced (Planck's constant divided by 2π) whose value is $6,582 \times 10^{-16} eV \cdot s$, and H is a Hermitian operator known under the name of closed Hamiltonian system. The Hamiltonian operator describes the total energy state of a system. Knowing the Hamiltonian system determines the understanding of the complete dynamics of a system.

1.1.3 Quantum measurements

Until now we postulated that closed quantum systems evolve in agreement with an evolution operator, but we also need to determine what happens within the systems. The following postulate [67] describes the effects of the measurements over the quantum systems.

Postulate 3. Quantum measurements are described with the help of measurement operators $\{M_m\}$. They are operators acting in the measured space state system. The index m refers to the results of the measurement in the experiment. If the state quantum system is $|\Psi\rangle$ immediately before the measurement, then the probability of the existence of the result m is given by the expression:

$$p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle$$

and the state system after measurement is:

$$\frac{M_m|\Psi\rangle}{\sqrt{\langle\Psi|M_m^\dagger M_m|\Psi\rangle}}$$

Measurement operators satisfy the equation:

$$\sum_m M_m^\dagger M_m = I$$

This equation is transcribed as it follows:

$$1 = \sum_m p(m) = \sum_m \langle\Psi|M_m^\dagger M_m|\Psi\rangle.$$

1.1.4 Projective measurements

A more special case is the one of the projective measurements [67] used in many applications of the quantum computing.

A projective measurement is described by an observable M, a Hermitian operator which can be noticed in the state space of the system. The observable can be written:

$$M = \sum_m mP_m$$

where P_m is the projector in M's own space, with its eigenvalues m. The possible results of the measurements correspond to the eigenvalues m of observable. At the measurement state $|\Psi\rangle$, the probability to obtain the result m is given by:

$$p(m) = \langle\Psi|P_m|\Psi\rangle$$

and the state quantum system immediately after the measurement is:

$$\frac{P_m|\Psi\rangle}{\sqrt{p(m)}}.$$

1.1.5 Compound systems

Suppose that we are interested in a system made of at least two distinct physical systems. The following postulate is describing the way of the construction of the state space of the system made of the state spaces of the component systems [28] [29].

Postulate 4. The state space of the compound physical system is the tensor product between the state spaces of the component systems. Further more, if the systems are numbered from 1 to n and the system number i is in the state $|\Psi_i\rangle$, then the total state system is written: $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes ... \otimes |\Psi_n\rangle$.

As it is already known, according to the principle of the superposition from quantum physics, if $|x\rangle$ and $|y\rangle$ are two states of a quantum system, then any superposition $\alpha|x\rangle + \beta|y\rangle$ is a state of the quantum system, where $|\alpha|^2 + |\beta|^2 = 1$. It is obvious that for the compound systems if $|A\rangle$ is a state of the system A and $|B\rangle$ is a state of the system B, then it is possible to have a corresponding state $|A\rangle|B\rangle$ for the system AB. Applying the principle of the superposition on the product of the states, we obtain the tensor product to which the postulate makes reference.

1.1.6 The Einstein-Podolsky-Rosen paradox

An important characteristic appearing in quantum physics is the phenomenon of states entanglement. The basic concept of states entanglement used in quantum informatics relies on the team work of three researchers. In 1935 Einstein together with Boris Podolsky and Nathan Rosen published a study in which they were describing a fundamental "characteristic" of the theory of matter [35]. The Einstein-Podolsky-Rosen (EPR) effect presents its complete character (Ïn a complete theory there is an element corresponding to each element of reality"), its local character ("The real factual situation of the system A is independent of what is done with the system B, which is spatially separated from the former") and defines the element of the physical reality in the following way: Ïf, 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". EPR demonstrates experimentally that two quantum systems that interacted cannot be described by states independent between them (as in classical physics). Thus, between the two systems will exist quantum correlations, independently of their spatial separation. The Hilbert space associated to the mix (compound) system is the tensor product of the spaces Hilbert H_i of the i components of the system. We will use as an example the case of a bipartite quantum system: $H = H_1 \otimes H_2$.

The bases of the Hilbert space H are constructed starting from the tensor product of the basis vectors of the Hilbert spaces H_1 and H_2. If the Hilbert spaces H_1 and H_2 are bi-dimensional, having each the basis vectors $\{|i>_1, |j>_1\}$ and $\{|i>_2, |j>_2\}$, respectively, then the Hilbert space H is determined by four vectors: $\{|i>_1 |i>_2, |i>_1 |j>_2, |j>_1 |i>_2, |j>_1 |j>_2\}$.

Consequently, according to the principle of superposition, the general state in the Hilbert space H is an arbitrary superposition of such states, and we can write it as it follows:

$$|\Psi\rangle = \sum_{i,j=0}^{1} c_{ij} |i\rangle_{H_1} \otimes |j\rangle_{H_2}$$

or:

$$|\Psi\rangle = \sum_{i,j} c_{ij} |ij\rangle$$

where the first index in $|ij\rangle$ refers to the state existent in the Hilbert space H_1 and the second to the state in H_2. The state in H is called entangled if it cannot be written as a simple tensor product of the states $|i\rangle$ belonging to H_1 and $|j\rangle$ respectively, belonging to H_2.

A state $|\Psi\rangle$ is *entangled* if the component states are inseparable:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|ii\rangle_{12} + |jj\rangle_{12})$$

and it is *separable* if it can be written as a tensor product of the component states:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|ij\rangle_{12} + |jj\rangle_{12}) = \frac{1}{\sqrt{2}}(|i\rangle_1 + |j\rangle_1) \otimes |j\rangle_2 .$$

When two systems are entangled it is not possible to attribute them the individual state vectors.

1.1.7 The non-cloning theorem

The demonstration of non-cloning performed by Zürek, Dieks and Wootters in 1982 [104], is based on a simple application of the linearity of the unitary transformations. The purpose of the demonstration is to prove the impossibility of the realization of identical copies of an unknown quantum state.

Suppose that U is a unitary operator who is cloning all the quantum states as it follows: $U(|a0\rangle) = |aa\rangle$. Assuming that $|a\rangle$ and $|b\rangle$ are two orthogonal quantum states, then $U(|a0\rangle) = |aa\rangle$ and $U(|b0\rangle) = |bb\rangle$. We consider $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$. The application of the operator U to the state $|c\rangle$, means:

$$U|c0\rangle = \frac{1}{\sqrt{2}}(U|a0\rangle + U|b0\rangle) = \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)$$

If U is cloning the state $|c\rangle$, then:

$$U|c0\rangle = |cc\rangle = [\frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)][\frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)] = \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle)$$

which is not equal to $\frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)$. Therefore, the unitary operator cannot realize the clone of an unknown quantum state. We can formulate this result as follows:

Theorem 1.1.1 It is impossible to construct a machine able to clone the generic state of a qubit.

This theorem is a vital ingredient of the quantum cryptography, because does not allow to the possible invaders to realize copies of the cryptographic keys.

1.1.8 The principle of uncertainty - Heisenberg

An important characteristic [45] in quantum physics is that any attempt to distinguish between two non-orthogonal states of a quantum system is prone to failure. In order to demonstrate this statement, we assume to have a quantum system in one of the non-orthogonal states $|\Phi\rangle$ and $|\Psi\rangle$ respectively. In order to examine a general evolution of the quantum system, an auxiliary quantum system will be used (ancilla) with the state $|u\rangle$ and a unitary transformation. Suppose the system evolution leaves the state $|\Phi\rangle$ or $|\Psi\rangle$, unchanged, evolving only the ancilla state:

$$|\Phi\rangle \otimes |u\rangle \rightarrow |\Phi\rangle \otimes |v\rangle$$

respectively:

$$|\Psi\rangle \otimes |u\rangle \rightarrow |\Psi\rangle \otimes |v^{'}\rangle$$

where $|v\rangle$ and $|v^{'}\rangle$ are the final states of the auxiliary system (ancilla) in the two cases. After the scalar multiplication of the two equations, we will have:

$$(\langle u| \otimes \langle \Phi|)(|\Psi\rangle \otimes |u\rangle) = (\langle v| \otimes \langle \Phi|)(|\Psi\rangle \otimes |v^{'}\rangle)$$

$$\langle u|u\rangle \cdot \langle \Phi|\Psi\rangle = \langle v|v^{'}\rangle \cdot \langle \Phi|\Psi\rangle$$

$$1 = \langle v|v^{'}\rangle$$

The equation shows that for the different non-orthogonal states $\langle \Phi|\Psi\rangle \neq 0$, the final state $|v\rangle$ is the same with $|v^{'}\rangle$. In other words, given two non-orthogonal states of a quantum system, it is impossible to distinguish the final state in which the system will evolve starting from those two states.

1.1.9 The irreversibility of the measurements

The general measurement irremediably perturbs the state system. In order to emphasis this aspect, a photon in one of the polarization states will be used: vertical, horizontal, diagonal left (45^o) and diagonal right (135^o) respectively. A birefringent calcite crystal can be used to distinguish with certainty between the horizontally polarized photons, and the vertically polarized ones. Figure 1.1-a shows that only the horizontally polarized

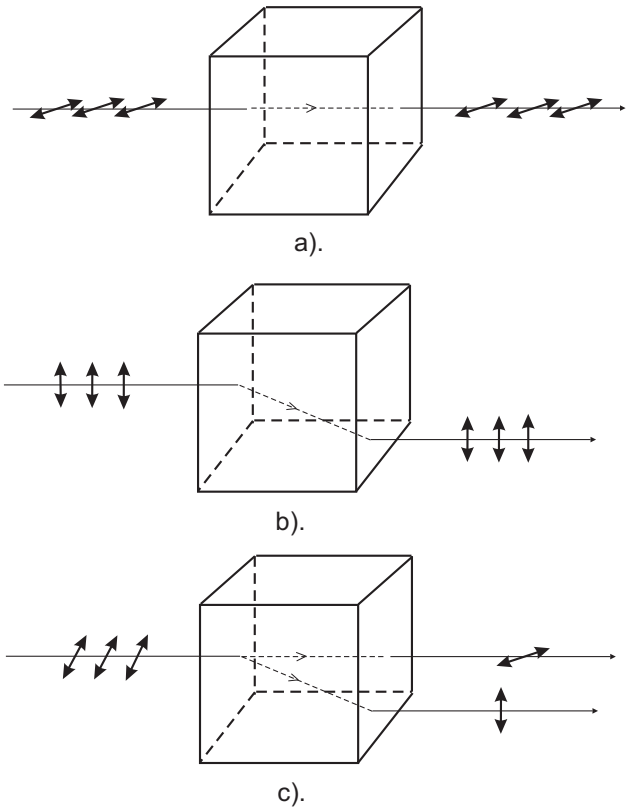


Figura 1.1: Calcite crystal - helps distinguishing the states of photons polarization.

photons will be able to pass through the crystal in a straight line, and figure 1.1-b, shows that the vertically polarized photons are pointed in another direction, which leads to the conclusion that the photons polarized like that will have deterministic routes when passing through the crystal. According to the quantum physics, we can say that a photon polarized in another direction (figure 1.1-c) when passing through a calcite crystal has a few options of the route to follow, the photon choosing eventually one of the routes, and suffering a re-polarization in that direction. Thus, for the diagonal polarization (45^o and 135^o respectively) the photon can choose equally one of the two directions, independent of the initial state of polarization.

If the photon is known to have a horizontal or vertical polarization, by a simple operation of adding some detectors it is possible to record it in the two directions. If the intention is to distinguish between the diagonally polarized photons, the system should be rotated (crystal and detector) by 45^o. In conclusion, when a photon in one of the four states of polarization is detected, a simple process of measurement will determine the state of perturbation, and the failure to determine the state of polarization. Thus, a measurement to determine the linearly polarized photons produces the perturbation of the diagonally polarized photons, and similarly, a measurement to determine the diagonally polarized photons produces the perturbation of the linearly polarized photons.

1.2 Qubits

In the theory of quantum informatics, the elementary information unit is the quantum bit - shortly, qubit [82]. A qubit is represented by a quantum system with two orthogonal states conventionally named $|0\rangle$ and $|1\rangle$. These states are forming a computing basis $\{|0\rangle, |1\rangle\}$, whose orthogonal characteristic leads to $\langle 0|1\rangle = 0$. As opposed to the classical bit which can take only two real values, the qubit can represent continuous states described by a unit vector in a complex bi-dimensional vector space. This bi-dimensional space is called *Hilbert space* [75]. A qubit can be either in the state $|0\rangle$, in the state $|1\rangle$, or in their superposition, expressed by the relation:

$$|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

where the coefficients α and β are arbitrary complex numbers normalized to the unit according to $|\alpha|^2 + |\beta|^2 = 1$.

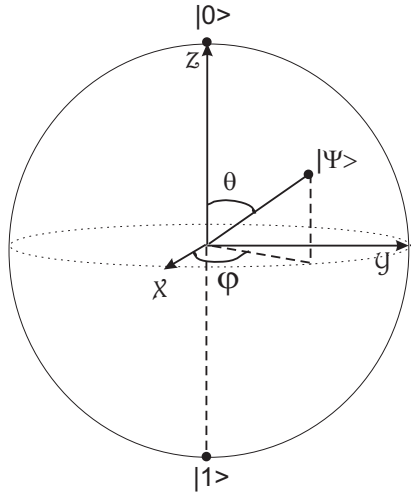


Figura 1.2: Bloch sphere.

The basis vectors of the Hilbert space associated to a qubit are written matriceally as it follows:

$$|0\rangle \doteq \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle \doteq \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.2}$$

The qubit can be geometrically represented as a dot on the Bloch sphere [17] (figure 1.2), which is a sphere with the ray equal to a unit, its state being written according to the polar coordinates as it follows:

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

When both coefficients of the superposition (1.1) are different from zero, the qubit has simultaneously the values 0 and 1, each with the probability of the corresponding amplitude α and β. This is the core of all the quantum algorithms using the principle

of superposition, and which in combination with the quantum interference determines a massive parallelism helping to solve the problems that in classical informatics are unsolvable.

A pair of qubits can exist in any state like the following:

$$|\Psi_2\rangle = c_{00}|00\rangle + c_{10}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \tag{1.3}$$

where the complex coefficients c_x $(x = 00, ..., 11)$ are normalized as it follows: $\sum_x |c_x|^2 = 1$. In general, the compound state $|\Psi_2\rangle$ is an entangled state of the two qubits, meaning that they cannot be factorized in a product of the following states of the two qubits: $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$. Only when the coefficients of the equation (1.3) satisfy: $c_{00} = \alpha\alpha'$, $c_{01} = \alpha\beta'$, $c_{10} = \beta\alpha'$ and $c_{11} = \beta\beta'$, the decomposition in states product is possible, case in which the state is factorizable.

The most important example of a two-qubit (bipartite) system of entangled states are the Bell states, known as the Einstein-Podolsky-Rosen (EPR) states:

$$\begin{array}{ll} |B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) & |B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) & |B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{array} \tag{1.4}$$

They are maximally entangled, i.e. if it is desired to remove the information belonging to a qubit, the measurement of the other qubit belonging to the pair can give a completely random result. The Bell states are used mostly in the protocols of quantum communication: teleportation, code density.

1.3 Qutrits

The qutrit [63] replaces the classical trit, and it is the unit of information in ternary quantum computing. It is represented as a unit vector in state space, which is a complex three-dimensional vector space (three-dimensional Hilbert space), $H(3)$. In the computing basis, the basis vectors (or the basis states) in H(3) using Dirac notation, are written: $|1\rangle$, $|2\rangle$ and $|3\rangle$, where $|1\rangle = (1,0,0)^T$, $|2\rangle = (0,1,0)^T$ and $|3\rangle = (0,0,1)^T$. An arbitrated vector $|\Psi\rangle$ in $H(3)$ can be expressed as a linear combination:

$$|\Psi\rangle = c_1|1\rangle + c_2|2\rangle + c_3|3\rangle$$

where $c_1, c_2, c_3 \in \mathbf{C}$ and $|c_1|^2 + |c_2|^2 + |c_3|^2 = 1$. The real number $|c_i|^2$ is the probability that the state vector $|\Psi\rangle$ be found in the basis of measurement i. In practice, the qubits were obtained using "bi-photons"[22] [57], i.e. from a pair of photons in symmetrical Fock states.

1.4 Qubit registers

In general, a register of n-qubits has 2^n mutual orthogonal states that in the computing basis look like that $|x_1x_2...x_n\rangle$, where $x_k \in \{0,1\}$, for $1 \leq k \leq n$. Thus, any state of a register can be specified with 2^n complex amplitudes c_x, $x \equiv x_1x_2...x_n$ by:

$$|\Psi_n\rangle = \sum_x c_x|x\rangle, \quad \sum_x |c_x|^2 = 1 \tag{1.5}$$

In the case of qubit registers, by analogy with the Bell states, their maximum entanglement is known as the Greenberger-Horne-Zeilinger states (GHZ):

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000..,0\rangle \pm |111..,1\rangle) \tag{1.6}$$

Another family of multi-qubit entangled states are the W states, which look as it follows:

$$|W_n\rangle = \frac{1}{\sqrt{N}}(|00..,01\rangle + |00..,10\rangle + ... + |01..,00\rangle + |10..,00\rangle) \tag{1.7}$$

These W states of n qubits consist of an equality of the superposition of n states, each of them with exactly a qubit in the state $|1\rangle$ and all the others in the state $|0\rangle$.

Until now, only two states quantum systems were presented. However, these considerations are also available for general quantum systems with n states of possible bases. Similar to the case of the two state systems, an n state system has associated a Hilbert space with n perpendicular axes (dim $H = n$) corresponding to the n measurable states of the quantum system.

A quantum system can also be analyzed only in the basis states; however, it can exist in any superposition of the basis states as long as it is not measured. For example, a quantum register containing two qubits is described by the Hilbert space $H \otimes H$ (tensor product), of size $2^2 = 4$, and the basis:

$$\begin{aligned} |0\rangle \otimes |0\rangle &= |0\rangle|0\rangle = |00\rangle, \\ |0\rangle \otimes |1\rangle &= |0\rangle|1\rangle = |01\rangle, \\ |1\rangle \otimes |0\rangle &= |1\rangle|0\rangle = |10\rangle, \\ |1\rangle \otimes |1\rangle &= |1\rangle|1\rangle = |11\rangle. \end{aligned} \tag{1.8}$$

Using matrices, these vectors are expressed by:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{1.9}$$

$$|01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Similarly, a quantum register with n qubits, is described by a Hilbert space $H \otimes H \otimes \cdots \otimes H$ (tensor product of n times the Hilbert space associated to a qubit) of size 2^n. The basis vectors of this space are obtained similarly to the register formed of two qubits, considering the tensor product n times the basis vectors of the H space combined in all the possible ways: $|010\cdots0\rangle$, $|011\cdots0\rangle$, etc.

A set of n qubits forms a register of size n. The space associated to these quantum states is a Hilbert space of size 2^n. Meanwhile, the state of a bit from a classical register formed of n bits is described in the binary notation by an integer $k \in \{0,1,...,2^n-1\}$ looking like:

$$k = k_{n-1}2^{n-1} + ... + k_1 2 + k_0 \tag{1.10}$$

where $k_0, k_1, ..., k_{n-1} \in \{0,1\}$ are binary digits, the qubit state from a quantum register of size n written as it follows:

$$|\Psi\rangle = \sum_{k=0}^{2^n-1} C_k |k\rangle \tag{1.11}$$

where $|k\rangle = |k_{n-1}\rangle ... |k_1\rangle |k_0\rangle$, k_j representing the state of the j-th qubit, and

$$\sum_{k=0}^{2^n-1} |C_k|^2 = 1$$

We emphasize that the number of states of the computing basis in this superposition is 2^n, fact which leads to new computing possibilities. Thus, when a computation is made on a classical computer, the different entries need separate runs, while a quantum computer is able to compute in a single run for an arbitrary (finite) number of entries. This emphasizes the extraordinary computing capacity of a quantum computer as compared to that of a classical computer, for certain classical algorithms existing the possibility to find quantum correspondents with lower complexity.

1.5 Quantum circuits

Similarly to the classical case, the quantum computing can be represented by circuits with quantum "wire"transporting qubits and quantum logic gates. The quantum gates used can be one-qubit or multi-qubit ones, acting over a single, and over several qubits respectively. Due to the fact that quantum computing is reversible, the number of inputs and outputs should be the same in any quantum gate. Further, only quantum gates always keeping the norm $\sum_x |c_x|^2 = 1$ for the vectors register $|\Psi_n\rangle$ are allowed in quantum circuits. The logic gates can be represented by unitary operators of the quantum mechanics acting on the state of a register.

1.5.1 Single qubit gates

In general, the logic gate [3] on a single qubit is described by a unitary matrix 2×2 which looks like:

$$U = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

which transforms the state of a qubit $|0\rangle$ in $\alpha|0\rangle+\beta|1\rangle$ and the state $|1\rangle$ in $\gamma|0\rangle+\delta|1\rangle$.

Single qubit gates are: Unit I; Hadamard H; Pauli X, Y, Z and the phase gate S. The matrices corresponding to these operators are written below:

$$\begin{array}{ll} I=\begin{bmatrix}1&0\\0&1\end{bmatrix} & H=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix} \\ X=\begin{bmatrix}0&1\\1&0\end{bmatrix} & Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix} \\ Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix} & S=\begin{bmatrix}1&0\\0&i\end{bmatrix} \end{array}$$

The action of a gate is equivalent to the corresponding operator action applied on the input states of the qubit. For example, the gate Unit, where we have $I|\Psi_1\rangle=|\Psi_1\rangle$ which leaves the qubit state unchanged.

Hadamard gate [44] [77] transforms the initial qubit state $|0\rangle$ or $|1\rangle$ in a superposition of these basic states:

$$\begin{array}{lll} H|0\rangle & \longrightarrow & \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\equiv|+\rangle \\ H|1\rangle & \longrightarrow & \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\equiv|-\rangle \end{array} \tag{1.12}$$

We can write it in a compact expression:

$$H|x\rangle=\sum_z\frac{(-1)^{xz}|z\rangle}{\sqrt{2}} \tag{1.13}$$

where $x,z\in\{0,1\}$. Consequently, for an arbitrary state $|\Psi_1\rangle$ represented by the equation (1.1), the application of the *Hadamard* gate means:

$$H|\Psi_1\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix}\longrightarrow\frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta\\\alpha-\beta\end{bmatrix}=\frac{1}{\sqrt{2}}[(\alpha+\beta)|0\rangle+(\alpha-\beta)|1\rangle] \tag{1.14}$$

The X, Y and Z gates are equivalent to Pauli operators for spin $-\frac{1}{2}$: σ_x, σ_y and σ_z respectively. The X gate shifts the qubit state as it follows:

$$\begin{array}{c} X|0\rangle\longrightarrow|1\rangle \\ X|1\rangle\longrightarrow|0\rangle \\ X|\Psi_1\rangle=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix}\longrightarrow\begin{bmatrix}\beta\\\alpha\end{bmatrix}=(\beta|0\rangle+\alpha|1\rangle) \end{array} \tag{1.15}$$

which is a quantum analogy of the *NOT* gate.

Similarly, for the Y gate we have:

$$\begin{array}{c} Y|0\rangle\longrightarrow i|1\rangle \\ Y|1\rangle\longrightarrow -i|0\rangle \\ Y|\Psi_1\rangle=\begin{bmatrix}0&-i\\i&0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix}\longrightarrow\begin{bmatrix}-i\beta\\i\alpha\end{bmatrix}=-i(\beta|0\rangle-\alpha|1\rangle) \end{array} \tag{1.16}$$

The Z gate introduces a phase shift π for the state $|1\rangle$ while the state $|0\rangle$ remains unchanged.

$$\begin{array}{c} Z|0\rangle \longrightarrow |0\rangle \\ Z|1\rangle \longrightarrow -|1\rangle \end{array}$$
$$Z|\Psi_1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \longrightarrow \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = (\alpha|0\rangle - \beta|1\rangle) \tag{1.17}$$

If the qubit is in one of the states $|+\rangle$ or $|-\rangle$ (using the Hadamard gate), the action of the Z gate determines an interchange between these states: $Z|\pm\rangle \longrightarrow |\mp\rangle$.

In the end, the S gate introduces a phase shift π for the state $|1\rangle$ and leaves the state $|0\rangle$ unchanged:

$$\begin{array}{c} S|0\rangle \longrightarrow |0\rangle \\ S|1\rangle \longrightarrow i|1\rangle \end{array}$$
$$S|\Psi_1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \longrightarrow \begin{bmatrix} \alpha \\ i\beta \end{bmatrix} = (\alpha|0\rangle + i\beta|1\rangle) \tag{1.18}$$

The relations between the gates on a single qubit are the following: $HH = XX = YY = ZZ = I$, $h = \frac{1}{\sqrt{2}}(X+Z)$, $XY = iZ$, $XZ = -iY$, $YZ = iX$, etc. In general, an arbitrary U transformation for a qubit can be decomposed in the product of the rotation operators $R_y(\theta)$ and $R_z(\theta')$ and a total phase factor given through $e^{i\alpha}$.

1.5.2 Multiple qubit gates

The gates [7] acting on two qubits are: the $C-NOT$ gate (controlled-NOT), the $SWAP$ gate, the $controlled-Z$ gate and the general $controlled-U$ [64].

The $C-NOT$ ***gate*** is a quantum analogy of the classical XOR, reversible gate, $|a\rangle|b\rangle \rightarrow |a\rangle|a \oplus b\rangle$, with $(a,b \in \{0,1\})$, where the target qubit b (the one below) shifts its state if the control qubit a (the one above) is in the state $|1\rangle$ and it remains unchanged if the control qubit is $|0\rangle$.

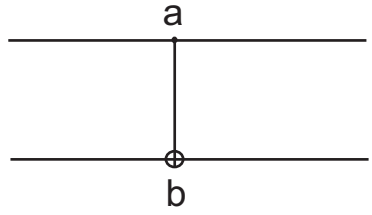


Figura 1.3: The C-NOT gate.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The SWAP gate is the analogy of the classical transformations $CROSSOVER$: $|a\rangle|b\rangle \rightarrow |b\rangle|a\rangle$ which interchanges the states of two qubits.

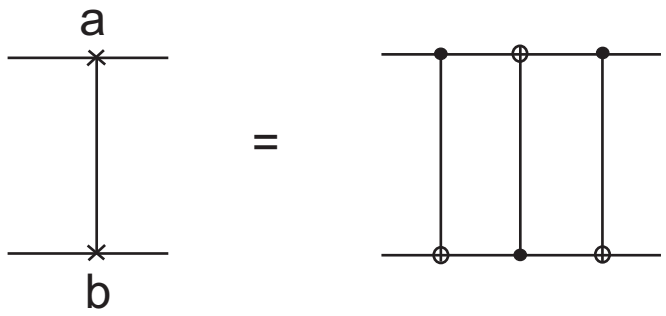


Figura 1.4: The SWAP gate.

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The $SWAP$ gate can be implemented by the triple action of the $C-NOT$ gate.

The controlled-Z gate has the following effect: $|a\rangle|b\rangle \rightarrow (-1)^{ab}|a\rangle|b\rangle$, where the Z operator is applied on the target qubit, conditioned by the control qubit state.

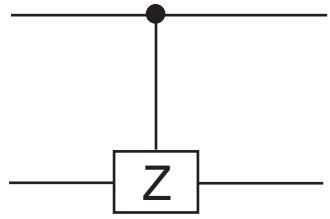


Figura 1.5: The controlled-Z gate.

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Generally speaking, any ***controlled-U*** transformation is performed according to figure (1.6) where the application of the operator U on the qubit target is conditioned if the control qubit state is $|1\rangle$.

The outcome of the application of the $C-NOT$ gate on a general two-qubit state represented by the equation 1.4, can be computed as it follows:

$$C-NOT|\Psi_2\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{bmatrix} = \begin{bmatrix} c_{00} \\ c_{01} \\ c_{11} \\ c_{10} \end{bmatrix} \tag{1.19}$$

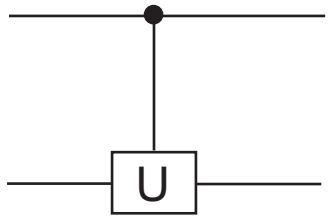


Figura 1.6: The controlled-U gate.

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \boxed{U} & \\ 0 & 0 & & \end{bmatrix}$$

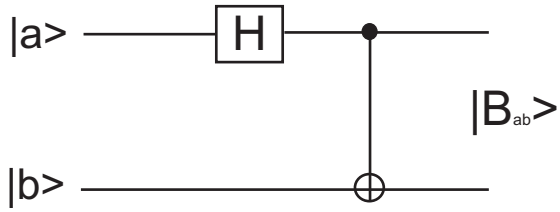


Figura 1.7: The circuit generating the four Bell states $|B_{ab}\rangle$.

IN	OUT
$\|00\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
$\|01\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$
$\|10\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
$\|11\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

Cuadro 1.1: The Bell states.

which shows that the coefficients of the states $|10\rangle$ and $|11\rangle$ are interchangeable. A similar procedure is used for the determination of the action of any gate on two qubits.

The Controlled-Controlled-NOT ($CC-NOT$) gate acts on three qubits, and it represents the quantum alternative of the classical gate Toffoli [95]: $|a\rangle|b\rangle|c\rangle \rightarrow |a\rangle|b\rangle|ab \oplus c\rangle$, hence the target qubit c shifts its state if the control qubits a and b are simultaneously in the state $|1\rangle$, otherwise it remains unchanged.

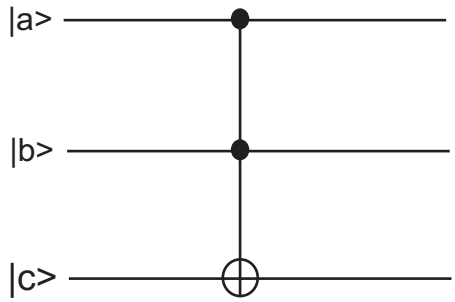


Figura 1.8: The CC-NOT gate.

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Any unitary transformation (gate) on several qubits, the Toffoli gate included, can be efficiently simulated by circuits containing operators (gates) on one or two qubits. Therefore, combinations between the gates on a qubit and $C-NOT$ gates can determine the obtaining of gates on any number of qubits, with an arbitrary number of target and control qubits.

1.6 Qubit measurement

A very important element of the quantum computing is the qubit measurement. The measurement of a single qubit using a basis $\{|0\rangle, |1\rangle\}$, means the obtaining of two results

defined by two measurement operators: $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$ respectively. We notice that each operator is Hermitian, i.e. $M_0^2 = M_0$, $M_1^2 = M_1$, $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. The probability to obtain 0 as result of the measurement is:

$$p(0) = \langle\Psi|M_0^\dagger M_0|\Psi\rangle = \langle\Psi|M_0|\Psi\rangle$$

Similarly, the probability to obtain the result 1 at the measurement is $p(1) = |b|^2$. The state after the measurement in the two cases is therefore:

$$\frac{M_0|\Psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle$$

and

$$\frac{M_1|\Psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle.$$

respectively.

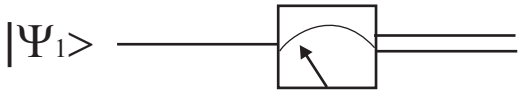


Figura 1.9: Symbol used for the representation of the qubit measurement.

In quantum circuits, the symbol used for the measuring instruments of the qubit can be seen in figure 1.9.

1.7 The qubit as a physical system

Until now we considered the qubit as an abstract mathematical object - a unit vector in a complex bi-dimensional space - with no specification about the physical systems by which we could represent it. In general, any quantum physical system with a pair of well established states could be a qubit. The choice of the system is dictated by practical considerations. Next we will present the simplest two-state quantum system, the polarized photon, system which can be obtained in laboratory conditions.

A two-state (two-level) quantum system is the polarized photon. The photon is a particle that can be obtained in laboratory conditions, allowing in the same time its observation and study. Experimentally, in order to obtain the photon, very little equipment is necessary, i.e. a source of powerful light, like a source of laser light, polarization filters, and a screen for the projection of light. The filters used are disposed between the light source and the screen. In the experiment, we assume that we do not know the type of polarization of the fascicle, and three filters of polarization are used: x - which allows only the passing of the horizontally polarized photons, y - which allows only the passing of the vertically polarized photons, and 45^o - respectively - which allows only the passing of the polarized photons under a 45^0 angle. If the filter x is placed between the fascicle and the screen (fig.1.10-a), the intensity of the fascicle obtained on the screen is half of its initial intensity, which means that only the horizontally polarized photons passed through the filter x. If the filter y is also added (fig.1.10-b), there will be nothing on the

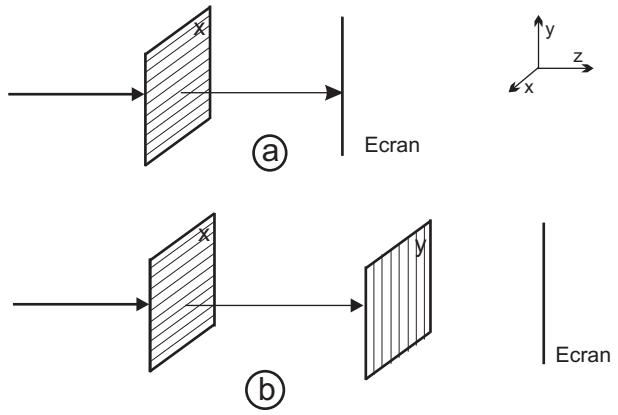


Figura 1.10: Vertically or horizontally polarized photon passes between the two perpendicular polarizers.

screen, because it is impossible that the horizontally polarized fascicle, which passed through the filter x, could also pass through the filter y. If between the two filters x and y the filter at 45^o is interposed (fig.1.11), a small quantity of will be visible on the screen, more precisely an eighth of the initial one. A polarized state of a photon can be modeled

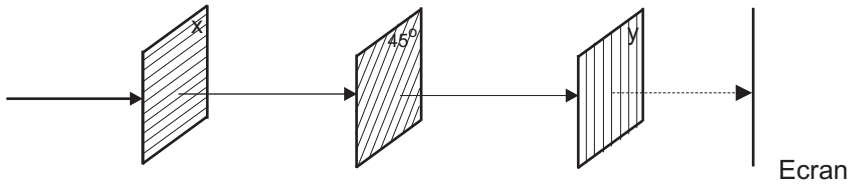


Figura 1.11: A polarizer at $45^o$is inserted between the two polarizers x and y.

through a unit vector with a determined direction. We assume that the two directions of linear polarization (vertical and horizontal) form an orthogonal system $\{|\uparrow\rangle, |\rightarrow\rangle\}$. Any arbitrary polarization state can be represented in this orthogonal system as a linear combination $\alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ of the basis vectors $|\uparrow\rangle$ and $|\rightarrow\rangle$. The coefficients α and β are complex numbers satisfying the relation: $|\alpha|^2 + |\beta|^2 = 1$. Considering also the case of the circular polarization of the photon (left and right), we could speak of a new basis $\{|\nwarrow\rangle, |\nearrow\rangle\}$ for the representation of an arbitrary polarization state of the photon.

1.8 Quantum parallelism

The quantum parallelism [30] is a fundamental characteristic of several quantum algorithms. The quantum parallelism allows quantum computers evaluate simultaneously a function $f(x)$ for many values different from x. We assume that $f(x) : \{0,1\} \rightarrow \{0,1\}$ is a function with one-qubit domain and co-domain. We suppose that y is a register target and x a data register over which an U_f, unitary transformation is applied, defined by:

$$|x,y\rangle \rightarrow |x, y \oplus f(x)\rangle.$$

the easiest way to demonstrate the quantum parallelism is to evaluate a function $f(x)$ for all the possible values of x. The scheme of the circuit for the demonstration of quantum parallelism is presented in Figure 1.12, where x is the data register, and y is the target register.

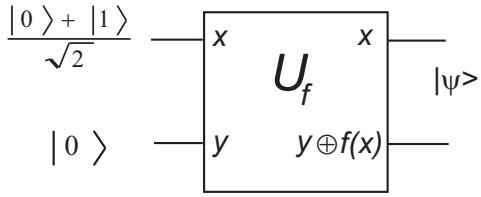


Figura 1.12: Circuit for the demonstration of quantum parallelism, simultaneous evaluation of $f(0)$ and $f(1)$.

The simplest case is that in which both the data register and the target register have each one qubit (the data qubit with the state $|0\rangle$, the target qubit with the state $|1\rangle$).

Applying the *Hadamard* gate, the data register is prepared as a superposition of states which looks like:

$$(|0\rangle + |1\rangle)/\sqrt{2}.$$

By the application of U_f, transformation, we will have:

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

As we can see, the expression contains information about $f(0)$ and $f(1)$, which means that the evaluation of the function $f(x)$ is performed simultaneously for the two values. As opposed to the classical parallelism where the construction of separate circuits for $f(x)$ simultaneous computation is necessary, in the quantum case, the circuit allows the simultaneous evaluation of $f(x)$ for several values of x.

Generalizing the quantum parallelism for the case when input data are represented from an n qubits, register, the preparation of the initial state imposes the application of the Hadamard gates on the whole register, followed afterwards by the implementation of U_f. The state obtained is written:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

Quantum parallelism makes possible the simultaneous evaluation of all the possible values of the function $f(x)$, allowing the extraction of the information for more than a value of $f(x)$ from the states of the superposition given by $\sum_x |x, f(x)\rangle$.

1.9 Quantum algorithms

The realization of a quantum computation requires:
- input data;

- logic gates;
- measuring instruments.

The operations of quantum computation consist of the following steps:

1. *Initialization* - the preparation of all the register qubits in the initial state;
2. *Input* - loading the input data;
3. *The computation itself* - the realization of the desired unitary transformations by the application of sequences of logic gates according to the program;
4. *Output* - the measurement of the final state of a register using the computing basis.

Next we will present several quantum algorithms for data processing.

1.9.1 Deutsch's algorithm

This is the simplest algorithm [31] [32], it uses two qubits, and it has the purpose to demonstrate the quantum parallelism power of computation.

Assume a Boolean function $f : \{0,1\} \longrightarrow \{0,1\}$, which has as argument a single qubit x and a quantum "oracle" or a quantum "black-box"U_f evaluating the function according to:

$$|x,y\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle.$$

The purpose is to determine the property of function f i.e. if this is *constant* $f(0) = f(1)$ or *balanced* $f(0) \neq f(1)$. In classical computing, in order to evaluate the function we need to evaluate the function $f(x)$ two times, first for $x = 0$, then for $x = 1$, after which the results are measured. The quantum computing permits U_f appealing only once.

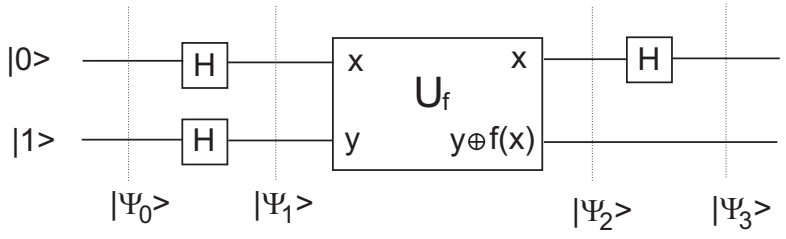


Figura 1.13: Deutsch's algorithm.

Deutsch's algorithm is presented in figure 1.13, and like the circuit used in the demonstration of the quantum parallelism, it contains a data register (x) and a target register (y). The registries of Deutsch algorithm are made of a qubit each, and the circuit contains Hadamard gates H and U_f - a control gate defined by the relation:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle . \tag{1.20}$$

The input state in the circuit is:

$$|\Psi_0\rangle = |0\rangle |1\rangle \tag{1.21}$$

Next we will analyze the action of the gates of the circuit on the input data (states). Deutsch's algorithm starts by obtaining the combined states of each register by the application of Hadamard operators (gates).

The first Hadamard operator acting over the state $|0\rangle$ determines the state:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} =$$

$$= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{1.22}$$

i.e.:

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{1.23}$$

We notice that the new state obtained is a combination of $|0\rangle$ and $|1\rangle$.

We will obtain a similar outcome when applying the Hadamard operator to the state $|1\rangle$:

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} =$$

$$= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{1.24}$$

i.e.:

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{1.25}$$

According to these results, the first pair of Hadamard gates transforms the initial state 1.21 in:

$$\frac{1}{2} (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \tag{1.26}$$

The following step consists in the application of the U_f controlled gate. We will analyze the action of the gate over every term of the expression above.

$$U_f |x\rangle \otimes (|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle) \tag{1.27}$$

Taking into account the equation (1.20) we have:

$$U_f |x\rangle \otimes (|0\rangle - |1\rangle) = |x\rangle \otimes (|0\rangle - |1\rangle \oplus f(x)) \tag{1.28}$$

If we choose $|x\rangle = |0\rangle$ and $f(x) = 0$, we obtain:

$$U_f |0\rangle \otimes (|0\rangle - |1\rangle) = |0\rangle - |1\rangle = (-1)^0 (|0\rangle - |1\rangle) = (-1)^{f(x)} (|0\rangle - |1\rangle) \tag{1.29}$$

and if we choose $|x\rangle = |0\rangle$ and $f(x) = 1$, the result will be:

$$U_f |0\rangle \otimes (|0\rangle - |1\rangle) = |1\rangle - |0\rangle = (-1)^1 (|0\rangle - |1\rangle) = (-1)^{f(x)} (|0\rangle - |1\rangle) \tag{1.30}$$

From the relations (1.29) and (1.30), we can deduce:

$$U_f |x\rangle \otimes (|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle)$$

which is the relation (1.27) itself.

We apply the formula (1.26) on the state expressed by the relation (1.30):

$$U_f \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle] \otimes (|0\rangle - |1\rangle) \quad (1.31)$$

The second Hadamard gate must be applied, especially on the term from the square parentheses of the relation (1.31). We obtain the final state:

$$\frac{1}{2}[(-1)^{f(0)} H |0\rangle + (-1)^{f(1)} H |1\rangle] \otimes (|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}[(-1)^{f(0)} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle + (-1)^{f(1)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$= \frac{1}{2}[((-1)^{f(0)} + (-1)^{f(1)}) |0\rangle + ((-1)^{f(0)} - (-1)^{f(1)}) |1\rangle] \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (1.32)$$

From this relation we can conclude the following:

1. If the function $f(x)$ is *constant* ($f(0) = f(1)$), then we have:

$$(-1)^{f(0)} - (-1)^{f(1)} = 0$$

and the right parenthesis from the relation (1.32) becomes:

$$\frac{1}{2}[(-1)^{f(0)} + (-1)^{f(1)}] |0\rangle = \pm |0\rangle \quad (1.33)$$

and the relation (1.33) represents the final state of the data register (x).

2. If the function $f(x)$ is *balanced* ($f(0) \neq f(1)$), then we have:

$$(-1)^{f(0)} + (-1)^{f(1)} = 0$$

and the final state of the data register is:

$$\frac{1}{2}[(-1)^{f(0)} - (-1)^{f(1)}] |1\rangle = \pm |1\rangle \quad (1.34)$$

In conclusion, in order to determine if the function $f(x)$ is constant or balanced we must measure the final state of the data register. If the result of the measurement is $|0\rangle$ then the function $f(x)$ is constant, and if we obtain $|1\rangle$ then the function $f(x)$ is balanced. Deutsch's algorithm perfectly illustrates the power of the quantum parallelism, evaluating the function in a single step.

1.9.2 Deutsch-Jozsa's algorithm

Deutsch-Jozsa's algorithm [33] is the generalization of Deutsch's algorithm for the case of several qubits. We assume that the Boolean function $f:\{0,1\}^n \longrightarrow \{0,1\}$ with n-qubits argument $q \equiv q_1 q_2 ... q_n$ is computed by the U_f quantum "black-boxïn the following way: $|x,y\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle$. Similar to the previous algorithm, we analyze if the function is *constant* $f(x) = const$ so that its values are identical for all $0 \leq q < 2^k$, or *balanced*, i.e. $f(x) = 0$ for exactly half of all possible q and $f(x) = 1$ for the other half of q values.

In the classical computing, it is necessary to evaluate the function $f(x)$ at least twice for two different arguments q and $q^{'}$ to determine the values of the function f in q and $q^{'}$. If the values obtained are different, the function is balanced, and if they are equal, the U_f operator should appeal for another argument $q^{"} \neq q, q^{'}$ and the result should be compared with the previous values of f. Again, if these values are different, then we can conclude that the function is balanced, otherwise another q is tested. Only after $2^k/2+1$ interrogations of the function with different arguments, but with the same outcome, we can conclude that the function is constant.

The quantum circuit presented in figure (1.14) solves the problem by a single evaluation of f for a superposition of all q. Let us analyze the register states.

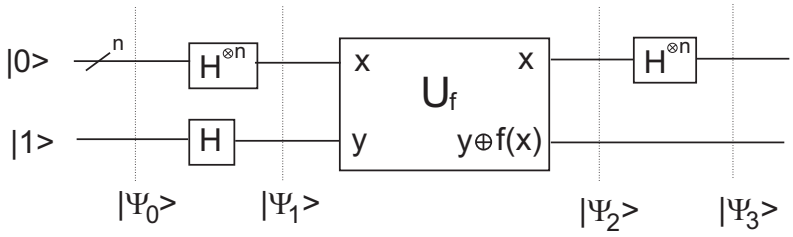


Figura 1.14: Deutsch-Jozsa's algorithm.

The input state is:

$$|\Psi_0\rangle = |0\rangle^{\otimes n} |1\rangle \tag{1.35}$$

which after the application of the $n+1$ parallel *Hadamard* gates transforms in:

$$|\Psi_1\rangle = (\frac{|0\rangle + |1\rangle}{\sqrt{2}})...(\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.36}$$

According to the similar step from Deutsch's algorithm, the effect on the operator U_f must be evaluated:

$$|\Psi_2\rangle = \sum \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.37}$$

In the end, the effect of the last set of *Hadamard* gates must be evaluated. For a single qubit, *Hadamard* effect can be written:

$$H|x\rangle = \sum_{z\in\{0,1\}} \frac{(-1)^{xz} |z\rangle}{\sqrt{2}} \tag{1.38}$$

Extending to the entire register, we obtain:

$$H^{\otimes n}|x_1,..,x_n\rangle = \sum_{z_1,...,z_n} \frac{(-1)^{x_1z_1+...+x_nz_n}|z_1,...,z_n\rangle}{\sqrt{2^n}} \tag{1.39}$$

We write: $x_1z_1+...+x_nz_n = x\cdot z$, and we obtain:

$$|\Psi_3\rangle = \sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{\sqrt{2^n}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) \tag{1.40}$$

The amplitude of the register is given by:

$$\sum_x \frac{(-1)^{f(x)}}{2^n}$$

In conclusion, if the function f is *constant*, all the 2^n terms forming the sum will have the same sign ("+" for $f(x)=0$ and "-" for $f(x)=1$), so as $\sum_x \frac{(-1)^{f(x)}}{2^n} = \pm 1$.

If the function f is constant, the measurement of the output data register shows that all the qubits are in the state $|0\rangle$.

When the function is *balanced*, exactly half of the terms forming the sum have the sign "+" and the other half of the terms have the sign "-", which means that $\sum_x \frac{(-1)^{f(x)}}{2^n} = 0$. The result of the measurement of the output data shows that at least one qubit from the data register is in the state $|1\rangle$, hence the function is balanced.

The particular cases of Deutsch-Jozsa's algorithm were developed by Bernstein-Vazirani and Simon.

1.9.3 Bernstein-Vazirani's algorithm

Bernstein-Vazirani's algorithm [14] is a Deutsch's algorithm for which $f(x) = a\cdot x$. Knowing that the final state in the case of Deutsch's algorithm (1.32), replacing $f(x)$, we obtain the final register state a in the case of Bernstein-Vazirani's algorithm:

$$\frac{1}{2^n}(\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{a\cdot x}(-1)^{x\cdot y}|y\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{1.41}$$

Assume the sum is over x:

$$\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}(-1)^{x\cdot y}|y\rangle$$

If $a \neq y$, then we will obtain zero.

If $a = y$, then:

$$(-1)^{a\cdot x}(-1)^{x\cdot y}|y\rangle = 1$$

The final state becomes:

$$(\sum_y \delta_{a,y}|y\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = |a\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

and the measurement of the control lines in this case returns a.

1.9.4 Simon's algorithm

Assume the function $f : \{0,1\}^n \longrightarrow \{0,1\}^n$. There is a range s, so as $f(x) = f(y) \Longleftrightarrow y = x \oplus s$, for any $x, y \in \{0,1\}$. The problem consists in determining s.

Simon proposes an algorithm [92] which starting from a register $|x\rangle$ can compute efficiently $|x\rangle |f(x)\rangle$ in n steps. The algorithm is presented in figure 1.15, with the

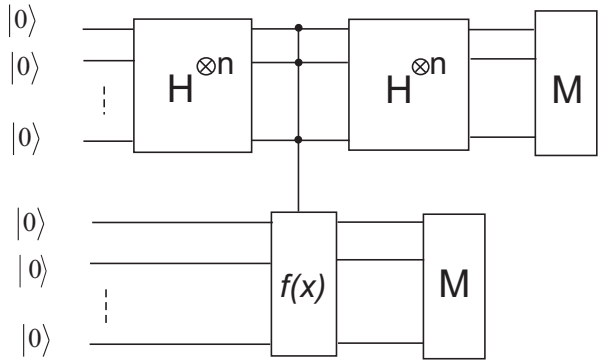


Figura 1.15: Simon's algorithm.

following steps:

1. The initial state:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

2. After applying f the state becomes:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

3. Measuring $|f(x)\rangle$, we obtain:

$$\frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle) |f(x)\rangle$$

4. H Hadamard gate applies for each qubit for $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$ leading to:

$$\frac{1}{2^{n/2}\sqrt{2}} \sum_{y \in \{0,1\}^n} ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) |y\rangle$$

where $x \cdot y = \sum_i (x_i \cdot y_i) \pmod 2$.

5. Measuring $(-1)^{xy} + (-1)^{(x \oplus s)y}$ we have zero if $x \cdot y \neq (x \oplus s) \cdot y$.
If the result is y, then $x \cdot y = (x \oplus s) \cdot y$, which means that $x \cdot y = 0$.
6. Steps $1-5$ are repeated n-times, obtaining a linear system:

$$s \cdot y^i = 0, \; i = 1, ..., n$$

7. The solution system is unique.

1.9.5 Grover's algorithm

The search quantum algorithm was invented by Grover [41] [42] and offers a square speed of search in the unsorted data bases.

Assume we have a list of $N = 2^k$ elements d_x stored in a computer memory.

The indices x, get different integer values, $x = 0, 1, ..., N-1$, represent the position of each element on the list. We are searching the position x_w of an element d_w satisfying a certain condition $C(d_w)$. The algorithm contains a "black-box"U_f evaluating a function f returning 1, if the condition $C(d_w)$ and zero are accomplished as it follows.

$$f(x) = \begin{cases} 1, & \text{if } C(d_w) = \text{TRUE} \\ 0, & \text{if } C(d_w) = \text{FALSE} \end{cases}$$

The purpose is to find the index x_w for which $f(x) = 1$.

Assume that only an element from the data base satisfies the condition C.

In the classical case of the algorithm the function f for each element of the data base should be evaluated, starting from $x = 0$ until the position x_m of the desired element is determined. As an average, there are necessary $N/2$ interrogations before x_m is identified.

The quantum algorithm is capable to find x_w with a probability very close to the unit after only $\sqrt{N}$ appeals of U_f. Initially, the data register made of k-qubits is prepared in

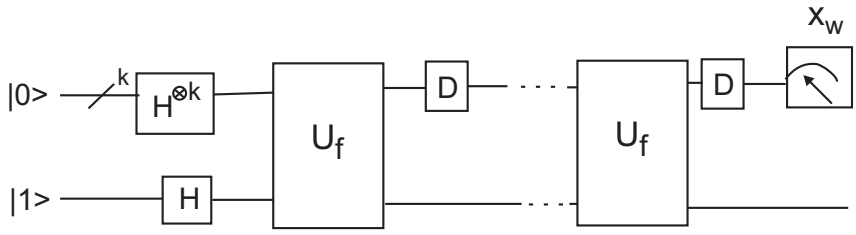


Figura 1.16: The implementation circuit of Grover's algorithm.

the state $|0\rangle \equiv |0\rangle^{\otimes k}$ and the register is made only of a single qubit in the state $|1\rangle$. Like in the case of Deutsch-Jozsa's algorithm, applying the *Hadamard* gates to the data and target qubit transforms the register in equal superposition of the states of all x:

$$H^{\otimes k}|0\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle \equiv |s\rangle \tag{1.42}$$

and the target register state is $(|0\rangle - |1\rangle)/\sqrt{2}$.

After the preparation, U_f is appealed, then there is the D transformation of $O(\sqrt{N})$ times, and in the end the state register is measured. With a probability close to the unity, the result, which was given by a sequence of 0 and 1, is a binary representation of the index x_w of the searched element.

Let us detail the two transformations used by the algorithm, the U_f oracle and the Grover D operator.

As we noticed in figure (1.17), the oracle has an input register of k-bits in the state $|x\rangle$ and a single target qubit in the state $(|0\rangle - |1\rangle)/\sqrt{2}$.

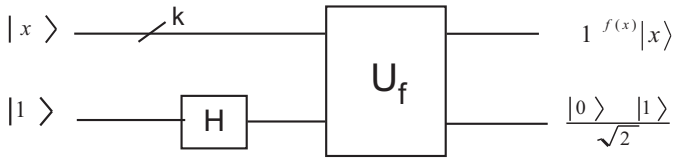


Figura 1.17: The action of U_f induces a phase-flip $(-1)^{f(x)}$.

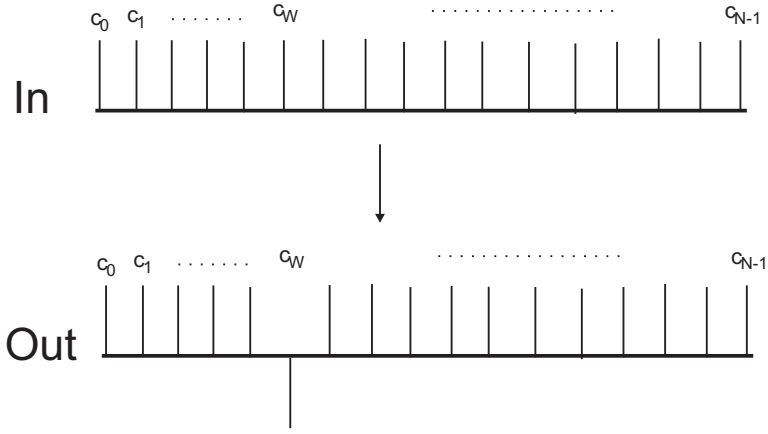


Figura 1.18: When the entry is in a superposition of states, only the amplitude c_w of the searched state changes its sign.

After their entanglement we obtain the state $|\Psi_{k+1}^{in}\rangle = |x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. The output register state goes through a phase-flip $(-1)^{f(x)}$,

$$|\Psi_{k+1}^{out}\rangle = U_f|\Psi_{k+1}^{in}\rangle = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

This happens only with the state we are searching $|x_w\rangle$, for which $f(x) = 1$, which is shifting its sign, while the other states $|x\rangle$ remain unchanged.

Therefore, the input register is prepared in a state superposition for all $0 \leq x < 2^k$, $|\Psi_{k+1}^{in}\rangle = \sum_x c_x|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, and regarding the output, the amplitude c_w of the state $|x_w\rangle$ changes its sign,

$$|\Psi_{k+1}^{out}\rangle = U_f|\Psi_{k+1}^{in}\rangle = (-c_w|x_w\rangle + \sum_{x\neq x_w} c_x|x\rangle)\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{1.43}$$

The second transformation, also called "inversion the mean", is described by the D operator acting on the data register:

$$D = H^{\otimes k}(2|0\rangle\langle 0| - I)H^{\otimes k} = 2|s\rangle\langle s| - I \tag{1.44}$$

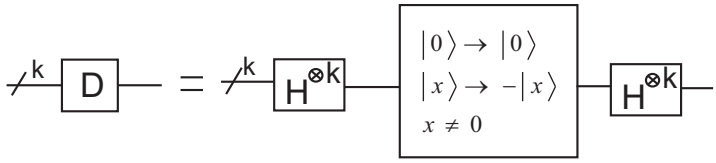


Figura 1.19: The D transformation is realized by the sequence of $H^{\otimes k}$, the conditional phase-flip $|0\rangle \to |0\rangle$, $|x\rangle \to -|x\rangle$ $(1 \leq x < 2^k)$ and transformations $H^{\otimes k}$.

D operator applied on the data register in a state of arbitrary superposition $|\Psi_k^{in}\rangle = \sum_x c_x|x\rangle$, produces:

$$|\Psi_k^{out}\rangle = D|\Psi_k^{in}\rangle = \sum_x (2\langle c\rangle - c_x)|x\rangle, \tag{1.45}$$

where $\langle c\rangle \equiv \sum_x c_x/N$ is the average value of all c_x.

Analyzing the entire scheme of Grover's algorithm, we notice that after several iterations of the sequence $U_f D$, the amplitude $|c_w\rangle$ amplifies by $O(1/\sqrt{N})$. Consequently, after $O(\sqrt{N})$ iterations, the probability to find the data register in the state $|x_w\rangle$ gets closer to 1 ($|c_w|^2 \sim 1$), and the measurement has the outcome x_w, which is the position itself of the searched element.

Grover's search algorithm can be generalized when the data base contains more than an element satisfying the condition C. The implementation of the quantum oracle U_f requires resources (auxiliary qubits and quantum logic gates) proportional to the necessities imposed by the computation of function f.

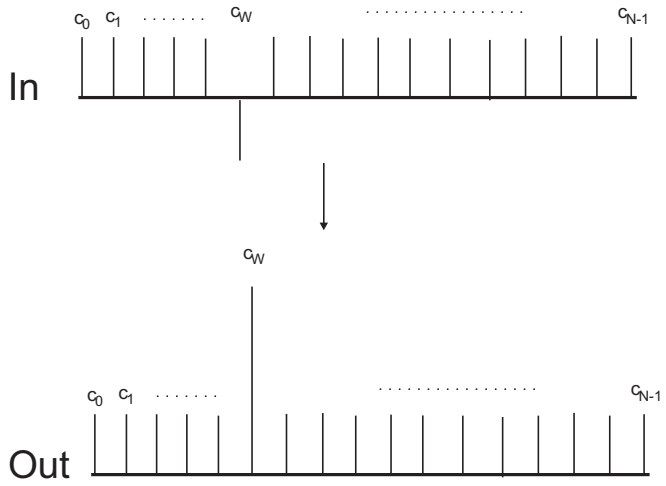


Figura 1.20: The increase of the amplitude $|c_w\rangle$ of the state which suffered a phase-flip.

1.9.6 Quantum Fourier transform and its applications

Quantum Fourier transform

The Fourier transform is the most important operation used in a large category of mathematical problems. Many problems of physics and computation from the real world, using frequently sets of discrete data, are efficiently analyzed and solved with the help of the discrete Fourier transforms, which transform a set of complex numbers $x_0, x_1, ..., x_{N-1}$ to another set $y_0, y_1, ..., y_{N-1}$, according to:

$$y_n = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp(\frac{2\pi i jn}{N}) x_j \tag{1.46}$$

The set $\{x_j\}$ can be thought of conventionally as the representation of a vector in a complex N-dimensional vector space, and the set $\{y_j\}$, the vector rotated under the action of Fourier transform, where $\sum |y_j|^2 = \sum |x_j|^2$.

Quantum Fourier transform [74] [71] is a transformation similar to the classical one. However, the notation convention is different. Quantum Fourier transform [68] in an orthonormal basis $|0\rangle, ..., |N-1\rangle$ is defined as a linear operator acting as it follows:

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \exp(\frac{2\pi i jn}{N}) |n\rangle \tag{1.47}$$

Similarly, the action over an arbitrary state can be written:

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{n=0}^{N-1} y_n |n\rangle \tag{1.48}$$

where amplitudes y_n are discrete Fourier transforms of the amplitudes x_j. This transformation is unitary, and can be implemented as a dynamic of quantum computing.

We assume that $N = 2^n$, where n is an integer and a computing basis $|0\rangle, ...|2^n - 1\rangle$ for n qubits.

We will express the state $|j\rangle$ using the binary representation $j = j_1 j_2 ... j_n$. More formally, $j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$.

We will adopt the notation $0.j_l j_{l+1} ... j_m$ for the binary representation $j_1/2 + j_{l+1}/4 + ... + j_m/2^{m-l+1}$. Quantum Fourier transform can be represented as it follows:

$$|j_1, ..., j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle)}{2^{n/2}} \quad (1.49)$$

This product can be considered as the definition of quantum Fourier transform. We can build a quantum circuit implementing the Fourier transform, a clear proof that quantum Fourier transform is unitary.

Using the equation (1.47) and the representation (1.49), we obtain:

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} |k\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} e^{2\pi i j(\sum_{l=1}^{n} k_l 2^{-l})} |k_1 ... k_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i jk_l 2^{-l}} |k_l\rangle = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} [\sum_{k_l=0}^{1} e^{2\pi i jk_l} |k_l\rangle] =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} [|0\rangle + 2^{2\pi i j 2^{-l}} |1\rangle] =$$

$$= \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle)}{2^{n/2}} \quad (1.50)$$

The representation of this product makes it easy to deduct a circuit for the quantum Fourier transform (figure 1.21).

The R_k gate is a unitary transformation:

$$R_d = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

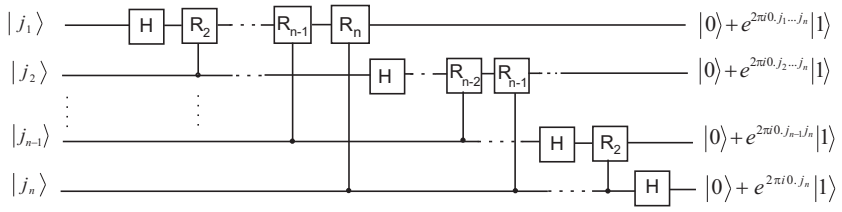


Figura 1.21: Circuit for quantum Fourier transform.

The initial state is $|j_1 ... j_n\rangle$:

1. After applying the *Hadamard* gate on the first qubit we obtain:

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 ... j_n\rangle$$

if $e^{2\pi i 0.j_1} = -1$ then $j_1 = 1$, otherwise $+1$.

2. The $controlled - R_2$ gate applies on the second step. R_2 action has as a result the phase shift if $|j_2\rangle$ is $|1\rangle$ or no effect if $|j_2\rangle$ is $|0\rangle$. We obtain:

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2 \ldots j_n\rangle$$

We continue to apply the $controlled - R_3$, R_4 gates, up to R_n, each of them adding an extra bit to the coefficient of phase of the first one $|1\rangle$.

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)|j_2 \ldots j_n\rangle$$

Similarly we apply the procedure on the second qubit. $Hadamard$ gate determines the state:

$$\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2}|1\rangle)|j_3 \ldots j_n\rangle$$

and the $controlled - R_2$ up to R_{n-1} gates produces:

$$\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle)|j_3 \ldots j_n\rangle$$

We continue in the same manner with each qubit, obtaining the final state:

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)|j_3 \ldots j_n\rangle$$

In order to reverse the qubits order, *SWAP* operators are used, and the qubits state is:

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle) \tag{1.51}$$

We obtained the equation (1.50) which was the desired outcome.

Phase computation using quantum Fourier transform

The Fourier transform is the key of a general procedure named phase computation, the key to many quantum algorithms.

We assume that a unitary U operator with its own vector $|u\rangle$ with its eigenvalues $e^{2\pi i\varphi}$, where the value of φ is unknown. The purpose of this algorithm is the computation of φ. For this, we assume a "black-box" capable to create the state $|u\rangle$ and to execute the $controlled - U^{2^j}$, operator for non-negative integers j. The necessity of the use of this oracle indicates the fact that the phase computation procedure is not a complete quantum algorithm in its true meaning. The phase computation procedure is in fact a "subroutine", which in combination with other subroutines creates a complex algorithm.

The phase computation procedure uses two registers. The first register contains t-qubits which initially are in the state $|0\rangle$. The choice of t depends on two things: the accuracy with which it is desired to obtain φ and the probability that the computation procedure is performed successfully.

The second register begins in the state $|u\rangle$ and contains as many qubits as are necessary for storing $|u\rangle$. In figure (1.22) is presented the phase computation procedure.

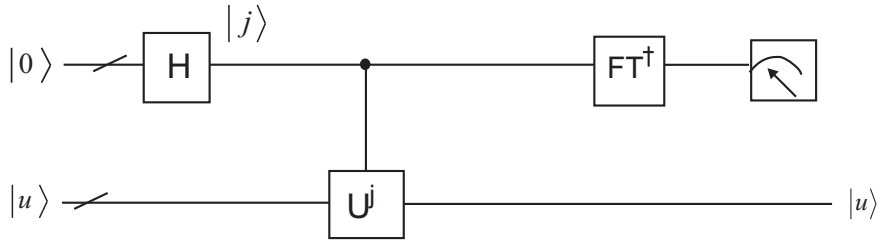


Figura 1.22: The schematic general procedure of the phase computation.

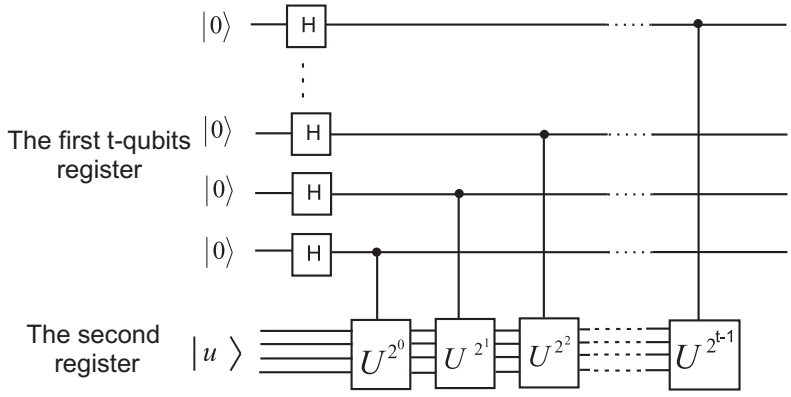


Figura 1.23: The first step of the phase computation procedure.

Phase computation is made in two steps.

First, *Hadamard* transform applies on the first register, then the controlled-U operators apply on the second register, with the successive raising of the power of 2. The final state of the first register is easy to see:

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle)(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle)...(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle) = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i \varphi k}|k\rangle \tag{1.52}$$

The second register was omitted during the whole computing operation, having the state $|u\rangle$.

The second step in the phase computation procedure is applying the reverse of quantum Fourier transform on the first register. This is obtained by reversing the quantum Fourier circuit previously presented in $\Theta(t^2)$ steps. The third and final step in phase computation is reading the first register state resulted.

We assume that φ can be expressed in exactly t-bits, as it follows: $\varphi = 0.\varphi_1...\varphi_t$. Then the state 1.52 obtained on the first step can be written:

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle)(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle)...(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2...\varphi_t}|1\rangle) \tag{1.53}$$

The second step of the computation procedure is to apply the reverse of quantum Fourier

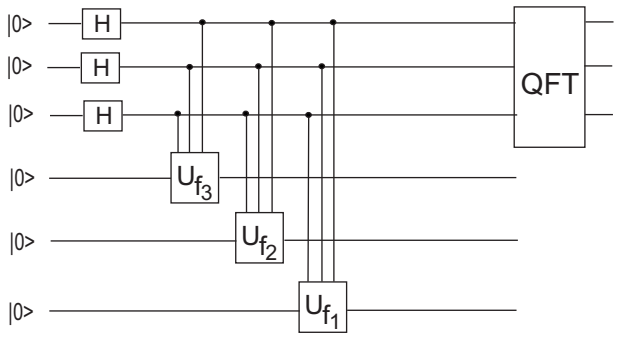


Figura 1.24: Shor's algorithm.

transform. Comparing the previous equations with the product of Fourier transform (1.49), we notice that the state resulted on the second step can be written as the product of the states $|\varphi_1\varphi_2...\varphi_t\rangle$.

A measurement in the computing basis will determine the obtaining of φ. The essential point of the procedure is represented by the reverse of Fourier transform which realizes the transformation:

$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle = |\widetilde{\varphi}\rangle|u\rangle$$

where $|\widetilde{\varphi}\rangle$ shows a state which is a good estimate of φ when it is measured.

1.9.7 Shor's algorithm. Determination of the period

Peter Shor replaced Hadamard gates from Simon's algorithm with quantum Fourier transform (figure 1.24), obtaining the scheme of a new algorithm [88] [90] for the determination of the period of a function $f : \mathbb{N} \ni x \to f(x) \in \mathbb{N}$.

A function is periodical, with period r, if:

$$f(x) = f(x+kr)$$

for any integer k.

The problem is approached both from a classical and a quantum point of view, using a finite number of values as input and output data, the function f being defined as it follows:

$$f : \{0,1\}^n \longrightarrow \{0,1\}^n, r \in [1,2^n]$$

Similar to Simon's algorithm, Hadamard gates will generate a superposition of states for the upper lines (the interval between 0 and 2^n-1):

$$\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle$$

The following step is represented by the action of the U_{f_k} gates from the lower lines, which will generate the state:

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

where:

$$|f(x)\rangle=|f_{n-1}(x)\rangle\otimes|f_{n-2}(x)\rangle\otimes...\otimes|f_0(x)\rangle$$

Assuming that the function is periodical, with period r, we can say that the same values of the function f correspond to x_0, x_0+r, x_0+2r etc., obtaining the state:

$$\frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle\otimes|f(x_0)\rangle$$

where A is an integer from the interval $[0,2^n]$. The application of the quantum Fourier transform determines the interference of the qubits from the upper lines with the ones from the lower lines, as it follows:

$$\begin{aligned}F(\frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle\otimes|f(x_0)\rangle) &= \frac{1}{\sqrt{A2^n}}\sum_{y=0}^{2^n-1}\sum_{j=0}^{A}e^{2\pi i(x_0+jr)y/2^n}|y\rangle= \\ &= \frac{1}{\sqrt{A2^n}}\sum_{y=0}^{2^n-1}e^{2\pi ix_0y/2^n}\sum_{j=0}^{A}e^{2\pi ijry/2^n}|y\rangle\end{aligned}$$

If this state is measured, the probability to determine the state $|y\rangle$ is given by the square of the amplitude, as it follows:

$$\frac{A}{2^n}\left|\frac{1}{A}\sum_{j=0}^{A}e^{2\pi ijry/2^n}\right|^2 \tag{1.54}$$

We assume that 2^n is divided exactly by the period r, then $A=2^n/r$ and $A/2^n=1/r$. The relation 1.54 becomes:

$$\frac{1}{r}\left|\frac{1}{A}\sum_{j=0}^{A}e^{2\pi ijy/A}\right|^2$$

For $y=A$, we have:

$$\frac{1}{r}\left|\frac{1}{A}(e^{2\pi i0}+e^{2\pi i1}+e^{2\pi i2}+...)\right|^2=$$

$$=\frac{1}{r}\left|\frac{1}{A}(1+1+1+...)\right|^2==\frac{1}{r}\left|\frac{1}{A}A\right|^2=\frac{1}{r}$$

For $y = 2A$, we have:

$$\frac{1}{r}\left|\frac{1}{A}(e^{2\pi i0} + e^{2\pi i2} + e^{2\pi i4} + ...)\right|^2 =$$

$$\frac{1}{r}\left|\frac{1}{A}(1+1+1+...)\right|^2 = \frac{1}{r}\left|\frac{1}{A}A\right|^2 = \frac{1}{r}$$

At the practical measurement we obtain $y \in \{A, 2A, 3A, ...rA\}$. Starting from this, it will be easy to determine A and knowing the domain 2^n, we can determine the period:

$$r = \frac{2^n}{A}$$

The period determination procedure can help decrypting the RSA system.

Steps to Shor's algorithm

Shor's algorithm for factoring an integer n requires the realization of the following sequence of steps:

Step 1

Determine if the number n is a prime, an even number, or an integer power of a prime number. If it is, there are efficient classical algorithms for determining the factorization, so as the use of Shor's algorithm would not be necessary. This step of the algorithm can be performed on a classical computer.

Step 2

Pick an integer q that is the power of 2 so that the relation $n^2 \leq q \leq 2n^2$ is verified. This step of the algorithm can be performed on a classical computer.

Step 3

Pick a random integer x that is prime to n. Since there are efficient classical methods for the realization of this step, this step of the algorithm can also be performed on classical computers.

Step 4

Create a quantum register of memory and partition it into two parts, register 1 and register 2 respectively. This state of the quantum computer is given by: $|reg1, reg2\rangle$. Register 1 must be large enough to represent integers up to the value $q-1$, and register 2 must permit the representation of the integers up to the value $n-1$. The computation for determining the number of qubits necessary for the two parts of the quantum register can be performed on a classical computer.

Step 5

Load register 1 with a superposition of all integers from 0 to $q-1$. Load register 2 with the 0 state. This operation would be performed by our quantum computer. At this point, the state of the quantum register is:

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,0\rangle \tag{1.55}$$

Step 6

Apply the transformation $x^a \bmod n$ to each number of register 1 and store the result in register 2. Due to the property of quantum parallelism these operations will take

only one step, hence the quantum computer will compute only $x^{|a\rangle} \bmod \text{n}$, where $|a\rangle$ is the superposition of states created in step 5. This step can be performed on a quantum computer. At this point, the state of the quantum register is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod \text{n}\rangle \tag{1.56}$$

Step 7

Measure the register 2 and observe some value k. This has the effect of collapsing register 1 in a superposition of the values $0, 1, \ldots q-1$ so as:

$$x^a \bmod \text{n} = k \tag{1.57}$$

This operation can be performed on a quantum computer. The state of the quantum register after this step is:

$$\frac{1}{\sqrt{\|A\|}} \sum_{a \in A} |a, k\rangle \tag{1.58}$$

where A is the set of elements a with the property that $x^a \bmod \text{n} = k$ and $\|A\|$ is the cardinal of the set A.

Step 8

Compute the discrete Fourier transform of the register 1. The discrete Fourier transform is applied to a state $|a\rangle$ shifting it in the following manner:

$$|a\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c\rangle^* \, e^{2\pi i a c/q} \tag{1.59}$$

Due to the property of quantum parallelism, this step of Shor's algorithm can be performed by the quantum computer in a single step. After applying the Fourier transform, the state of the register becomes:

$$\frac{1}{\|A\|} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c, k\rangle^* \, e^{2\pi i a' c/q} \tag{1.60}$$

Step 9

Measure the state of register 1 obtaining the value m, which is almost certain a multiple of q/r, where r is the period of the function. This step is performed on a quantum computer.

Step 10

Determine r on a classical computer, based on the knowledge of m and q.

Step 11

After determining the period r, a factor of the number n can be determined by the computation of greatest common divisor $gcd(x^{r/2} - 1, n)$ and $gcd(x^{r/2} + 1, n)$. If a factor of the number n was not obtained, then go back to *step 4* of Shor's algorithm.

This final step is done on a classical computer.

Shor's algorithm might fail for multiple reasons: the discrete Fourier transform used in *step 9* can produce 0 making impossible the processing in *step 10*, the algorithm can produce factors of n on 1 or n.

Conclusions regarding Shor's algorithm

Taking into account the principle of superposition in quantum systems, memory components of atomic size or even smaller could be created. The use of quantum registries opens the way to the exponential acceleration of the computation speed based on the principle of quantum parallelism.

Peter Shor discovered an algorithm permitting the factorization of large numbers, being one of the first important algorithms discovered in the field of quantum computing. Besides, this algorithm was a turning point in the field of quantum computing, being the first algorithm really important. As long as an adequate hardware for quantum computing will exist, the decrypting of the present security schemes will be made easy with the help of Shor's algorithm.

1.10 Quantum errors

The errors are inevitable, they appear anywhere, and computers are no exception. Though modern computers are extremely secure, the communication through networks is more and more exposed to errors produced by noises and imperfections. The technology associated to the quantum information processing is at the beginning of its development, and it has a long way to go until it will get to the implementation of secure digital technologies. As the information encoded in qubits used in the communication protocols is very fragile nowadays, there were developed a few methods to protect it, and to correct the errors. The errors related to this specific information are classified as it follows:

- *internal errors*, which have as source the imperfections of the equipment design, the software and hardware errors; errors in initial and final calibration of the measuring instruments.

- *external errors*, produced by the interaction with the environment. The interaction of the qubits with the external environment leads to the perturbation of the quantum system by the appearance of two phenomena: dissipation and decoherence.

The dissipation is the phenomenon in which a qubit loses energy at the interaction with the environment, and it can suffer spontaneous state transitions.

The decoherence is due to the phenomenon of coupling between two interacting systems, which initially were isolated.

Quantum error correction [40] [24] has the purpose to keep the coherence of the quantum state when the communication is perturbed by noises (physical interactions between quantum systems and the environment) which cannot be avoided.

The action of an error over a piece of information encoded in qubits means in fact an evolution of a qubit to another quantum state. This evolution is described with the help of a unitary operator.

The errors [69] which can appear at a qubit are:

- **bit-flip error**. The unitary operator describing the bit-flip error is:

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

The action of the operator X over a qubit has the effect of shifting its state:

$$X(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

- **phase-flip error**. The unitary operator describing this error is:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The action of the operator Z over a qubit determines a phase-flip:

$$Z(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle$$

- **bit-flip and phase-flip errors**. The unitary operator of this transformation is:

$$Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = XZ$$

The action of the operator Y over a qubit has the effect of shifting both the state and the phase:

$$Y(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -\beta \\ \alpha \end{pmatrix} = -\beta|0\rangle + \alpha|1\rangle$$

In order to re-establish the quantum information which was communicated it is necessary to detect and to correct these three types of errors. Considering the classical case of the code repetition, quantum errors can be corrected on the same principle, taking however into account the fundamental limitations imposed by quantum physics:

- the non-cloning theorem, which is forbidding the exact copying of a qubit in an arbitrary state;

- the projective measurement of a qubit does not offer complete information about its state, and destroys the quantum information stored in it.

1.10.1 Quantum error correction

The general strategy used in quantum error correction [55] can be resumed in the following way:

1. State encoding of a qubit in a collective state of several qubits.

2. The realization of the multi-qubit measurements in the encoded "block", which emphasizes the difference between an uncorrupted state and other states, which appeared because of the errors. We will use syndrome pairs which identify the type and location of the errors.

3. Knowing the syndrome errors, they are corrected by applying the corresponding transformations.

The scheme of error correction is represented schematically as it follows:

Next we will present and explain the blocks forming the scheme (1.25).

1.10.2 The encoding block

As we previously mentioned, a secure communication requires the detection and the correction of errors appeared in the communication. If classical informatics offers the easy solution of the code repetition, quantum informatics offers the possibility of encoding states in a collective state. This type of encoding is used in the detection and correction schemes of the three types of errors presented above.

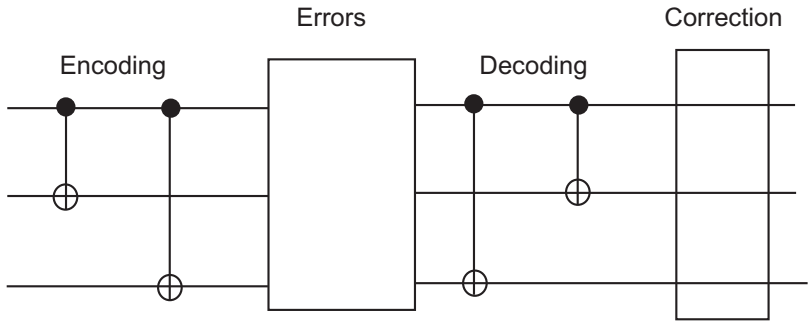


Figura 1.25: The generic scheme of error correction.

In order to encode the state

$$|\Psi_1\rangle = \alpha|0\rangle_1 + \beta|1\rangle_1 \tag{1.61}$$

in a collective state and to obtain the so-called repetitive code, we use two qubits with the initial quantum state $|0\rangle$. These two qubits are called *syndrome* and their values show which one of the qubits from the group was affected by the error. Due to the fact that the non-cloning theorem does not allow to copy the arbitrary states (1.61), in order to obtain redundant qubits (code repetition), we will use the $C-NOT$ quantum gates.

The encoding block is presented schematically in figure (1.25) where we notice that the $C-NOT$ gates are applied between the qubits $(1,2)$ and $(1,3)$.

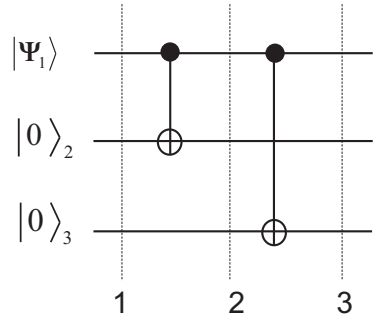


Figura 1.26: The scheme of the encoding block (3 qubits).

We can encode a single qubit with three qubits as it follows:

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle \tag{1.62}$$

The encoding of the qubit $|\Psi_1\rangle$ is obtained step by step:

Step 1:

$$(\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes |0\rangle_2 \otimes |0\rangle_3$$

Step 2:

$$(\alpha|00\rangle_{12} + \beta|11\rangle_{12}) \otimes |0\rangle_3$$

Step 3:

$$\alpha|000\rangle_{123} + \beta|111\rangle_{123}$$

1.10.3 The block of errors

The bit-flip error

As we previously mentioned, the bit-flip error has over a qubit the effect of shifting from a state to the other:

$$|0\rangle \to |1\rangle$$
$$|1\rangle \to |0\rangle$$
$$\alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle$$

We will study the bit-flip errors appeared at a qubit with the generic state $|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ encoded in the form (1.62).

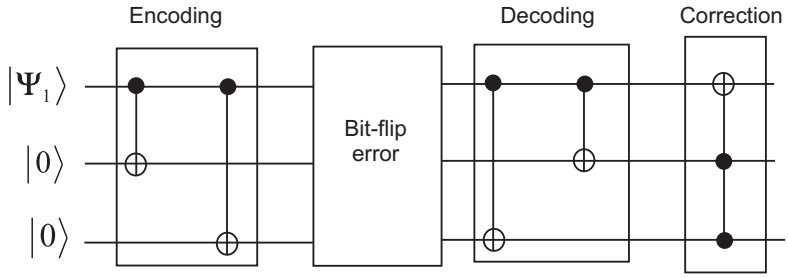


Figura 1.27: The scheme of a bit-flip error correction.

We assume that after the communication, the qubits suffered bit-flip errors.
There are four possibilities of error situations:

$\alpha|000\rangle + \beta|111\rangle$ - no error
$\alpha|100\rangle + \beta|011\rangle$ - error at qubit 1 !!!!
$\alpha|010\rangle + \beta|101\rangle$ - error at qubit 2
$\alpha|001\rangle + \beta|110\rangle$ - error at qubit 3

The most important case is when the error affects the qubit 1, qubit 2 and 3 having only a "supporting" role. This correction method will reconstitute the initial state of qubit 1.

Decoding

Based on the knowledge that the $C-NOT$ gates are reversible, the decoding will be realized using the $C-NOT$ gates applied in a reversed order.

The $C-NOT$ gate between (1,3) determines:

$$\alpha|000\rangle + \beta|111\rangle \longrightarrow \alpha|000\rangle + \beta|11\mathbf{0}\rangle$$
$$\alpha|100\rangle + \beta|011\rangle \longrightarrow \alpha|10\mathbf{1}\rangle + \beta|011\rangle$$
$$\alpha|010\rangle + \beta|101\rangle \longrightarrow \alpha|010\rangle + \beta|10\mathbf{0}\rangle$$
$$\alpha|001\rangle + \beta|110\rangle \longrightarrow \alpha|001\rangle + \beta|11\mathbf{1}\rangle$$

We notice a state shift of qubit 3.

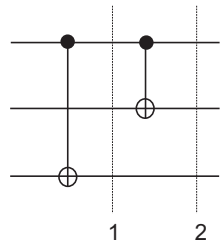


Figura 1.28: The decoding block (3 qubits).

The values of the syndrome pair	Error
00	no error
11	flip qubit 1 ⟵
10	flip qubit 2
01	flip qubit 3

Cuadro 1.2: Locating the error according to the value of the syndrome pair.

The second $C-NOT$ gate applied to qubits $(1,2)$ determines:

$$\begin{aligned}
\alpha|000\rangle+\beta|110\rangle &\longrightarrow \alpha|000\rangle+\beta|1\mathbf{0}0\rangle\\
\alpha|101\rangle+\beta|011\rangle &\longrightarrow \alpha|1\mathbf{1}1\rangle+\beta|011\rangle\\
\alpha|010\rangle+\beta|100\rangle &\longrightarrow \alpha|010\rangle+\beta|1\mathbf{1}0\rangle\\
\alpha|001\rangle+\beta|111\rangle &\longrightarrow \alpha|001\rangle+\beta|1\mathbf{0}1\rangle
\end{aligned}$$

We notice a state shift of qubit 2.

All the possible states obtained at the end of the decoding circuit can be written according to the syndrome pair as it follows:

$$\begin{aligned}
&\alpha|000\rangle+\beta|111\rangle=(\alpha|0\rangle+\beta|1\rangle)\otimes|00\rangle && \text{no errors}\\
&\alpha|100\rangle+\beta|011\rangle=(\alpha|1\rangle+\beta|0\rangle)\otimes|11\rangle && \text{error qubit 1 !!!!}\\
&\alpha|010\rangle+\beta|101\rangle=(\alpha|0\rangle+\beta|1\rangle)\otimes|10\rangle && \text{error qubit 2}\\
&\alpha|001\rangle+\beta|110\rangle=(\alpha|0\rangle+\beta|1\rangle)\otimes|01\rangle && \text{error qubit 3}
\end{aligned}$$

We notice that in the case when the syndrome pair has the state $|1\rangle$ the qubit 1 is affected by a bit-flip, and in the rest of the situations the qubit 1 keeps its state unchanged.

We can conclude that the value of the syndrome pair offers clues regarding the qubit affected by the bit-flip error. As we are interested only in the state of qubit 1 examined in the experiment, we will correct the error affecting it.

Error correction

For the correction of the bit-flip error appeared at the qubit 1, the $CC-NOT$ gate applies using the syndrome pair as control qubits.

The $CC-NOT$ gate acts over the target qubit (the qubit 1) shifting only its state if the control qubits are simultaneously in the state $|1\rangle$.

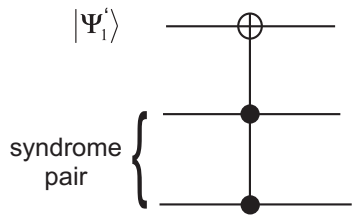


Figura 1.29: The correction circuit of a bit-flip error.

The action of this gate is the following:

$$\begin{aligned}
(\alpha|0\rangle+\beta|1\rangle)\otimes|00\rangle &\longrightarrow (\alpha|0\rangle+\beta|1\rangle)\otimes|00\rangle\\
(\alpha|1\rangle+\beta|0\rangle)\otimes|11\rangle &\longrightarrow (\alpha|0\rangle+\beta|1\rangle)\otimes|11\rangle\\
(\alpha|0\rangle+\beta|1\rangle)\otimes|10\rangle &\longrightarrow (\alpha|0\rangle+\beta|1\rangle)\otimes|10\rangle\\
(\alpha|0\rangle+\beta|1\rangle)\otimes|01\rangle &\longrightarrow (\alpha|0\rangle+\beta|1\rangle)\otimes|01\rangle
\end{aligned}$$

We notice that the state of the qubit 1 went back to the initial one (1.61).

The phase-flip error

The phase-flip error consists of a phase-flip by 180^o of the state $|1\rangle$, as in the following example:

$$\begin{aligned}
&|0\rangle \rightarrow |0\rangle\\
&|1\rangle \rightarrow -|1\rangle\\
&\alpha|0\rangle+\beta|1\rangle \rightarrow \alpha|0\rangle-\beta|1\rangle
\end{aligned}$$

Next we will present the influence of the phase-flip error over a qubit encoded in the form (1.62), as well as the correction of this type of error.

Figure 1.30 presents the correction scheme of a phase-flip error.

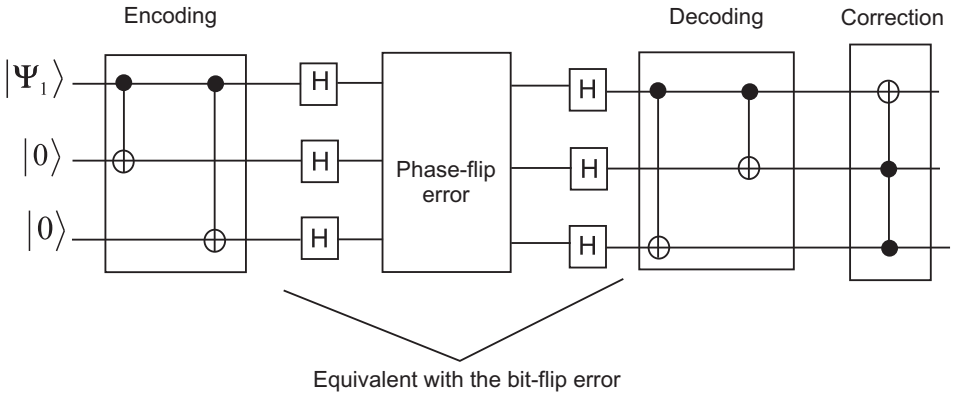


Figura 1.30: The correction scheme of phase-flip error.

In order to detect the phase-flip error, the *Hadamard* gates are added at the end of the encoding and at the beginning of the decoding.

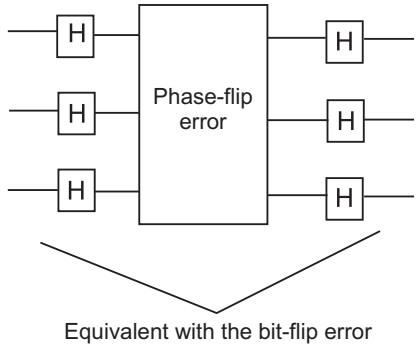


Figura 1.31: The detection scheme of the phase-flip error.

If after the communication through the network no qubit is affected by the phase-flip error, then the action of the two *Hadamard* gates is canceling one another.

For the demonstration, we assume that the group of qubits was not affected by any error, and the initial state (transmitted) is the same with the final one (received):

$$\alpha|000\rangle+\beta|111\rangle \quad \longrightarrow \quad \alpha|000\rangle+\beta|111\rangle$$

We prove that in these conditions, the action of the two *Hadamard* gates disposed at the end of the encoding, and at the beginning of the decoding, are canceling one another.

The action of the *Hadamard* gates at the end of the encoding block is the following:

$$H(\alpha|000\rangle+\beta|111\rangle)=\alpha H|000\rangle+\beta H|111\rangle=\alpha(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})+$$

$$+\beta(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$$

The application of the *Hadamard* gates at the beginning of the decoding block has the outcome:

$$H[\alpha(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})+\beta(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})]=$$

$$=\alpha[H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})]+\beta[H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})] \tag{1.63}$$

The *Hadamard* gate applied on the states $|0\rangle$ and $|1\rangle$ has the following effect:

$$H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}} \tag{1.64}$$

$$H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{1.65}$$

and:

$$H(|0\rangle+|1\rangle)=H|0\rangle+H|1\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\frac{|0\rangle-|1\rangle}{\sqrt{2}}=\sqrt{2}|0\rangle \tag{1.66}$$

$$H(|0\rangle-|1\rangle)=H|0\rangle-H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}-\frac{|0\rangle-|1\rangle}{\sqrt{2}}=\sqrt{2}|1\rangle \tag{1.67}$$

Replacing the equations (1.66) and (1.67), respectively in the relation (1.63), we obtain:

$$\alpha|000\rangle+\beta|111\rangle$$

which is the initial state of the qubit.

Thus, we demonstrated that as long as the qubits are not affected by the error, the *Hadamard* gates placed at the end of the encoding, and at the beginning of the decoding are canceling one another.

Next we will analyze the case when a qubit is affected by a phase-flip error, where the presence of the two *Hadamard* gates transforms this type of error in a bit-flip error.

The action of the *Hadamard* gate from the end of the encoding block has the following effect:

$$H(\alpha|000\rangle+\beta|111\rangle)=\alpha H|000\rangle+\beta H|111\rangle=\alpha(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})+$$

$$+\beta(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) \tag{1.68}$$

We assume that the qubit 1 is affected by a phase-flip error, which is:

$$|1\rangle\rightarrow-|1\rangle$$

The equation (1.68) becomes:

$$\alpha(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})+\beta(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$$

Applying the *Hadamard* gate at the entry of the decoding block, we obtain:

$$H[\alpha(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}})+\beta(\frac{|0\rangle+|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})(\frac{|0\rangle-|1\rangle}{\sqrt{2}})]=$$

$$=\alpha[H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})]+\beta[H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})] \tag{1.69}$$

Using the equations (1.66) and (1.67) respectively, the equation (1.69) is written:

$$\alpha|100\rangle+\beta|011\rangle$$

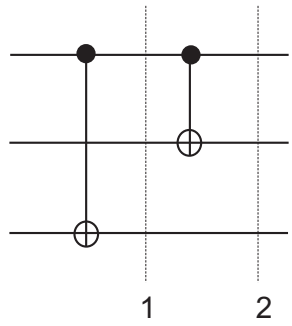


Figura 1.32: The decoding block (3 qubits).

Decoding and error correction

Based on the knowledge that the $C-NOT$ gates are reversible, decoding will be realised using the $C-NOT$ gates applied in reversed order.

The $C-NOT$ gate between the qubits (1,3) determines:

$$\alpha|100\rangle+\beta|011\rangle \longrightarrow \alpha|101\rangle+\beta|011\rangle$$

The $C-NOT$ gate between the qubits $(1,2)$ determines:

$$\alpha|101\rangle+\beta|011\rangle \longrightarrow \alpha|111\rangle+\beta|011\rangle \tag{1.70}$$

At the end of the decoding circuit, the state (1.70) can be expressed function of the syndrome pair:

$$\alpha|111\rangle+\beta|011\rangle=(\alpha|1\rangle+\beta|0\rangle)\otimes|1\rangle\otimes|1\rangle$$

We notice that the presence of *Hadamard* gates at the end of the encoding, and at the beginning of the decoding transforms the phase-flip error in a bit-flip error, and for the correction of these errors, the $CC-NOT$ gates will be used as shown previously.

1.10.4 Shor's error correction scheme (9,1)

Shor realized a scheme [89] on 9 qubits (figure 1.33) for the correction of the bit-flip and phase-flip errors which can affect a qubit simultaneously.

Encoding

Shor's encoding scheme combines the encoding blocks used in the detection and correction schemes of phase-flip, and bit-flip errors respectively.

Next we will analyze the step by step action of each block over the qubit $|\Psi_1\rangle$.

THE PHASE-FLIP BLOCK

In the phase-flip encoding block takes place the qubit "multiplication" using the syndrome pair.

Step 1 - the action of the $C-NOT$ gates over the qubits (1,2) and (1,3) :

$$\alpha|0_1 0_2 0_3\rangle+\beta|1_1 1_2 1_3\rangle$$

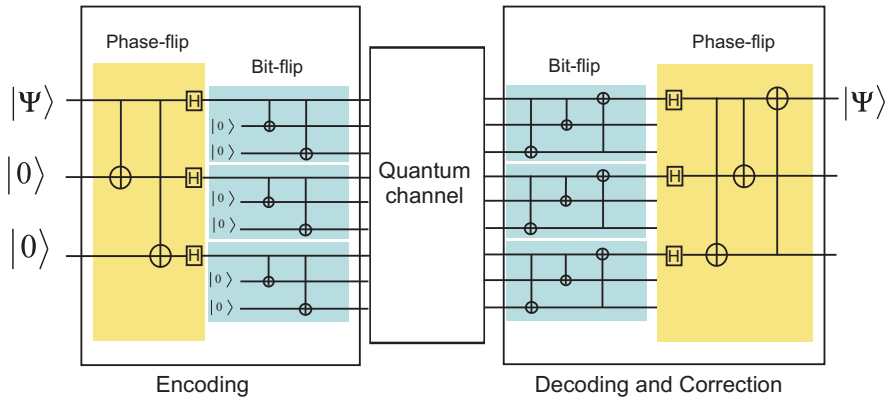


Figura 1.33: Shor scheme (9 qubits) of error correction.

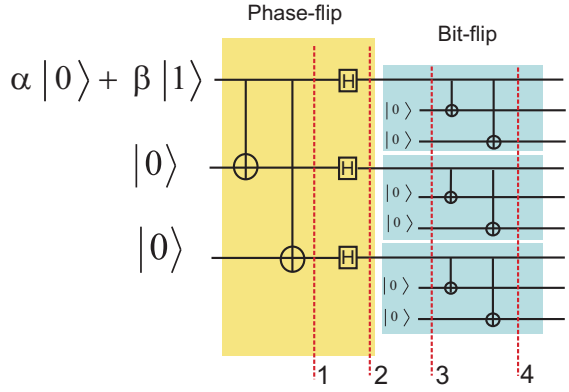


Figura 1.34: Shor's encoding scheme.

Step 2 - the action of the *Hadamard* gates:

$$\alpha[(\frac{|0_1\rangle+|1_1\rangle}{\sqrt{2}})(\frac{|0_2\rangle+|1_2\rangle}{\sqrt{2}})(\frac{|0_3\rangle+|1_3\rangle}{\sqrt{2}})]+\beta[(\frac{|0_1\rangle-|1_1\rangle}{\sqrt{2}})(\frac{|0_2\rangle-|1_2\rangle}{\sqrt{2}})(\frac{|0_3\rangle-|1_3\rangle}{\sqrt{2}})]$$

THE BIT-FLIP ENCODING BLOCK

Step 3 - in the bit-flip encoding block we continue the "multiplication" by adding a syndrome pair to each qubit obtained after the encoding from the previous block:

$$\alpha\frac{1}{\sqrt{2}}(|0_1 0_2 0_3\rangle+|1_1 0_2 0_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle+|1_4 0_5 0_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle+|1_7 0_8 0_9\rangle)+$$

$$+\beta\frac{1}{\sqrt{2}}(|0_1 0_2 0_3\rangle-|1_1 0_2 0_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle-|1_4 0_5 0_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle-|1_7 0_8 0_9\rangle)$$

Step 4 - the action of the $C-NOT$ gates have the result:

$$\alpha\frac{1}{\sqrt{2}}(|0_1 0_2 0_3\rangle+|1_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle+|1_4 1_5 1_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle+|1_7 1_8 1_9\rangle)+$$

$$+\beta\frac{1}{\sqrt{2}}(|0_1 0_2 0_3\rangle-|1_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle-|1_4 1_5 1_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle-|1_7 1_8 1_9\rangle) \tag{1.71}$$

After going through the two blocks, we notice that the qubit $|\Psi_1\rangle=\alpha|0_1\rangle+\beta|1_1\rangle$ was encoded by a group of 9 qubits. The transmission of this group through a communication channel with imperfections determines the appearance of bit-flip and phase-flip errors. Next we will present the method of error decoding and correction, for the situation when they affect the qubit simultaneously.

Error decoding and correction

We assume that the first qubit is affected by the two types of errors: phase-flip and bit-flip, and the qubit state suffers the following transformations: $|1_1\rangle\rightarrow-|1_1\rangle$ (phase-flip error), $|0_1\rangle\rightarrow|1_1\rangle$ şi $|1_1\rangle\rightarrow|0_1\rangle$ (bit-flip error).

The equation (1.71) becomes:

$$\alpha\frac{1}{\sqrt{2}}(|1_1 0_2 0_3\rangle-|0_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle+|1_4 1_5 1_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle+|1_7 1_8 1_9\rangle)+$$

$$+\beta\frac{1}{\sqrt{2}}(|1_1 0_2 0_3\rangle+|0_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle-|1_4 1_5 1_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle-|1_7 1_8 1_9\rangle) \tag{1.72}$$

The equation (1.72) represents the state of the group before entering the bit-flip and phase-flip blocks of error decoding and correction - ***step 1***.

The error decoding and correction are realized by applying these blocks in the reversed order of encoding, i.e. bit-flip error decoding and correction, followed by the phase-flip error decoding and correction.

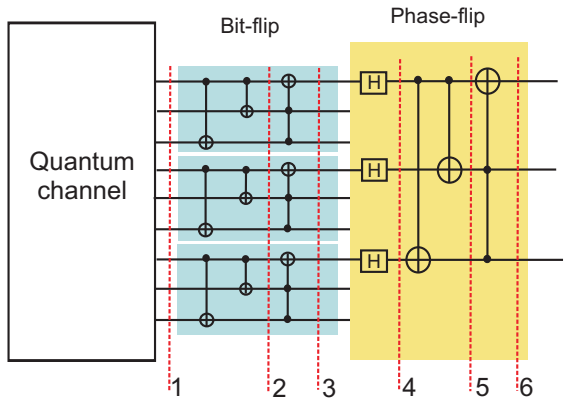


Figura 1.35: Shor's scheme - error decoding and correction.

THE BIT-FLIP BLOCK

Step 2 - decoding requires applying the $C-NOT$ gates in reversed order, hence the equation (1.72) becomes:

$$\alpha\frac{1}{\sqrt{2}}(|1_1 1_2 1_3\rangle - |0_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle + |1_4 0_5 0_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle + |1_7 0_8 0_9\rangle)+$$

$$+\beta\frac{1}{\sqrt{2}}(|1_1 1_2 1_3\rangle + |0_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle - |1_4 0_5 0_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle - |1_7 0_8 0_9\rangle) \tag{1.73}$$

Step 3 - the error correction is realized by using the $CC-NOT$ gate, hence the equation (1.73), becomes:

$$\alpha\frac{1}{\sqrt{2}}(|0_1 1_2 1_3\rangle - |1_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle + |1_4 0_5 0_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle + |1_7 0_8 0_9\rangle)+$$

$$+\beta\frac{1}{\sqrt{2}}(|0_1 1_2 1_3\rangle + |1_1 1_2 1_3\rangle)\frac{1}{\sqrt{2}}(|0_4 0_5 0_6\rangle - |1_4 0_5 0_6\rangle)\frac{1}{\sqrt{2}}(|0_7 0_8 0_9\rangle - |1_7 0_8 0_9\rangle) =$$

$$= \alpha[\frac{(|0_1\rangle - |1_1\rangle)}{\sqrt{2}}|1_2 1_3\rangle][\frac{(|0_4\rangle + |1_4\rangle)}{\sqrt{2}}|0_5 0_6\rangle][\frac{(|0_7\rangle + |1_7\rangle)}{\sqrt{2}}|0_8 0_9\rangle]+$$

$$+\beta[\frac{(|0_1\rangle + |1_1\rangle)}{\sqrt{2}}|1_2 1_3\rangle][\frac{(|0_4\rangle - |1_4\rangle)}{\sqrt{2}}|0_5 0_6\rangle][\frac{(|0_7\rangle - |1_7\rangle)}{\sqrt{2}}|0_8 0_9\rangle] \tag{1.74}$$

THE PHASE-FLIP BLOCK

At the entry of the phase-flip block, the state of the group of qubits is described by the equation (1.74).

Step 4 - applying $Hadamard$ gates leads to:

$$\alpha|1_1\rangle|0_4\rangle|0_7\rangle + \beta|0_1\rangle|1_4\rangle|1_7\rangle \tag{1.75}$$

Step 5 - decoding. After applying the $C-NOT$ gates, the equation (1.75) becomes:

$$\alpha|1_1\rangle|1_4\rangle|1_7\rangle + \beta|0_1\rangle|1_4\rangle|1_7\rangle = (\alpha|1_1\rangle + \beta|0_1\rangle)|1_4\rangle|1_7\rangle \tag{1.76}$$

Step 6 - error correction. The $CC-NOT$ gate is applied for correction of the phase-flip error which affected the qubit 1, hence the equation (1.76) becomes:

$$\alpha|0_1\rangle|1_4\rangle|1_7\rangle + \beta|1_1\rangle|1_4\rangle|1_7\rangle = (\alpha|0_1\rangle + \beta|1_1\rangle) \otimes |1_4\rangle|1_7\rangle \tag{1.77}$$

We notice in the equation (1.77) that the state of qubit 1 is identical with the initial one, even if at its passing through a communication channel was affected by a phase-flip error and a bit-flip error.

2. Quantum Cryptography

2.1 Introduction to cryptography

Cryptography provides a set of standards and protocols for the encryption of data and messages so that these are more securely stored and sent. Cryptography is the basis for many security services and mechanisms from the Internet. It uses mathematical methods to transform data, in order to prevent them to be seen or to get their content altered. Cryptography can be used in order to assure the data integrity and secrecy, and to verify the source of data or messages by the use of digital signatures and certificates.

The explicit purpose of cryptography is to make it difficult or impossible for a third party to access the protected information. Cryptography helps in getting a more secure communication, even when the transmission environment is not to be trusted.

The fundamental purpose of cryptography is:

Confidentiality - assurance that nobody can read the message except the sender and the designated receiver;

Data integrity - protection of data against alteration or manipulation (insertions, delays etc.) by unauthorized persons;

Authentication - possibility to identify the source of the information and of the entity (person, computer terminal);

Non-repudiation - prevents the refusal to admit previous declarations or actions.

There are two types of cryptosystems:

- *symmetric* (secret key) - the decryption rule can be determined based on the knowledge of the encryption rule, and the other way around;

- *asymmetric* (public key) - the key is divided in two sub-keys: a private (secret) one, and a public one. The public sub-key can be used by anyone who wants to send an encrypted message to the key owner. The private (secret) sub-key is known only by the key owner, and it is used at the decryption of the message received.

2.2 Quantum cryptography

Quantum cryptography is a combination between quantum physics and the art of encoding. For the first time, the idea of quantum cryptography was introduced in an unpublished manuscript by Stephen Wiesner in 1970 [102] and was presented by Bennett and Brassard in 1984 [8], becoming thus a subject of interest. The purpose of quantum cryptography is to solve problems that are impossible or hard to solve by classical cryptography. Quantum cryptography uses quantum physics properties like: the no-cloning theorem, the Heisenberg uncertainty principle, and irreversibility of quantum measurements. As compared to the classical cryptography, whose security is most often based on undemonstrated assumptions, quantum cryptography has the great advantage of its security, which is based on physical laws. In a bigger context, quantum cryptography is a field of quantum information processing, including quantum computation, quantum measurements, and quantum teleportation. Of all these, quantum cryptography is the closest field to realistic applications. At a fundamental level, quantum cryptography is deeply related to the laws of quantum physics, and at a technological level, it uses technologies like single photon measurement, and detection of single-photon sources.

2.3 Quantum key distribution

The most common application of quantum cryptography is the quantum key distribution (Q.K.D.). Quantum key distribution is a protocol which is provably secure, by which private key bits can be created between two parties over a public channel.

The purpose of quantum key distribution is that two participants situated far away from each other, traditionally called Alice and Bob, could share a secret in the presence of an intruder, generally called Eve. The key can be used either for a perfect secure communication, or for a perfect secure authentication.

Quantum physics can foresee a solutionconcerning the problem of key distribution. In quantum key distribution, the encryption key is randomly generated between Alice and Bob using quantum states. As compared to classical physics, in quantum physics there is the no-cloning theorem, which makes it impossible for anyone, including an intruder, to copy an unknown quantum state. The great advantage of quantum cryptography is the so-called "forward security". If in classical cryptography an intruder can transcribe all the communications and then wait for years to decrypt them when new algorithms or hardware devices are discovered, due to the no-cloning theorem, an intruder cannot transcribe (save) all the quantum signals sent between Alice and Bob. Up to the present time, the schemes of quantum keys distribution are based on two important properties of quantum physics: the uncertainty principle (Heisenberg's principle), and the quantum link principle (the paradox Einstein-Podosky-Rosen). Using two communication channels, a classical one and a quantum one, all the schemes of quantum key distribution go through the following steps:

1. **Preparation of the states and their transmission.** Alice and Bob are preparing separately a number of quantum and classical states. They can keep a part of them, sending the rest to the other party using secure classical channels, and insecure quantum ones. They will repeat this thing several times (the preparation and sending processes).

2. **Verifying the quality of the states.** Alice and Bob will test the fidelity of the exchange of quantum states, taking into account the fact that they use an insecure quantum channel, also full of noises. Considering the fact that the process of quantum

measurement is irreversible, some quantum states will consume during the checking process. The purpose of this test is to estimate the noise on the channel, but also to determine the maximum level from which the existence of an intruder is suspected. Alice and Bob will start the process again if they consider that the result of the fidelity test is incorrect.

3. **Error correction and Privacy Amplification.** Alice and Bob must correct the errors from the rest of the rows of bits. Furthermore, they will want to remove any residual information which an intruder (Eve) could introduce. In other words, Alice and Bob will select from the untested quantum states a set of states almost perfectly unaltered by any intruder or noises. This process is called privacy amplification. At the end, Alice and Bob will realize the secret key from the states obtained.

The preparation of the states and their sending as a first step within the scheme of quantum key distribution is realized using a series of protocols. Next we will present the most important ones.

2.3.1 The Ekert protocol

Ekert proposed [36] a key distribution protocol based on the principle of quantum link, and using pairs of EPR photons. At the realization of the experiment, Ekert used a

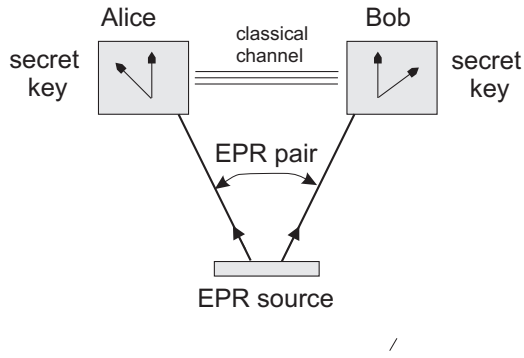


Figura 2.1: The Ekert protocol

source of EPR photons, the two photons emitted being always in opposite polarization states.

The Ekert protocol is the following:

The pair of EPR photons is distributed as follows: a photon to Alice, and the other to Bob, each measuring them using randomly one of the two bases. In the absence of the noise or of an intruder, Alice and Bob will obtain the same measurement result if they choose the same basis. Using a public channel, Alice and Bob will communicate to each other the measurement basis used, without revealing the result obtained. For the cases when the measurement bases are not well chosen, the results will be erased. Hence, the *raw key* is obtained.

2.3.2 The Bennett-Brassard BB84 protocol

Charles Bennett from IBM together with Gilles Brassard from the University of Montreal (1984, 1985) [8] [9], starting from Stephen Wiesner's study "Conjugate Coding"

[102], developed a key distribution protocol using polarized photons.

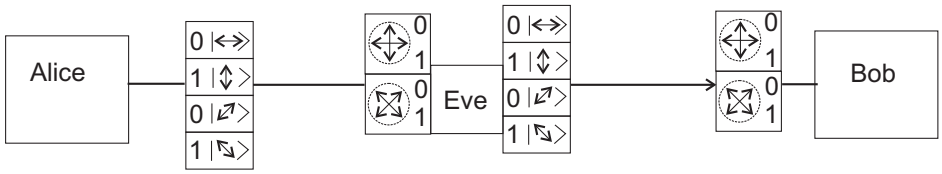


Figura 2.2: The Bennett-Brassard protocol

The polarization states form two orthonormal bases as follows:
- a rectilinear (linear) basis $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ - linear polarization;
- a diagonal basis $\{|\nearrow\rangle, |\nwarrow\rangle\}$ - circular polarization.

The states of the diagonal basis are polarization states at $\pm 45^{\circ}$ of the states of the rectilinear basis.

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle)$$
$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle)$$

Conventionally, we assume that the photon polarization states have the following binary values:

	State	Binary value
linear basis	$\|\updownarrow\rangle$	0
	$\|\leftrightarrow\rangle$	1
diagonal basis	$\|\nearrow\rangle$	0
	$\|\nwarrow\rangle$	1

The Bennett-Brassard protocol is as follows:

Alice sends to Bob a row of polarized photons. Bob, using randomly one of the two bases, will measure each photon. In the absence of the noise, or of an intruder, Alice and Bob will obtain the same measurement result if they choose the same basis. Using a public channel, Bob communicates to Alice the measurement basis he has used, without revealing the result obtained. When the measurement bases are not well chosen, the results will be erased. The sequence of bits thus obtained is called *raw key*.

The encryption key obtained with the help of Bennett-Brassard protocol is the ”one time pad” type, and cannot assure a "perfect security”, because there are situations of "denial.ºf the message ownership (the sender encrypts the message with the key obtained, and after sending it, he pretends that the message was encrypted with another key).

2.3.3 The Bennett B92 protocol

In 1992, Charles Bennett proposed a simplified alternative of Bennett-Brassard protocol [10]. The difference consists in the use of a single measurement basis, as compared to Bennett-Brassard protocol. These bases encode 0 with $|\rightarrow\rangle$ and 1 with $|\nearrow\rangle$. The same as Bennett-Brassard protocol, Alice sends to Bob a sequence of photons, using a quantum communication channel. Bob decides randomly and independently from Alice how to measure each photon, and he will register every measurement result with ”YES” or ”NO”. The result ”YES” will be when Bob chooses the measurement

basis correctly, and "NO" in the opposite case. As a result of the protocol, the two will be in the possession of a sequence of bits called *raw key*.

2.3.4 The Bechmann-Pasquinucci and Peres protocol for qutrits

The protocol known as Bennett-Brassard uses two bases, each with two orthogonal states (qubits). Helle Bechmann-Pasquinucci and Asher Peres [13] extended the protocol of quantum key distribution for the three-state systems, the so-called qutrits.

If in the case of the qubits Alice chooses in which of the two bases she will prepare the state, in the case of the qutrits she will use some bases called mutually unbiased bases [51] [103]. Suppose the first basis randomly chosen is: $\{|\alpha\rangle, |\beta\rangle, |\gamma\rangle\}$. The other bases are obtained by the application of discrete Fourier transforms. The first basis is $\{|\alpha^{'}\rangle, |\beta^{'}\rangle, |\gamma^{'}\rangle\}$:

$$\begin{cases} |\alpha^{'}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + |\gamma\rangle) \\ |\beta^{'}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + e^{2\pi i/3}|\beta\rangle + e^{4\pi i/3}|\gamma\rangle) \\ |\gamma^{'}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + e^{4\pi i/3}|\beta\rangle + e^{2\pi i/3}|\gamma\rangle) \end{cases} \tag{2.1}$$

The second $\{|\alpha^{"}\rangle, |\beta^{"}\rangle, |\gamma^{"}\rangle\}$ and third basis $\{|\alpha^{"'}\rangle, |\beta^{"'}\rangle, |\gamma^{"'}\rangle\}$ are obtained by cyclic permutations:

$$\begin{cases} |\alpha^{"}\rangle = \frac{1}{\sqrt{3}}(e^{2\pi i/3}|\alpha\rangle + |\beta\rangle + |\gamma\rangle) \\ |\beta^{"}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + e^{2\pi i/3}|\beta\rangle + |\gamma\rangle) \\ |\gamma^{"}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + e^{2\pi i/3}|\gamma\rangle) \end{cases} \tag{2.2}$$

$$\begin{cases} |\alpha^{"'}\rangle = \frac{1}{\sqrt{3}}(e^{4\pi i/3}|\alpha\rangle + |\beta\rangle + |\gamma\rangle) \\ |\beta^{"'}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + e^{4\pi i/3}|\beta\rangle + |\gamma\rangle) \\ |\gamma^{"'}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + e^{4\pi i/3}|\gamma\rangle) \end{cases} \tag{2.3}$$

Alice chooses randomly one of the 12 (4 basis x 3 states on each) states and sends it to Bob. Bob chooses randomly one of the four bases and measures the state, then announces publicly which basis he used, without revealing the result obtained. Alice verifies if the choice is correct. If it was, the two of them are in the possession of the same qutrit; if not, they give it up. The procedure is repeated until Alice and Bob obtain a sufficiently big key. Then they will sacrifice some of them for errors correction and privacy amplification [9].

In order to obtain the final encryption key which will be used in any encryption method, there are four more steps, as follows:

2.3.5 Raw Key Extraction

This step has the purpose to eliminate the erroneous transmissions. This application is different from one protocol to the other.

For the **Ekert**, protocol, at this step Alice and Bob compare the bases used in the process of measurement of EPR photons. If they use different bases, they will eliminate the bit whose value corresponds to that of the photon. For the Ekert protocol, the

announcement of the basis used is realized through a public channel. The sequence of binary values obtained by Bob at the end of the transmission will be called *raw key*.

For **Bennett-Brassard** and **Bechmann-Pasquinucci and Peres**, at this step Alice and Bob compare the bases used in the process of measurement of polarized photons. The correct choice of the basis determines the maintenance of the value, and in the opposite case they will eliminate the bit whose value corresponds to that of the photon. As in Ekert protocol, in BB84 protocol the announcement of the basis used is realized through a public channel. The sequence of binary values obtained by Bob at the end of the transmission will be called *raw key*.

For the **Bennett**, protocol, Bob will not reveal his measurement basis, because he used photons in two polarization states. Consequently, Bob will label the measurement results with ”yes” for the case of the correct choice of the basis, and ”no” for the opposite situation. He will then send these ”notes” to Alice through a public channel, and she will erase from her sequence of bits the ones that had a negative response. At the end of this step, both will be in the possession of a row of bits called *raw key*.

2.3.6 Error Estimation

If the parties use in the process of quantum keys distribution a channel with noises, it would be extremely advantageous for an intruder. If Alice and Bob use the same basis in the process of sending / measurement, and they do not have the same values, this is the proof of an intruder's existence, and of a transmission environment full of noises. The existence of a channel full of noises is a favorable environment for an intruder to produce attacks over the key distribution protocol. In order to avoid such attacks, both parties determine an error threshold R_{max} determined when they are certain that there is no intruder in the transmission environment. Then, after each sequence of the key distribution session, they compare and sacrifice some bits from the *raw key* with the purpose to compute the error percentage R at the transmission. They are certain of the presence of an intruder when $R > R_{max}$, which determines them to restart the protocol.

2.3.7 Key Reconciliation

When $R < R_{max}$ it means that there are some errors in the not compared parts of the key. In this case, the step of errors minimization is applied, called Key Reconciliation. This step includes the sub-steps:

1. Alice and Bob rearrange their sequence of bits using permutation functions, and they agree over every permutation, communicating through a public channel. After that, they will obtain a uniform error distribution.

2. The bit sequences are divided in blocks of k bits. In order to reduce the existence of more than an error in each block, an ideal k is chosen.

3. For each block, Alice and Bob will compute the parity value, and they will make it public. The last bit of every block whose parity value is announced will be erased.

4. Parties divide each block in sub-blocks by different parity values, and compare the parity values of these sub-blocks in order to find the error [70]. This method is similar to the ”binary search”. The last bit of every sub-block whose parity value is announced will be erased.

5. If there is more than an error in a block, the operation is repeated from step 4.

6. In order to determine the errors remained, Alice and Bob compute the parity value for half of their sequence of bits, and announce the result publicly. If these values are

still different, they will apply the ”binary search” method.

2.3.8 Privacy Amplification

At this point, Alice and Bob have two identical rows which are not completely individual. The intruder (Eve) can possess some parts of information obtained during the process of transmission/reception. Though this strategy can produce errors in Bob's row if Eve uses only a low number of bits, the errors will get lost among those produced by the detector, or due to other physical problems. During the reconciliation, Eve will not obtain any information from the last bit of every parity test that will be erased. However, some pieces of the information possessed can be converted in information concerning the parity bits. Therefore, if she knows the value of the bit x from the row y, and Alice and Bob will show the parity of y and will give up x, Eve will be able to find out the parity of the bits remained in the row y. We say that Eve knows the parity bit of a row if she knows the parity of a subset of that row, and if Eve knows at most k physical bits from the key, then she will know at most k parity bits from the key after reconciliation.

Starting from the error ratio R, Alice and Bob can foresee the maximal number of bits k that can be intercepted by Eve. Assuming s is a security parameter, Alice and Bob can choose at random $n-k-s$ subsets of their key, where n is the number of bits of the key. The parities of these subsets become the secret final key - shifted key.

2.3.9 Other schemes of quantum key distribution

After the publication of the schemes Bennett-Brassard 84, Bennett 92 and Ekert, more schemes of quantum key distribution were proposed. The first variations were the schemes using Einstein-Podolsky-Rosen pairs [38], two non-orthogonal states instead of four states [10], and the schemes using the phase modulation instead of the polarization [10] [37] [4]. Towsend et al [98] discussed about the practical implementation of quantum cryptography on a network communication with several users. It was proposed a method for the network quantum cryptography based on quantum memories [15]. Using the idea of the scheme Bennett-Brassard from 1984 the most efficient schemes for quantum cryptography were introduced: H.K.Lo and H.F.Chau [60] and A.Ardehali, H.F.Chau and H,-K.Lo [1]. A series of experimental machines were realized for the implementation of quantum key distribution, of which we mention: the first prototype, built in Geneva, following the original protocol [9] and using four different polarization states to transport the information through an optical cable of 1 km [65]; a prototype realized by British Telecom in partnership with Defence Research Agency, using the phase modulation, having the length of the optical fibre of 10 km [96] [97]; an experiment using EPR pairs was implemented for communication over several km through the optical fibre [76].

2.3.10 The degree of security

The security control of the protocol of quantum key distribution against an attack was a very difficult problem. This issue has been of interest for more than 10 years, and the security of the protocol was eventually established. Mayers [62], by his approach of the direct security of the protocol Bennett-Brassard $BB'84$; Lo and Chau [61] using Bennett's idea of the state entanglement distillation; DiVincenzo, Smolin and Wootters [12] and Deutsch et al [34] using the quantum privacy amplification, have solved the security problem of the protocol of quantum key distribution using the state entanglement.

Two of these approaches were unified by Shor and Preskill' works [91] and developed a simple method of checking the security of the protocol Bennett-Brassard BB84 using the idea of state entanglement distillation.

Quantum key distribution, though it cannot prevent the existence of intruders, is, however, able to detect them. The appearance of a high ratio of abnormality leads to the conclusion of the existence of an intruder, and has the effect of interrupting the transmission. If the error ratio is sufficiently low, the two parties will exclude the existence of an intruder.

The demonstration of the security is very important, because it assures the basis security protocol of quantum key distribution, it assures a formula for the key generation ratio using the protocol Q.K.D. and can assure the construction of a classical post-processing protocol (for the error correction and private amplification) necessary to generate the final key. Without the demonstration of the security, a system Q.K.D. is incomplete, because we cannot be certain of the way in which a secure secret key is generated, and how secure the final key is.

An intruder can use different strategies to break through in the communication process:

i). *Interception and re-sending*.

The intruder will try to intercept a photon, to measure it, and then to send a forged copy back to Bob. He will encounter the problems of a forger: he will not know the basis in which to measure the photon. There are times when the attack irremediably perturbs the photon state, or, at best, a photon with an identical state is sent, and can be detected by the existence of an error of delay in the information transfer from Alice to Bob. However, in reality the intruder can use a special equipment to introduce further errors due to the quantum channel used, to the noise detector, etc., which contribute to the raise of the error ratio;

ii). *Translucent attack.*

Eve can use a probe to interact with the photons sent by Alice, and she measures the state of this probe;

iii). *Collective attack.*

Eve is blocking all the photons exchanged by Alice and Bob. The presence of an intruder is easy to notice, due to the high value of the error (Quantum Bit Error Rate), which is much higher than $50\,\%$, determining the interruption and the restart of the protocol.

iv). *Attack over the protocol Bechmann-Pasquinucci and Peres.*

Assuming the existence of an intruder, Eve, who intercepts the qutrits, measures them, and sends back to Bob the determined state. In $3/4$ of the cases, she will use a wrong basis, so she will not be able to obtain the desired information, and in the same time she will produce a maximal distortion of the transmission, with an error ratio at reception of $2/3$. Consequently, using this method of quantum key distribution, any intruder from the communication channel will be able to obtain a very small fraction of the sent information, determining in exchange the serious deterioration of the transmission.

2.4 Entangled Quantum States

As we presented in the first part of this book, any quantum state which cannot be written as a product or as product entanglement is called "entangled". In practice it is

very difficult to determine if an unknown state can be written like that or not.

A mathematical description of the "entanglement" was offered by Werner in 1984 [101], extending the principle of inseparability: *If two systems interacted in the past, it is possible to find the whole system in a state which could not be written as an entanglement of state product*. This principle leads to a general definition of the entangled states.

Defintion 2.4.1 *A state ρ is entangled or inseparable if and only if it cannot be written as a convex combination of state product:*

$$\rho^{AB} \neq \sum_i p_i \rho_i^A \otimes \rho_i^B$$

with $\sum_i p_i = 1$.

On the contrary, the bi-partite states that allow the factorization in the terms of a combination of state product are *separable*. The easiest example of the state separability is: $\rho = \rho^A \otimes \rho^B$.

2.4.1 Bi-partite systems

Defintion 2.4.2 *Two quantum systems labeled A and B are in a quantum correlation - entangled - if the compound state ρ^{AB} cannot be factorized as a sum of the state product:*

$$\rho^{AB} \neq \sum_i p_i \rho_i^A \otimes \rho_i^B$$

with $\sum_i p_i = 1$.

The compound state $|\Psi\rangle^{AB}$ is entangled if and only if it cannot be factorized in two separate states $|\Psi\rangle^A$ and $|\Phi\rangle^B$ respectively:

$$|\Psi\rangle^{AB} \neq |\psi\rangle^A \otimes |\phi\rangle^B$$

All the states $|\Psi\rangle^{AB}$ of the compound systems form a set $\mathscr{S}$. Generally, these states are entangled, and very rarely are separable.

Defintion 2.4.3 *We say that two systems A and B are maximally entangled when their compound state $|\Psi\rangle$ can be written using Schmidt's decomposition, as follows:*

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{i=N} |\phi_i\rangle \otimes |\psi_i\rangle$$

with $\{|\phi_i\rangle^A\}$ and $\{|\psi_i\rangle^B\}$ two orthonormal bases in $\mathscr{H}^A$ and $\mathscr{H}^A$ of dimension d_A, d_B respectively. N is equal to the lowest dimension.

For example, for two two-level systems 1 and 2 whose states can be written in the orthonormal basis $\{|\uparrow\rangle, |\downarrow\rangle\}$, any of their compound state can be written in the bases with four orthogonal states $|\uparrow\uparrow\rangle, |\downarrow\downarrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle$. Together, these basis states generate a Hilbert four-dimensional space. However, these bases are not unique, other orthonormal

bases, called *Bell bases*, are also possible, as follows:

$$\begin{cases} |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle) \\ |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle) \end{cases}$$

2.4.2 Tri-partite systems

The bi-partite entangled states can be extended to three parts. Similarly, we can define an entangled tri-partite state if and only if we cannot write it as the sum of products of the tri-partite state.

Defintion 2.4.4 *A state is called fully tri-partite entangled if and only if the decomposition:*

$$\rho = \sum_i p_i \rho_i, \quad \text{where } p_i \geq 0, \sum_i p_i = 1$$

eexists for all the states ρ_i and is factorizable in state products of at least two parts.

This definition excludes the totally separable states ($\rho = \rho_A \otimes \rho_B \otimes \rho_C$) and the bi-partite states ($\rho = \rho_{AB} \otimes \rho_C$). A case of tri-partite entanglement is the so-called state

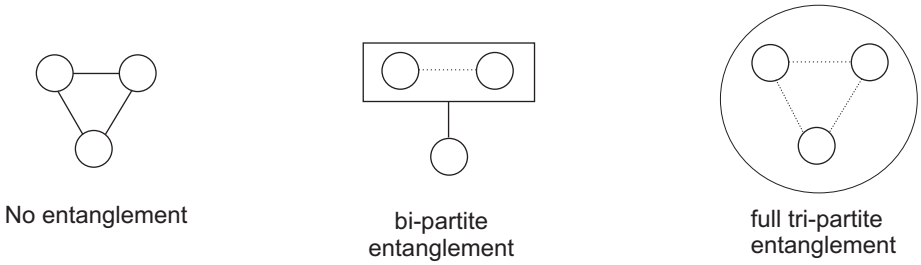


Figura 2.3: Types of entanglement in tri-partite systems.

Greenberger-Horne-Zeilinger or GHZ, defined as follows:

$$|\Psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\rangle)$$

2.4.3 N-partite entanglement

M.Seevinck and Uffink [83] [99] extended the study for the case of N systems.

Defintion 2.4.5 *Suppose we have an N-partite system described by a Hilbert space $\mathscr{H} = \mathscr{H}_1 \otimes ... \otimes \mathscr{H}_N$. A general state ρ of this system is called fully N-partite entangled if and only if the following factorization:*

$$\rho = \sum_i p_i \rho_i \quad \text{with } p_i \geq 0, \sum_i p_i = 1$$

exists in all the states ρ_i and is factorizable in state products of at least N parts.

An example of an N-state which is fully N-partite entangled, is the generalized state Greenberger-Horne-Zeilinger:

$$|\Psi^N_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow ... \uparrow\rangle + |\downarrow\downarrow ... \downarrow\rangle)$$

Defintion 2.4.6 *An N-partite state is called M-partite entangled $(M < N)$ if and only if there is a factorization as follows:*

$$\rho = \sum_i p_i \rho_i^{K_1^{(i)}} \otimes ... \otimes \rho_i^{K_{r_i}^{(i)}}$$

for each $i, K_1^{(1)}, ..., K_{r_i}^{(i)}$ are some partitions $\{1, ..., N\}$ in a subset disjunction r_i, and each subset $K_j^{(i)}$ contains maximum M elements; but no factorization is possible when all these subsets contain less than M elements.

All M-partite entangled M-particles with $M < N$ are called *non-fully entangled states* or *partially separable states*.

An example is the N - state which is made of $(N-1)$ - partite entangled, that is a tri-partite entangled state with four particles:

$$|\Psi\rangle = |\uparrow\rangle \otimes |\Psi^3_{GHZ}\rangle$$

2.5 Quantum Secret Sharing

The secret sharing was proposed for the first time by Blakley et al [16] [86] in 1979. The easiest way to describe it is as a secret shared by the sender in two parts for two receivers. The secret can be reconstructed only if both receivers act together, having either no knowledge about the original message.

In 1999, this concept was generalized for the quantum case by Hillery, Büzek and Berthiaume [47], who introduced the notion of quantum secret sharing (Q.S.S.). Quantum secret sharing plays an important role in the protection of secret quantum information. In 1999, it was presented the first scheme [47] using the three-qubit or four-qubit state Greenberger-Horne-Zeilinger (GHZ) for sharing securely an unknown random single-qubit state. Later, Cleve et al [26] described the general case of the scheme. In 2000, Bandyopadhyay [2] proposed a new Q.ST.S. scheme, using optimal methods, and in 2003, Hsu [48], proposed another method based on Grover's algorithm. The last scheme of secret sharing was introduced by Lance et al [56] in 2004 and is called quantum state sharing (Q.ST.S). In conclusion, all these methods are analyzing the case of a single-particle qubit or multi-particle qubit state.

The method of sharing the message in two parts [47] uses the maximal entangled three-particle states, also called Greenberger-Horne-Zeilinger states (GHZ states), and admits that Alice is sending a row of qubits to Bob and Charlie so that only by their cooperation the whole row can be determined. The quantum information is shared in two parts, and neither of them, taken separately, contains the original information, but they do, when taken together.

Suppose that Alice, Bob and Charlie have each a particle from the GHZ triplet with the state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Each of them will choose randomly how to measure the particle. They will announce publicly the basis in which they made the measurement, but they will not tell the result of the measurement. By the combination of the two results obtained by Bob and Charlie, they will be able to determine the result obtained by Alice at her measurement, which enables Alice to establish a connection key with Bob and Charlie, which she can use when sending the message. Suppose x and y the specific states:

$$|0_x\rangle = |+x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad |0_y\rangle = |+y\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$
$$|1_x\rangle = |-x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \quad |1_y\rangle = |-y\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

We can notice the effects of the measurements realized by Alice and Bob over the state of Charlie's qubit if we express the GHZ state in different ways. We write:

$$|0\rangle = \tfrac{1}{\sqrt{2}}(|+x\rangle + |-x\rangle), \quad |1\rangle = \tfrac{1}{\sqrt{2}}(|+x\rangle - |-x\rangle)$$

or:

$$|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_x + |1\rangle_x), \quad |1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_x - |1\rangle_x)$$
$$|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_y + |1\rangle_y), \quad |1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_y - |1\rangle_y)$$

We can write:

$$|\Psi\rangle = \frac{1}{2\sqrt{2}}[(|+x\rangle_a|+x\rangle_b + |-x\rangle_a|-x\rangle_b)(|0\rangle_c + |1\rangle_c) +$$

$$+(|+x\rangle_a|-x\rangle_b + |-x\rangle_a|+x\rangle_b)(|0\rangle_c - |1\rangle_c)]$$

This factorization of $|\Psi\rangle$ shows what can happen when Alice and Bob measure together in the x direction. If they obtain the same result, then Charlie will have the state $|0\rangle_c + |1\rangle_c/\sqrt{2}$; and if they obtain different results, Charlie will have the state $|0\rangle_c - |1\rangle_c/\sqrt{2}$. The following table presents the effects of the measurements of Alice and Bob over the state of Charlie's qubit:

		Alice			
		+x	-x	+y	- y
Bob	+x	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle - i\|1\rangle$	$\|0\rangle + i\|1\rangle$
	-x	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle + i\|1\rangle$	$\|0\rangle - i\|1\rangle$
	+y	$\|0\rangle - i\|1\rangle$	$\|0\rangle + i\|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$
	-y	$\|0\rangle + i\|1\rangle$	$\|0\rangle - i\|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$

Alice's measurements are presented in the columns, and Bob's in the rows. It is obvious that Charlie needs the measurement results of Alice and Bob. Similarly, Bob cannot determine Alice's measurement results without Charlie's help. If each of the parties chooses to perform randomly the measurements in the x or y bases, only half of GHZ triplets will offer the expected result. For example, if both Alice and Bob measure the

particles in the x, direction, Charlie must measure the particle in the same direction to determine if the measurement results of Alice and Bob are correlated or not. If he measures in the y, direction, he will obtain no information. Due to the fact that Charlie chooses a random measurement direction, only in half of the situations he will choose correctly. Therefore, it is very important that the three parties announce the measurement direction they used, in order to decide if they keep or not the results from the given triplet. This announcement is made as follows: Bob and Charlie will send to Alice the direction in which they performed the measurement, and Alice will then send them back the three measurement directions.

Intruders can affect the protocol of the Quantum Secret Sharing. Their types of attacks could be:

- **External attack**. Eve does not know the basis chosen by Bob and Charlie in order to have access to the qubits exchanged by them. If Eve measures the qubits, and sends them to Bob and Charlie, they will not form a GHZ state with Alice's qubit. Alice will realize this at the end of the process, when Bob and Charlie reveal publicly the parts in their possession.

- **Internal attack**. If an intruder captures and measures one of the qubits, this will lead to the destruction of the correlation of the three GHZ particles. Alice will realize this at the end of the process, when Bob and Charlie reveal publicly the parts in their possession.

2.6 Multi-party Quantum Secret Sharing

As it was mentioned above, the Quantum Secret Sharing scheme uses GHZ state, and Alice, Bob and Charlie choose randomly one of the measurement bases, similar to the protocol Bennett-Brassard of the secret key distribution. Generally, in order to establish the secret sharing scheme, it should be realized a detailed table, containing all the possible combinations of the measurement bases, and the possible results for all the parties. When the participants are in a great number, the construction of such a table is very difficult, and hard to use.

Next, we will present the scheme of quantum secret sharing for a great number of participants [105]. Suppose n parties participate in the process of secret sharing. The multiple GHZ state is as follows:

$$|\Psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}(|000..,0\rangle + |111..,1\rangle)$$

We will use a sequence $b_1(j), b_2(j), ..., b_i(j), ...b_n(j)$ to note the measurement bases of the information for Alice, Bob,..... for the j state of GHZ.

The number 1 is Alice's particle, the number 2 is Bob's particle, and so on. If $b_i(j) = 0$ then for the i group it is used the x basis, and if $b_i(j) = 1$ it means that the i group uses the y axis. The component $|00..,0\rangle$ can be written:

$$|00..,0\rangle = \prod_{i=1}^{n}(\sqrt{\frac{1}{2}}(|0\rangle_{b_i} + |1\rangle_{b_i}))$$

and the component $|11..,1\rangle$:

$$|11..,1\rangle = \prod_{i=1}^{n}(\frac{-i}{\sqrt{2}}(|0\rangle_{b_i} - |1\rangle_{b_i}))$$

When the y basis is chosen by an odd number of participants, the representation of $|00..,0\rangle$, can be extended as follows:

$$|11..,1\rangle = \frac{\pm i}{(\sqrt{2})^n}\prod_{i=1}^{n}(|0\rangle_{b_i} - |1\rangle_{b_i})$$

where the sign -ïs for $n = 2k+1$ and the sign ïs for $n = 4k+1$, where k is integer and positive. The GHZ state can be re-written:

$$|\Psi\rangle_{GHZ} = \frac{1}{2^{(n+1)/2}}(\prod_{i=1}^{n}(|0\rangle_{b_i} + |1\rangle_{b_i} \pm i\prod_{i=1}^{n}(|0\rangle_{b_i} - |1\rangle_{b_i})$$

for an odd number of participants who choose the y basis. In other words, for a set of measured values $i_2,...,i_n$ in the bases $b_2,...b_n$ by the participants Bob, Charlie, and so on, the results of Alice's measurements will have two alternatives.

If the number of the parties choosing the y basis is equal, then:

$$|\Psi\rangle_{GHZ} = \frac{1}{2^{(n+1)/2}}(\prod_{i=1}^{n}(|0\rangle_{b_i} + |1\rangle_{b_i} \pm \prod_{i=1}^{n}(|0\rangle_{b_i} - |1\rangle_{b_i})$$

Due to the fact that some terms from the second product have negative sign, they are canceling each other with the terms from the first product, obtaining only the terms 2^{n-1}. Among the terms 2^{n-1}, the values of the first bit, the result of Alice's measurement is uniquely determined by the $n-1$ values remained. In this case, when $n-1$ parties are gathered together, and the result is measured, they can determine uniquely the value of Alice's bit. If not all the $n-1$ participants are present, the determination of the value of Alice's bit is impossible. To conclude, the general rules for secret sharing among n parties are as follows:

1. The number of parties using the same basis must be equal;

2. When the number of parties using the y basis is equal to $2(2k+1)$, where k - is a non-negative integer, the value of Alice's bit is the sum modulo 2 of the bit values of the $n-1$ parties plus 1:

$$i_{Alice} = i_1 = i_2 \oplus i_3 \oplus ... \oplus i_n \oplus 1$$

3. When the number of parties choosing the y basis is $4k$, then the value of Alice's bit is the sum modulo 2 of the bit values of the $n-1$ parties:

$$i_{Alice} = i_1 = i_2 \oplus i_3 \oplus ... \oplus i_n$$

The scheme of Quantum Secret Sharing for n parties is as follows:

1. Alice prepares the GHZ state of the n particles;

2. Alice keeps a particle and sends the rest of $n-1$ particles to the $n-1$ participants, receiving each one particle;

3. Each party chooses randomly one of the x or y measurement bases to measure the particle. They keep the measurement result and the information related to the measurement basis they used.

4. The procedures $1-3$ are repeated several times until a sufficient number of results was obtained. This could be at least twice the desired number of shared bits;

5. After the procedure 4, every participant, using a classical communication channel, sends information to Alice regarding the measurement basis they chose. Alice keeps track of the number of parties who chose the y basis. Alice announces publicly the nature of this number for each round: an odd or even number of the form $2(2k+1)$, or an even number of the form $4k$. The exact number of k must not be revealed. If the number is odd, then this round of measurements is cancelled, and if the number is even, all the participants will keep the values they measured, as well as the information concerning the basis used in this case.

6. Alice selects a sufficiently big set of such cases, and asks the participants to reveal the measurement results. This information is necessary in order to determine the existence of potential intruders. If the error ratio is high, Alice concludes that there are intruders, and the session of quantum secret sharing is cancelled. If the error ratio is low, the session of quantum secret sharing is considered secure, and they will continue with quantum errors correction, and privacy amplification, obtaining in the end the row of bits of the shared secret. The $n-1$ participants can determine the bit from the shared secret using the rules of quantum secret sharing for each valid transmission.

3. Quantum communication

3.1 Mixed states. Density operator

Are many situations when the studied quantum systems can be found in the state $|\Psi_i\rangle$ with a probability p_i. In this cases, we can't know for sure what is the status of the system, therefore we can only do a random description of the system. This description random should not be confused with probabilistic behavior of the system. A quantum system whose status is not completely known, we can say that are in a **mixed state**, and if the status of the system quantum is known accurately, means that the system is in a **pure state**.

A pure state is a special case of mixed state, in which $p_i = 1$ for some i şi $p_j = 0 (j \neq i)$.

Some example of mixed state in the following cases:

- Suppose a total polarized light fascicle (polarization vector oscillates in all directions) and we want to measure if photons are vertically or horizontally polarized. The measurements result of a particular photon can be either horizontal or vertical. Therefore, when the fascicle pass through a linear polarizer, the fascicle intensity is halved, because this is a mixture of polarized photons of the vertical and horizontal directions.

- A source of particles emit particles on state $|\Psi_i\rangle$ with a probability $p_i, (1 \leq i \leq N)$.

We can see that, a specially state $|\Psi_i\rangle \in H$ appear with a probability p_i, in which case the expected value of the observable a is: $\langle\Psi_i|A|\Psi_i\rangle$, where $|\Psi_i\rangle$ is normalized: $\langle\Psi_i|\Psi_i\rangle = 1$.

This means that the value of a is given by:

$$\langle A\rangle = \sum_{i=1}^{N} p_i \langle\Psi_i|A|\Psi_i\rangle$$

where N - number of available states.

The density operator (matrix) describes a quantum system whose state is not complete known.

We introduce **the density operator**:

$$\rho = \sum_{i=1}^{N} p_i |\Psi_i\rangle\langle\Psi_i|$$

If $\rho = |\Psi_i\rangle\langle\Psi_i|$, means that the quantum state of the system is known, so it is in a pure state.

Therefore, we can write the value of a, as:

$$\langle A\rangle = tr(\rho A)$$

Density operator (matrix) was introduced to describe ensembles of quantum states.

3.1.1 Properties of density operator

An operator ρ is the density operator associated with an ensemble $\{p_i, |\Psi_i\rangle\}$, if and only if it satisfies the following conditions:

1. Trace of ρ is equal to 1.
2. ρ is a positive operator.

So, we can define the operator density as a positive operator with trace equal to 1.

Taking into account the density operator, we reformulate some of the postulates of quantum physics, as follows:

Postulate 1. A quantum system is complete described by its density operator, which is a positive operator, with trace equal to 1, and acting on the state space of the system.

Postulate 2. The evolution of a closed quantum system can be described by a unitary transformation U. If ρ is the system state at time t_1 and $\rho^{'}$ is the state at time t_2, we have:

$$\rho^{'} = U\rho U^{\dagger}$$

Postulate 4. The state space of the compound physical system is the tensor product between the state spaces of the component systems: $\rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n$.

3.1.2 Reduced density operator

To analyze the components of a composed quantum system was introduced **reduced density operator**.

Suppose we have physical systems A and B, whose state is described by density operator ρ^{AB}. We define the reduced density operator of the system A, as follows:

$$\rho^{A} \equiv tr_B(\rho^{AB})$$

where tr_B is called **partial trace** over system B.

The partial trace is defined as:

$$tr_B(|a_1\rangle\langle a_2 \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2|tr(|b_1\rangle\langle b_2|)$$

where $|a_1\rangle$ and $|a_2\rangle$ are any vectors in the state space of A, and $|b_1\rangle$ and $|b_2\rangle$ are any vectors in the state space of B.

The trace operator appears in the right term, and addressing system B: $tr(|b_1\rangle\langle b_2|) = \langle b_1|b_2\rangle$.

The reduce density operator offers a description of the A's system state. Reduced density operator provides accurate measurement statistics for measurements on system A.

3.2 Shannon classical entropy

Entropy is a measure of uncertainty. The term was borrowed from the thermodynamic entropy, a branch of physics in which the phenomena studied are mainly probabilistic.

The concept of source entropy was introduced by Shannon [87] in classical information theory.

A discrete information source emits a series of letters $\{x_1, x_2, ..., x_L\}$ from an alphabet of L. We assume that each letter of the alphabet $\{x_1, x_2, ..., x_L\}$ has a given probability of occurrence p_k:

$$p_k = P(X = x_k), 1 \leq k \leq L$$

where $\sum_{k=1}^{L} p_k = 1$

We are interested to evaluate the amount of information that comes from the source.

The entropy of the source is defined as follows:

$$H(X) = -\sum_{i-1}^{n} p_i \log p_i = \langle \log \frac{1}{p} \rangle \tag{3.1}$$

with $x \log x = 0$ în $x \to 0$.

Entropy is the average information per symbol (an average of the obtained information for each symbol). Entropy is equal to the priori average uncertainty of events. Point out that entropy is a measure of the information emitted by the source as a whole and is not an information emitted by any symbol. Maximum entropy is when symbols are *equally probable*.

Only in this case, the issuance of a symbol (a bit) transmits a ïnformation"bit.

In information theory, entropy is a measure of the uncertainty of an event. Entropy is a *measure of the existing disorder*.

Source redundancy is defined as the difference between the maximum possible entropy and the real entropy (source emits useless):

$$R_S = H_{MAX}(S) - H(S)$$

where $H_{MAX}(S) = \log n$ - a source entropy with n symbols and equal probability of occurrence.

We can use the notion of *relative redundancy*:

$$r_S = 1 - \frac{H(S)}{H_{MAX}(S)}$$

3.2.1 Properties of Shannon entropy

1. Informational entropy, the measure of information, is an nonnegative entity :

$$H(p_1, p_2, ..., p_n) \geq 0.$$

2. If for an index $i \in \{1, 2, .., n\}$, we have $p_i = 1$, then the informational entropy is zero:

$$H(p_1, p_2, ..., p_n) = 0.$$

.

3. The entropy of a system of events is maximum (highest) when events have the same probability of occurrence:

$$H(p_1, p_2, ..., p_n) \leq H(1/n, 1/n, ..., 1/n).$$

4. Events impossible not change the value of information entropy of a system:

$$H(p_1, p_2, ..., p_n, 0) = H(p_1, p_2, ..., p_n).$$

5. The product of several independent sources of information is equal with the sum of entropy of each source separately:

$$H(X_1 \times X_2 \times .....X_n) = H(X_1) + H(X_2) + ..H(X_n).$$

The product of several sources of information is a compound experiment that consists of the simultaneous realization of each event corresponding to each source.

6. The entropy of the product of any two X and Y source of information is:

$$H(X \times Y) = H(X) + H(Y/X).$$

where $H(Y/X)$ is the average amount of information that is obtained after completion of the experiment Y, conditioned by the experiment X.

Two X and Y experiments have properties:

7. $H(Y/X) \leq H(Y)$
8. $H(X \times Y) \leq H(X) + H(Y)$
9. $H(X/Y) = H(Y/X) + H(X) - H(Y)$

3.2.2 Types of Shannon entropy

Shannon entropy can be used to define "ways"to measure information.

There are four types of such measurements:

1. *Relative entropy* - which measures the similarity between two random events.

$$H(X||Y) = -\sum_{x,y} p(x) \log(p(x)) - H(X) = \sum_{x,y} p(x) \log p(x)/p(y)$$

The relative entropy is the difference between the expected and the obtained information from Y events given that they are distributed according to X.

2. *Common entropy* - which measures the combined information of two random events.

$$H(X,Y) = -\sum_{x,y} p(x,y)\log(p(x,y))$$

If X and Y are independent, is available the sum operation of entropies.

3. *Mutual entropy* - measures the correlation between two random events.

$$I(X:Y) = H(X) - H(X|Y)$$

If X and Y are independent, then, the mutual entropy between X and Y is zero. If they are fully correlated, then the mutual information between them is the same as that contained by X. Mutual entropy is *symmetric*:

$$I(X:Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(X:Y)$$

3.3 Von Neumann quantum entropy

Consider a quantum system in state $|\Psi\rangle$. This state can be represented as a mixture of pure states $|x_i\rangle$. These pure states which cannot be represented as mixtures of pure states, are orthogonal one to each other and have unit length, so that $\langle x_i|x_j\rangle = \delta_{ij}$.

A set of pure states $\{|x_i\rangle\} = \{|x_1\rangle, |x_2\rangle, ..., |x_n\rangle\}$, define an orthonormal basis for a space n - dimensional of all possible quantum states of the system. Any state $|\Psi\rangle$ supports a unique decomposition of the form:

$$|\Psi\rangle = \{x_1|x_1\rangle, x_2|x_2\rangle, ..., x_n|x_n\rangle\} = \sum_{i=1}^{n} x_i|x_i\rangle$$

where $x_i, i = 1...n$ are complex coordinates.

We represent a quantum system with state $|\Psi\rangle$, and $\langle\Psi|\Psi\rangle = \sum_i |x_i|^2 = 1$, where $p_i = |x_i|^2$ is the probability of finding state $|\Psi\rangle$ in a pure state $|x_i\rangle$.

A quantum system in the state $|\Psi\rangle$ acts as the source of "random events" and the concept of "information" and "entropy" may be associated with such a system. We use the concept of *density operator*, means we use another way to represent a quantum system in the state $|\Psi\rangle$:

$$\rho = \sum_{i=1}^{n} p_i|x_i\rangle\langle x_i|$$

where: $|x_i\rangle\langle x_i|$ is the projection of operator on basis state $|x_i\rangle$. It is obvious that $\rho|x_i\rangle = p_i|x_i\rangle$, which shows that $|x_i\rangle$ is an eigenstate of ρ with eigenvalue p_i.

As we know, the matrix elements ρ_{ij} of density operator satisfies the relation $\rho_{ij} = \langle x_i|\rho|x_j\rangle = |x_i|^2 = p_i\delta_{ij}$, which indicates that the matrix is diagonal in the computing basis $\{|x_i\rangle\}$.

The matrix of ρ is:

$$\rho = \begin{pmatrix} p_1 & 0 & ... & 0 \\ 0 & p_2 & ... & .. \\ ... & ... & ... & 0 \\ 0 & ... & 0 & p_n \end{pmatrix}$$

We have:

$$\rho \log \rho = \begin{pmatrix} p_1 \log p_1 & 0 & ... & 0 \\ 0 & p_2 \log p_2 & ... & .. \\ ... & ... & ... & 0 \\ 0 & ... & 0 & p_n \log p_n \end{pmatrix}$$

Standard measurement of information contained in a quantum system described by the statistical operator ρ, is **the von Neumann entropy** $S(\rho)$ [67], defined as:

$$S(\rho) = -tr(\rho \log \rho) = -\sum_{i=1}^{n} p_i \log p_i \tag{3.2}$$

Comparing equations (3.1) and (3.2) we obtain $S(\rho) = -tr(\rho \log \rho)$ which is strictly analogous with Shannon classical entropy. The only difference is that in quantum case, the source is characterized by the density operator ρ, not by the probability distribution.

The Neumann entropy represent the measurement of the quantum information contained by a quantum system (quantum state ρ, with $S(\rho) > 0$). A pure state $\rho = |\varphi\rangle\langle\varphi|$, has $S(\rho) = 0$.

In a both cases, classical and quantum, we can speak about *common von Neumann entropy* $S(A,B) \equiv S(\rho_{AB})$, $S(A,B,C) \equiv S(\rho_{ABC})$.

3.3.1 Properties of von Neumann entropy

1. *Von Neumann entropy* is additive for independent systems. Given two density matrices describing independent systems A and B, we have:

$$S(\rho_A \otimes \rho_B) = S(A) + S(B)$$

2. *Von Neumann entropy* - is strongly subadditive for any three systems A, B, and C:

$$S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$$

3. *Von Neumann entropy* is concave:

$$S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i)$$

4. *Von Neumann entropy* is invariant under changes in the basis of ρ, that is:

$$S(U \rho U^{\dagger}) = S(\rho)$$

5. *Araki-Lieb inequality*. The von Neumann entropy is also strongly subadditive. Given three Hilbert spaces: A, B, C:

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$$

Each of the three numbers $S(\rho_{AB})$, $S(\rho_{BC})$ and $S(\rho_{AC})$ is less than or equal to the sum of the other two. By using the proof technique that establishes the left side of the triangle inequality above, one can show that the strong subadditivity inequality is equivalent to the following inequality.

$$S(\rho_A) + S(\rho_C) \leq S(\rho_{AB}) + S(\rho_{BC})$$

3.3.2 Types of von Neumann entropy

The von Neumann entropy of ρ, which is the quantum mechanical analogy of the Shannon entropy, is given by:

$$S(\rho_{AB}) = Tr\rho_{AB} log \rho_{AB}$$

Like the classic case, in quantum case are several types of entropy. These are:

1. *Relative quantum entropy* - is defined between two states ρ and σ of a quantum system, as:

$$S(\rho||\sigma) \equiv tr(\rho(\log_2 \rho - \log_2 \sigma))$$

This quantity provide from Klein inequality:

$$S(\rho||\sigma) \geq 0$$

becomes equality if only $\rho = \sigma$.

2. *Mutual quantum entropy* - is a measure of correlation between subsystems (with states ρ_A and ρ_B) of quantum state.

$$I(A:B) = I(\rho_{AB}) \equiv S(A) + S(B) - S(A,B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

Using the strongly subadditive property can be written the mutual quantum entropy as a relative entropy as follows:

$$I(A:B) = S(\rho_{AB}||\rho_B \otimes \rho_B)$$

3. *Conditional quantum entropy*:

$$S(A|B) \equiv S(A,B) - S(B) = S(\rho_{AB}) + S(\rho_B)$$

Unlike the classical conditional entropy, the conditional quantum entropy can be negative. This is true even though the quantum von Neumann entropy of single variable is never negative.

The negative conditional entropy is also known as the coherent information, and gives the additional number of bits above the classical limit that can be transmitted in a quantum dense coding protocol.

Positive conditional entropy of a state thus means the state cannot reach even the classical limit, while the negative conditional entropy provides for additional information.

3.4 Quantum communication

3.4.1 Classical communication channels

When we send information from source to destination we must consider the efficiency and security of transmission. To ensure efficiency is necessary to minimize the amount of transmitted data, means to compress it. This compression can be with or without loss of information.

Another important issue is ensuring the confidentiality and security of message content, against the actions of intruders using cryptographic methods. Compression and encryption information are tasks that are part of *coding source*.

The information is transmitted from source to destination through a communication channel. As we know, we can choose exactly how the source information is structured and how it is treated at the receiver, but the channel behavior does not depend on us. There are many types of channels. No matter the type of channel, the effect is the distortion of information that passes through it.

The aim is to protect the information, communication in general, by using error detection and correction codes. Information coding in order to protect against errors caused by channel coding part of the channel. Coding information, to protect against errors, is part of *channel coding*.

Most of the scientific community believes that the early profile information theory was marked by the appearance of the article "A Mathematical Theory of Communications"written by Claude Shannon in 1948. There were two related disciplines: information theory and coding theory, the main aim being a safe and efficient transmission of information, typically through a hostile environment.

We believe that the transmission is secure, if the information received is identical to the transmitted and the tolerance required is relatively small. Transmission is efficient if the effort and time consumption are minimized.

Let be:

- X - the set of emitted messages of a information source (input);
- Y - the set of received messages (output);
- $p(y/x)$ - the probability to receive the message $y \in Y$ when is given $x \in X$.

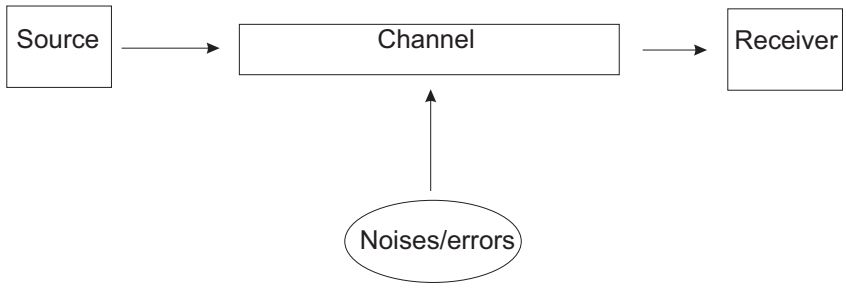


Figura 3.1: Scheme of Transmission information system

In the figure (3.1) is shown schematically a transmission system.

Transmission information system consists of two finite sets X and Y and a conditional probability $p(y/x)$, defined on Y for every $x \in X$ is denoted by $[X, p(y/x), Y]$.

Source of transmission information system is represented by probability field $\{X, x, p(x)\}$, for a emission probability $p(x)$ with $\forall x \in X$, such that $\sum_{x \in X} p(x) = 1$.

Receiver of transmission information system is represented by probability field $\{Y, y, p(y)\}$, for a emission probability $p(x)$ with $\forall x \in X$, and, the reception probability can be calculate using relation: $p(y) = \sum_{x \in X} p(x) p(y/x)$.

The propagation environment of information from the source to the receiver, is called *channel of transmission information system*.

We can know the communication channel of a system, if we know the probabilities $p(y/x)$ for all messages $x \in X$ şi $y \in Y$.

If $p(y/x)$ takes only the values 0 or 1 for every $x \in X$ and $y \in Y$, on channel does not acting perturbations. Otherwise, it is a noisy channel.

In a transmission information system, the entropies of events at the input and output are:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x) \quad H(Y) = -\sum_{y \in Y} p(y) \log_2 p(y)$$

If we denote by $p(x/y)$ the probability to emit a message $x \in X$, when it receives $y \in Y$, the expression:

$$H(X/y) = -\sum_{x \in X} p(x/y) \log_2 p(x/y)$$

represent the amount of information that must be emitted by the source to receive the message $y \in Y$.

The average amount of emitted information needed to receive the whole set of messages $y \in Y$ will be:

$$H(X/Y) = -\sum_{y \in Y} p(y) H(X/y)$$

The communication channel is a probabilistic output depends on the input.

For a communication channel with input X and output Y, *capacitance* C is defined by:

$$C = \max_{p(x)} I(X;Y)$$

where $I(X;Y)$ is the mutual entropy.

$$I(X;Y) = H(X) - H(X/Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$

The mutual entropy $I(X;Y)$ is a measure of dependence between two random variables. The entropy is symmetrical about X and Y, and, is always non-negative.

Capacity is the maximum velocity that can be transmitted the information through the channel, and, the output information can be recovered with a probability of error extremely low.

Example of communication channels:

- *Binary symmetric channel without noises.* In this channel, the input binary 1 or 0, is reproduced accurately as the output, without errors. Each transmission can deliver safely 1 bit, and capacity is $C = 1$ bit.

- *Binary symmetric channel with noises.* - communication systems affected by noises.

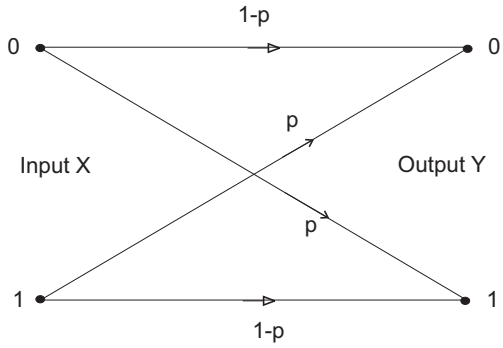


Figura 3.2: Binary symmetric channel

The channel has a binary input;
- with probability $1-p$ the input is the same as the output,
- with probability p, 0 will be received as 1 and 1 is received as 0.
In this case the capacity is $C = 1 + p\log p + (1-p)\log(1-p)$ bits per transmission.

3.4.2 Quantum communication channels

To study the transmission of a quantum channel N, denote by: D - the capacity of transmission of a quantum data; C - the capacity of transmission of a classical data, and, $Q_{1,2}$- the mixed ability for transmitting quantum states.

According to Shannon's theory, classical channel capacity $C(N)$ can be defined as supremum transmission rate $R := k/n$ of classic word with length k - bits, so:

1. Transmission is carried out by a coding word, n-bits words that are transmitted through the channel N, followed by a decryption.

2. The fidelity of transmission is asymptotically 1. Quantum channel capacity $Q(N)$ is defined similar to the classical case where we replace the traditional input / output words with k - pure or mixed states of qubits (Bennett and Shor, 1998).

The quantum channels, are *quantum erase channels*, there is a probability p that the channel to replace a qubit with the orthogonal symbol of states $\{|0\rangle, |1\rangle\}$, and, a complementary probability $1-p$ to leave the qubit in the same state. For these types of channels $C = Q_2 = 1-p$ and $Q = max\{0, 1-2p\}$.

Unlike the classical case, where capacity can be calculated by maximizing mutual information between input and output in a single use of the channel, capacity of quantum channels does not allow a similar calculation.

In quantum case, encoding is achieved by mixing of states of the input data, and, decoding is done through common measures of output states. Mix state between sender and recipient improves the capacity of transport of the quantum channels (note for dense coding and quantum teleportation).

Passing quantum systems through communication channels, causes *decoherence* and *interference*, phenomena that influence the quantum states. Decoherence occurs as a result of the interaction between a quantum system and the environment, and interference occurs as a result of the interaction between quantum systems.

The following are some of the types of distortion that can occur when crossing quantum information through noisy communication channels.

3.4.3 Depolarization

Depolarization when passing through the communication channel is a model of decoherence of the quantum system. It can be described as: when pass through the communication channel a quantum system state (qubit) remains intact with probability $1-p$, while with probability p there is an "error".

Types of quantum errors

There are three types of errors: *bit-flip*; *phase-flip* and *both*.

- **Bit-flip** - a qubit has the effect of shifting its state.

$$\begin{array}{l}|0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle,\end{array} \quad |\Psi\rangle \to \sigma_1|\Psi\rangle \quad \texttt{where} \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- **Phase-flip** - over a qubit determines a phase-flip (the basic vector $|1\rangle$ is rotated by 180°).

$$\begin{array}{l}|0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle,\end{array} \quad |\Psi\rangle \to \sigma_2|\Psi\rangle \quad \texttt{where} \quad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- **Bit-flip and Phase-flip** - over a qubit has the effect of shifting both the state and the phase:

$$\begin{array}{l}|0\rangle \to i|1\rangle \\ |1\rangle \to -i|0\rangle,\end{array} \quad |\Psi\rangle \to \sigma_3|\Psi\rangle \quad \texttt{where} \quad \sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Therefore, if an error occurs, then state quantum system (qubit) $|\Psi\rangle$ can evolve with equal probability, to one of the three states $\sigma_1|\Psi\rangle, \sigma_2|\Psi\rangle, \sigma_3|\Psi\rangle$.

Unitary representation

Depolarization can be represented by a unitary operator acting on $H_A \otimes H_E$, where H_E - has 4 - dimensions and represents the environment. The operator shall:

$$U_{AE}|\Psi_A\rangle \otimes |0_E\rangle \longrightarrow \sqrt{1-p}|\Psi_A\rangle \otimes |0_E\rangle + \sqrt{\frac{p}{3}}[\sigma_1|\Psi_A\rangle \otimes |1_E\rangle + \sigma_2|\Psi_A\rangle \otimes |2_E\rangle +$$

$$+\sigma_3|\Psi_A\rangle \otimes |3_E\rangle]$$

The environment will perform one of the four states orthogonal, to determine the type of error is necessary to measure the environment using basis $\{0,1,2,3\}$.

3.4.4 Quantum amortization phase

Unitary representation

The unitary representation of channel is:

$$|0\rangle_A|0\rangle_E \to \sqrt{1-p}|0\rangle_A|0\rangle_E + \sqrt{p}|0\rangle_A|1\rangle_E$$
$$|1\rangle_A|0\rangle_E \to \sqrt{1-p}|1\rangle_A|0\rangle_E + \sqrt{p}|1\rangle_A|2\rangle_E$$

This could be explained as the environment E would be scattered by qubits, occasionally (with probability p), its status is changed to $|1\rangle_E$ if it spreads qubit is in the state $|0\rangle_A$, or pass into the state $|2\rangle_E$ if the qubit is in the state $|1\rangle_A$. The phenomenon can be understood as a clash between small particles (environment E) with heavy particles (quantum systems / qubits A) and has the effect scattering of environment particles and change their status, according to the state qubits that collided. Unlike depolarization, in this case, channel removes one basis of qubit A, the basis $\{|0\rangle_A, |1\rangle_A\}$ is the only base that bit-flip errors do not occur.

3.4.5 Amplitude amortization

The quantum states (qubits) that are transmitted through the communication channel is encoded by excited states of atoms: the ground state of the atom = status $|0\rangle$ respectively excited state = state $|1\rangle$. This channel can be explained as a schematic de-excitation model of excited states of an atom by emission of a photon. By detecting photons ("observing the environment") can achieve a POVM (Positive Operator Valued Measure) which will provide information about the initial state of the atom.

Unitary representation

Consider quantum information (qubits) that is transmitted through the channel as represented by atoms. We denote the ground state (non-excited) atom with $|0\rangle_A$ and the excited state $|1\rangle_A$. Channel's environment is an electromagnetic field in a state of vacuum $|0\rangle_E$. When passing through the channel, there is possible (with probability p) that the excited atom to flip into ground state (non-excited), after its de-excitation is delivered a photon. Following de-excitation, the environment undergoes a transition from state $|0\rangle_E$ (without photon) to state $|1\rangle_E$ (with the photon). This evolution is described by the unitary operator acting on the atom and the environment, as follows:

$$|0\rangle_A|0\rangle_E \to |0\rangle_A|0\rangle_E$$
$$|1\rangle_A|0\rangle_E \to \sqrt{1-p}|1\rangle_A|0\rangle_E + \sqrt{p}|0\rangle_A|1\rangle_E$$

Suppose that the atom is in a state superposition (non-excited and excited states) and pass the communication channel, the state of the entire system is:

$$(a|0\rangle + b|1\rangle)_A|0\rangle_E \to (a|0\rangle_A + b\sqrt{1-p}|1\rangle_A)|0\rangle_E + \sqrt{p}|0\rangle_A|1\rangle_E$$

If a photon is not detected, then using the projection of environment's state $|0\rangle_E$, is obtained the atom's state:

$$a|0\rangle_A + b\sqrt{1-p}|1\rangle_A.$$

A POVM performs an orthogonal measurement, that is measured the initial state of the atom in base $\{|0\rangle_A, |1\rangle_A\}$.

3.4.6 Quantum data compression

Fidelity

A pure state of a quantum system is given by a unit vector Hilbert space.

Suppose a source emits quantum pure states $|\varphi\rangle$. After coding and decoding that we have a state $|\Psi\rangle$ instead of $|\varphi\rangle$. We need to know how close are that the two states. Quantum mechanics uses the concept of transition probability $|\langle\varphi|\varphi\rangle|^2$, which takes values between 0 and 1. The transition probability is equal to 1 if and only if that the two state are the same, this means the states are equal to a phase. Square root of the transition probability is called ***fidelity***

$$F(|\varphi\rangle, |\Psi\rangle) = |\langle\varphi|\Psi\rangle|$$

Shannon uses a measure of distortion and can look at $1 - F(|\varphi\rangle, |\Psi\rangle)$ as a function of the distortion quantum state. Under the action of quantum operations, pure states can be transformed into mixed states, extending fidelity to:

$$F(|\varphi\rangle, \langle\Psi|, \rho) = \sqrt{\langle\varphi|\rho|\Psi\rangle}$$

or as general form:

$$F(\rho_1, \rho_2) = tr\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}}$$

for positive matrix ρ_1 şi ρ_2.

Schumacher coding

The optimum method to communicate through channels without noise using pure quantum states, is equivalent to data compression. As is well known, the compression limit of conventional data is given by the entropy of the probability distribution data. The limit of quantum data compression is given by the von Neumann entropy of the set of states that is intended to be compressed.

Quantum data compression has been studied by Schumacher in 1995 [82].

In order to quantify the compressibility of quantum information, have introduced the *subspace* term. The basic idea of Schumacher quantum coding theorem is that we can encode on subspace without losing fidelity.

Let $A := \{|\varphi_x\rangle, p_x\}_{x=1}^{|A|}$ be a "quantum alphabet" consisting of many distinct quantum states (not necessarily orthogonal), each of them corresponding probabilities ($\sum_x p_x = 1$). The density matrix of a single letter is:

$$\rho = \sum_x p_x |\varphi_x\rangle\langle\varphi_x|$$

Because the letters are independent, the collection of messages with n - letter is represented by a density matrix:

$$\rho^n \equiv \rho \otimes ... \otimes \rho$$

which will have a Hilbert space with maximum dimension $2^{n \log_2 |A|}$.

The question is: it can compress the information contained in $\rho^{\otimes n}$? The answer was found by Schumacher in 1995 and is similar to the first theorem of Shannon: asymptotically ($n \geq 1$) the state $\rho^{\otimes n}$ is compressed to a state in the $2^{nS(\rho)}$ dimension Hilbert space, with a *fidelity* F arbitrarily close to 1 (probability of the coding state coincides with the decoded state).

In other words, can be compressed to $nS(\rho)$ qubits. $S(\rho)$ can be considered as the average number of qubits for quantum information essential per each character in the alphabet.

The density matrix $\rho = \sum_r \lambda |r\rangle\langle r|$ is diagonalized. Von Neumann entropy $S(\rho)$ coincides with the Shannon entropy $H(D)$ of the classical alphabet $D := \{r, \lambda_r\}_{r=1}^{|D|}$.

We introduce typical messages of these strings as tensorial product of vectors $\varphi_{i_1...i_n} := |\varphi_{i_1}\rangle...|\varphi_{i_n}\rangle$ in the orthonormal basis in which the density matrix ρ was diagonalized, so that their probability $\lambda_{i_1...i_n} := \prod_j \lambda_{i_j}$ satisfy $\lambda_{i_1...i_n} \sim 2^{-nH(D)}$ for $n \gg 1$.

$\rho^{\otimes n}$ is asymptotically concentrated in a typical subspace T, let P_T be the projection on this subspace, with $tr(P_T \rho^{\otimes n}) \sim 1$. Compression strategy is to develop projections of the original message, on subspace T or on subspace $T^{\perp}$.

3.5 Schmidt decomposition

If $|\Psi^{AB}\rangle$ is a bipartite state (consisting of parts A and B), and $|i^A\rangle$ respectively $|j^B\rangle$ are basis for systems A and B, then we write $|i^A\rangle$, as follows:

$$|\Psi^{AB}\rangle = \sum_{i,j} \beta_{ij} |i^A\rangle |j^B\rangle \tag{3.3}$$

for β_{ij} - real and non-negative numbers, $\sum_{i,j} \beta_{ij}$ are *Schmidt coefficients*, and basis $|i^A\rangle$ respectively $|j^B\rangle$ are *Schmidt basis* for A and B.

Schmidt decomposition [69] for two basis $|\Psi_i^A\rangle$ and $|\Phi_i^B\rangle$, so that $|\Psi^{AB}\rangle$ is written:

$$|\Psi^{AB}\rangle = \sum_i \alpha_i |\Psi_i^A\rangle |\Phi_i^B\rangle \tag{3.4}$$

is a more convenient form because it uses the sum by i compared to the sum by i and j.

Based on Schmidt decomposition, the system A and B can be written:

$$tr_A(|\Psi^{AB}\rangle) = \sum_i |\alpha_i|^2 |\Psi_i^A\rangle\langle\Psi_i^A| \tag{3.5}$$

$$tr_B(|\Psi^{AB}\rangle) = \sum_i |\alpha_i|^2 |\Phi_i^B\rangle\langle\Phi_i^B| \tag{3.6}$$

We can determine whether the two systems are mixed. It is important to note that Schmidt decomposition can be applied only to pure states.

Suppose that A is an m - dimensional system and B is an n - dimensional system, where $m > n$ (without loss of generality, as long as the two systems are interchangeable). We can build Schmidt decomposition [69] using the following steps:

1. The density operator can be written:

$$\rho^{AB} = |\Psi^{AB}\rangle\langle\Psi^{AB}| = \sum_{i,j} \alpha_{ij} |i^A j^B\rangle \sum_{k,l} \alpha^*_{kl} |k^A l^B\rangle =$$

$$= \sum_{i,j,k,l} \alpha_{ij}\alpha^*_{kl} |i^A\rangle\langle k^A| \otimes |j^B\rangle\langle j^B| \tag{3.7}$$

2. Follow the system B:

$$\rho^A = tr_B(\rho^{AB}) = \sum_r \sum_{i,j,k,l} \alpha_{ij}\alpha^*_{kl} |i\rangle\langle k| \otimes \langle r|j\rangle\langle l|r\rangle =$$

$$= \sum_{i,j,r} \alpha_{ir}\alpha^*_{kr} |i\rangle\langle k| \tag{3.8}$$

3. Diagonalizing ρ^A to give:

$$\rho^A = \sum_i |\beta_i| |\Psi_i\rangle\langle\Psi_i| \tag{3.9}$$

4. Express $|\Psi^{AB}\rangle$ in terms of $|\Psi^A_i\rangle$ thus:

$$|\Psi^{AB}\rangle = \sum_{i,j} c_{ij} |\Psi^A_i\rangle |j^B\rangle \tag{3.10}$$

where $c_{ij} = \langle\Psi^A_i| j^B |\Psi^{AB}\rangle$.

5. To obtain the system B in Schmidt form, we define $|\Phi_i\rangle$:

$$|\Phi_i\rangle = \sum_j \frac{c_{ij}}{\beta_i} |j\rangle \tag{3.11}$$

$|\Phi_i\rangle$ is orthogonal, if $\langle\Phi_i|\Phi_j\rangle = 0$.

6. We can rewrite $|\Psi^{AB}\rangle$ by $|\Psi^A_i\rangle$ and $|\Psi^B_i\rangle$, such that:

$$|\Psi^{AB}\rangle = \sum_{i,j} c_{ij} |\Psi^A_i\rangle |j^B\rangle = \sum_{i,j} \beta_i |\Psi^A_i\rangle \frac{c_{ij}}{\beta_i} |j^B\rangle = \sum_i \beta_i |\Psi_i\rangle |\Phi_i\rangle \tag{3.12}$$

where β_i are Schmidt coefficients. They can be calculated from the matrix::

$$tr_B(|\Psi\rangle\langle\Psi|)$$

This matrix has the eigenvalues λ_i.

The Schmidt number is used to determine that the system state is separable or not, as follows:

- if the state of a composed system is *separable*, the number Schmidt $= 1$,
- if the state of a composed system is *mixed*, the number Schmidt > 1.

Schmidt decomposition is very important when it discusses about mixed systems (entangled). It can be seen that: if we follow each part A or B, the remaining part of the density operator has the same eigenvalues, means that the two parts are mixed, at par.

3.6 Mixed-state entanglement and distillation

The phenomenon of mixed state is very important in quantum information theory, in processes such as quantum teleportation, dense coding, etc. In terms of these protocols, a state of qubits pair $\Psi^+ = \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$ (are mixed maximal) is a unit of entanglement, called *e-bit*.

Suppose that two parties, Alice and Bob want to achieve a protocol that is based on the phenomenon of entanglement, but instead to share copies of the state Ψ^+, they will share copies of the other quantum state Φ. For example, Φ can be a copy of "distorted", full of noise, parasites of state Ψ^+ that will not allow the transmission of quantum information sufficiently accurate, or, Φ can be a strange quantum state, a mixed state which is not resemblance to Ψ^+.

Distillation of the mixed-state, first introduced by Bennett [69], allows Alice and Bob to apply only local quantum operations and communicate classically (protocol LOCCC - Local Operations and Classical Communications), that a number of copies of states Φ can be transformed into a number (perhaps smaller) of copies of Ψ with a high accuracy.

When it is possible for Alice and Bob to make one or more copies of Φ at least one copy of Ψ with very high accuracy, we say that Φ is *distilled*. In general mixed states,

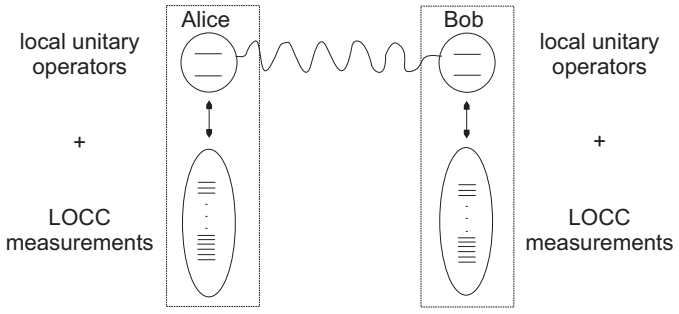


Figura 3.3: Quantum state distillation

they are entangled but not distilled. These states are called *bounded mixed states*. All such states have the property that the partially transposed density operator of that state is

positive semi-defined. This is called *PPT (positive partial transpose)*, and any PPT state is undistilled.

Two parts that share a number of copies of bi-partite systems (that can be pure or mixed never maximal entanglement) for the purification protocol of a mixed state use quantum local operators and classical communication (2 - LOCC).

Let be H_A and H_B two Hilbert spaces and $\Psi \in H_A \otimes H_B$ - a vector.

A density matrix ρ acting over $H_A \otimes H_B$ is considered 1 - *distilled* if and only if there is a number $k \in \mathbf{N}$ (Schmidt coefficients) and the state $|\Psi\rangle \in H_S \subset (H_A \otimes H_B)$, where H_S is a $2x2$- dimensional Hilbert space, so that:

$$\langle\Psi|T_A(\rho)|\Psi\rangle < 0$$

and ρ - is considered n - *distilled* if and only if $\rho^{\otimes n}$ - is 1 - distilled.

If ρ is distilled for some integer $n \geq 1$, then ρ is distilled, otherwise it isn't distilled.

In general, it is difficult to distill a mixed state in exactly the number of Bell states used to its production. In EPR protocol, two parties, Alice and Bob start with a bi-partite state ρ_M consists of n pairs.

The protocol consists of repeated application of the following actions by the two parties.

1. Application of local unitary transformations (LUT)

2. Realize local measurements

3. The results of measurements determines the next step. During this process, some of the common particles are disposed, and the others are brought progressively closer to the desired state, such as a smaller number of Bell pairs than the number of the original particles shared.

N-pairs qubit distillation

Suppose we have a pair of non-maximally mixed state. The two pairs are the same state:

$$|\Psi\rangle^{\otimes 2} = (\alpha|0\rangle_a|0\rangle_b + \beta|1\rangle_a|1\rangle_b)(\alpha|0\rangle_{a'}|0\rangle_{b'} + \beta|1\rangle_{a'}|1\rangle_{b'})$$

with $|a| \leq |b|$.

The state can be described as:

$$|\Psi\rangle^{\otimes 2} = \alpha^2|0\rangle_a|0\rangle_{a'}|0\rangle_b|0\rangle_{b'} + \beta^2|1\rangle_a|1\rangle_{a'}|1\rangle_b|1\rangle_{b'} +$$

$$\sqrt{2}\alpha\beta\left(\frac{|0\rangle_a|0\rangle_{a'}|0\rangle_b|0\rangle_{b'} + |1\rangle_a|1\rangle_{a'}|1\rangle_b|1\rangle_{b'}}{\sqrt{2}}\right)$$

If Alice measures her particles a and $a^{'}$ using the operator $\sigma_T = \sigma_z^a + \sigma_z^{a^{'}}$, she can obtain three possible results.

$$|\Psi\rangle^{\otimes 2} \quad \underrightarrow{\sigma_T = 2} \quad |0\rangle_a|0\rangle_{a'}|0\rangle_b|0\rangle_{b'}$$

$$|\Psi\rangle^{\otimes 2} \quad \underrightarrow{\sigma_T = -2} \quad |1\rangle_a|1\rangle_{a'}|1\rangle_b|1\rangle_{b'}$$

$$|\Psi\rangle^{\otimes 2} \quad \underrightarrow{\sigma_T = 0} \quad \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_{a'}|0\rangle_b|1\rangle_{b'} + |1\rangle_a|0\rangle_{a'}|1\rangle_b|0\rangle_{b'})$$

where, in first case, that it is the most important, the probability is:

$$prob(\sigma_T = 0) = 2|\alpha\beta|^2$$

If the original state $|\Psi\rangle^{\otimes 2}$ collapses in this state, then we have almost a pure state.

Alice and Bob will perform a local operation $C-NOT$ on particles that have each, that particles $(a^{'}, b^{'})$ will be the target particles.

$$|\Psi\rangle^{\otimes 2} \quad \underrightarrow{\sigma_T = 0} \quad \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_{a'}|0\rangle_b|1\rangle_{b'} + |1\rangle_a|0\rangle_{a'}|1\rangle_b|0\rangle_{b'})$$

$$|\Psi\rangle^{\otimes 2} \quad \underrightarrow{C-NOT} \quad \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_{a'}|0\rangle_b|1\rangle_{b'} + |1\rangle_a|1\rangle_{a'}|1\rangle_b|1\rangle_{b'}) =$$

$$= \frac{1}{\sqrt{2}}|1\rangle_{a'}|1\rangle_{b'}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b)$$

It is noted that the two particles a and b are in an entanglement state.

Let's see de case of n - pair of qubits:

$$|\Psi\rangle^{\otimes n} = (\alpha|0\rangle_{a_i}|0\rangle_{b_i} + \beta|1\rangle_{a_i}|1\rangle_{b_i})^{\otimes n} =$$

$$= \alpha^n \prod_{i=1}^{n} |0\rangle_{a_i}|0\rangle_{b_i} + \alpha^{n-1}\beta \sum_{j=1}^{n}(|1\rangle_{a_i}|1\rangle_{b_i} \prod_{i\neq j}|0\rangle_{a_i}|0\rangle_{b_i}) + ...$$

it is the tensorial product of n-pair.

Similar, defines:

$$\sigma_T^a = \sum \sigma_{z_i}$$

When Alice measures σ_T^a will obtain a result $m-(n-m) = 2m-n$ with probability equal to that in 2-pairs case: $|\alpha^m\beta^{n-m}|^2$.

If $n \to \infty$, the probability will be maximum.

3.7 Communication using entangled states

In the following, we will discuss some ways that quantum interference can be used in the communication process. The phenomenon of quantum entanglement is characteristic only of quantum phenomena, so that none of the protocols that will be presented in this chapter have no equivalent in classical computing.

We consider two parties communicate generically called Alice and Bob. If Alice and Bob share a entangled state of qubits, they can send two bits of classical information using *dense coding* process.

The same phenomenon is used in *teleportation* an unknown state of a qubit.

Entanglement swapping (exchange of entangled states) can be used in a tripartite communication protocol (Alice-Bob-John), in which Alice and Bob share a entangled state, and Bob and John share a entangled states. Using *entanglement swapping* causes entanglement of states held by Alice and John. Each of these types of communication will be detailed in the following.

3.7.1 Bell states and Pauli operators

A quantum state $|\Psi_{AB}\rangle$ is a entangled state, if can not be expressed as a tensorial product of components of the states: $|\Psi_A\rangle \otimes |\Psi_B\rangle$. Bell states containing four orthogonal states entangled, that states to be used in protocols. Bell states are:

$$|\Phi^{\pm}_{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A 0^B\rangle \pm |1^A 1^B\rangle)$$
$$|\Psi^{\pm}_{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A 1^B\rangle \pm |1^A 0^B\rangle)$$

Can be used the Pauli operators:

$$\sigma_1 = |1\rangle\langle 0| + |0\rangle\langle 1|$$
$$\sigma_2 = i|1\rangle\langle 0| - i|0\rangle\langle 1|$$
$$\sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$$

You can apply one or more local Pauli operators, the effect being to flip from one state to another, between Bell states::

$$(\sigma_1 \otimes I) = |\Psi^{\pm}_{AB}\rangle$$
$$(\sigma_1 \otimes I) = |\Phi^{\pm}_{AB}\rangle$$
$$(\sigma_3 \otimes I) = |\Phi^{\mp}_{AB}\rangle$$
$$(\sigma_3 \otimes I) = |\Psi^{\mp}_{AB}\rangle$$

Effect of σ_2 operator is identical to that produced by the operators σ_1 and σ_3. If the state $|\Psi_{AB}\rangle$ is entangled, when detecting a state of the two, leading to a mixed state.

If $|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$ (non-entangled state) can be easily determined both Part A and Part B. In other words, $tr(\rho^2) = 1$ if and only if ρ is a pure state . There is a simple way to check whether or not a state is entangled.

A state is entangled if and only if:

$$tr(tr_A(|\Psi_{AB}\rangle\langle\Psi_{AB}|)^2) < 1$$

We can see that all Bell states are entangled.

$$tr(tr_B(|\Phi^{\pm}_{AB}\rangle\langle\Phi^{\pm}_{AB}|)^2) = tr(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|) = \frac{1}{4} + \frac{1}{4} < 1$$

3.7.2 Quantum dense coding

Quantum dense coding [69] is a communication protocol using the phenomenon of entanglement.

Using quantum dense coding, Alice can send Bob two bits of information using a qubit.

Initially Alice and Bob share the Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0^A 0^B\rangle + |1^A 1^B\rangle) \tag{3.13}$$

So Alice has two bits x and y, classical information, which wants to send to Bob. Alice and Bob have previously established unitary operators that Alice will use during the protocol.

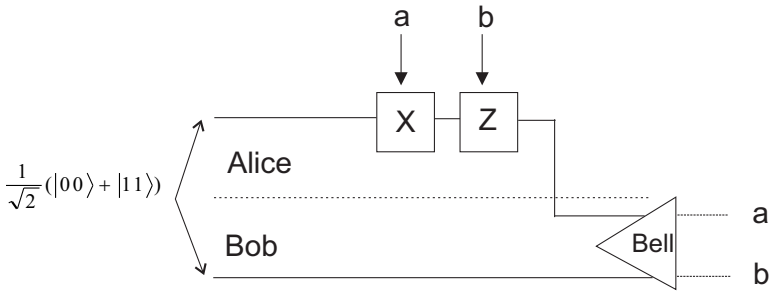


Figura 3.4: Quantum dense coding

Alice read the first bit of x. If $x = 0$, Alice will not do anything. If $x = 1$, Alice will perform an operation σ_1 (state-shift) on her qubit that transforms $|\Phi^+\rangle$ in:

$$(\sigma_1 \otimes I)|\Phi^+\rangle = |\Phi^+\rangle \tag{3.14}$$

Alice read the second bit y. If $y = 0$, Alice will not do anything. If $y = 1$, Alice will perform a phase-shift σ_3 on her qubit. Changing phase, transform $|\Phi^+\rangle$ and $|\Psi^+\rangle$ in:

$$(\sigma_3 \otimes I)|\Phi^+\rangle = |\Phi^-\rangle \tag{3.15}$$

and

$$(\sigma_3 \otimes I)|\Psi^+\rangle = |\Psi^-\rangle \tag{3.16}$$

Depending on the values of x and y, Alice and Bob share one of the four Bell states. Status is seen by Alice and Bob as a maximal entangled state.

$$tr_A|\Phi^\pm\rangle\langle\Phi^\pm| = tr_A|\Psi^\pm\rangle\langle\Psi^\pm| = tr_B|\Phi^\pm\rangle\langle\Phi^\pm| = tr_B|\Psi^\pm\rangle\langle\Psi^\pm| =$$

$$= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{3.17}$$

Alice and Bob can not deduce by measurement its own system that the Bell states shared it. However, Alice can send her qubit to Bob, so Bob will hold one of the four orthogonal Bell states, which can measure and then deduce the values of x and y.

It is used by Alice using Pauli operators to change the qubit states sent by Alice to Bob in one of the four Bell states.

3.7.3 Quantum teleportation

Teleportation [69] is one of the most beautiful application of quantum entanglement that seeks transmission of quantum information from Alice to Bob. Qubits that Alice wants to send Bob has an unknown state:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{3.18}$$

We say that a state is unknown because it is not necessary to know the values of α and β, but the state is normalized to satisfy the condition: $|\alpha|^2 + |\beta|^2 = 1$.

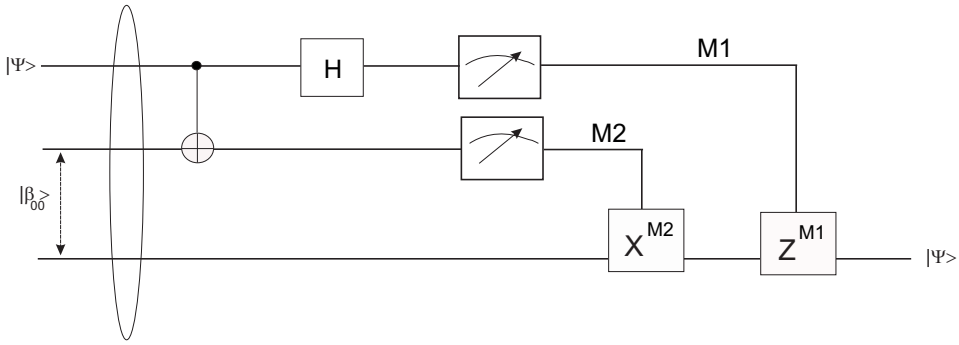


Figura 3.5: Quantum teleportation scheme

In what follows, I will explain step by step how it looks the quantum teleportation.

Step 1. Alice and Bob share an entangled pair of qubits.

Alice and Bob create an entangled state:

$$|\beta_{00}\rangle = \frac{(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle)}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.19}$$

We establish that the first member of the pair will remain in possession of Alice and the second in Bob possession.

Alice decides to send the state 3.18 to Bob. She will make that qubit with state the state 3.18 to interact with one of members's pair 3.19. How?

Step 2. Alice applies *C-NOT* gate. System's state is:

$$|\Psi\rangle = |\Psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\frac{|00\rangle + |11\rangle}{\sqrt{2}}) =$$

$$= \frac{\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)}{\sqrt{2}} \tag{3.20}$$

The first two qubits of this state belong to Alice, and the third belongs to Bob. Alice applies C-NOT gate between the second qubit of her own the EPR pair and qubit with state (3.18). The qubit with state (3.18) will be used as control-qubit and qubit of the EPR pair as target-qubit.

State is:

$$|\Psi'\rangle = CNOT|\Psi\rangle =$$

$$= \frac{\alpha(U_{CNOT}|000\rangle + U_{CNOT}|011\rangle) + \beta(U_{CNOT}|100\rangle + U_{CNOT}|111\rangle)}{\sqrt{2}} =$$

$$= \frac{\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)}{\sqrt{2}} \tag{3.21}$$

Pasul 3. Alice applies *Hadamard gate*.

Next, Alice will apply Hadamard gate on the first qubit. Hadamard gate transforms a state into a superposition of states:

$$H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Hadamard gate acting on the state (3.21) as follows:

$$|\Psi'\rangle = \frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}} \tag{3.22}$$

Alice transforms this state into:

$$|\Psi''\rangle = \frac{\alpha H|0\rangle(|00\rangle + |11\rangle) + \beta H|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}} =$$

$$= \alpha\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}\frac{(|00\rangle + |11\rangle)}{\sqrt{2}} + \beta\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\frac{(|10\rangle + |01\rangle)}{\sqrt{2}} \tag{3.23}$$

Do not forget, the third qubit is in Bob's possession.

Step 4. Alice measures the pair of qubits in his possession.

To highlight Alice's qubits, we rewrite the state (3.23) as follows:

$$|\Psi''\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle +$$

$$+|11\rangle(\alpha|1\rangle - \beta|0\rangle)] \tag{3.24}$$

If Alice measures $|00\rangle$, then the state collapses and Bob will have $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, exactly the state that Alice wanted to send it to Bob.

If Alice measures $|01\rangle$, then to obtain the qubit state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, Bob will have to apply a X gate over his qubit:

$$X(\alpha|1\rangle + \beta|0\rangle) = \alpha X|1\rangle + \beta X|0\rangle = \alpha|0\rangle + \beta|1\rangle = |\Psi\rangle$$

If Alice measures $|10\rangle$, then, to have the qubit's state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, Bob will have to apply a Z gate on his qubit:

$$Z(\alpha|0\rangle - \beta|1\rangle) = \alpha Z|0\rangle - \beta Z|1\rangle = \alpha|0\rangle + \beta|1\rangle = |\Psi\rangle$$

If Alice measures $|11\rangle$, then, to have the qubit's state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, Bob will have to apply the Z and X on his qubit:

$$ZX(\alpha|1\rangle - \beta|0\rangle) = \alpha ZX|1\rangle - \beta ZX|0\rangle = \alpha|0\rangle + \beta|1\rangle = |\Psi\rangle$$

Step 5. Alice send to Bob his measurement result using a classical communication channel.

At this point of the protocol, Alice needs to communicate its result to Bob, and for this she must use a classical communication channel.

It is important to note that communication is characterized by two aspects, namely, the application of local operators and classical communication (LOCC-Local Operations and Classical Communications). Each of these issues has the following purposes:

a. apply a local (unitary) operators on previous state

b. using a classical communication device (telephone, email, fax, radio, etc) to communicate results.

If not used a classical communication, and Bob will not get the necessary information, then he will be considered as a result a random state.

3.7.4 Communication using quantum entanglement swapping

Quantum entanglement swapping [108] is a phenomenon by which two or several qubits which did not interact in the past are brought in an entangled state.

The communication process that is based on this phenomenon is as follows:

Alice and Bob, each, have two qubits. Labelling the qubits with $1,2,3$ and 4. Alice has qubits 1 and 2, and Bob 3 and 4. Qubits 1 and 2 are prepared in Bell state:

$$|\beta_{00}\rangle_{12} = \frac{|00\rangle_{12} + |11\rangle_{12}}{\sqrt{2}} \tag{3.25}$$

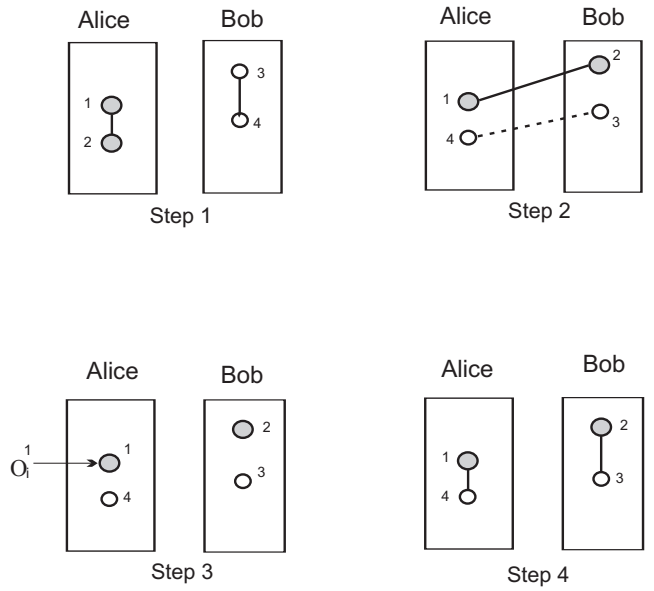


Figura 3.6: Entanglement swapping - scheme

Similar, qubits 3 and 4 are prepared in Bell state:

$$|\beta_{00}\rangle_{34} = \frac{|00\rangle_{34} + |11\rangle_{34}}{\sqrt{2}} \tag{3.26}$$

The product of states is:

$$|\beta_{00}\rangle_{12}|\beta_{00}\rangle_{34} = (\frac{|00\rangle_{12} + |11\rangle_{12}}{\sqrt{2}})(\frac{|00\rangle_{34} + |11\rangle_{34}}{\sqrt{2}}) =$$

$$= \frac{1}{2}(|00\rangle_{12}|00\rangle_{34} + |00\rangle_{12}|11\rangle_{34} + |11\rangle_{12}|00\rangle_{34} + |11\rangle_{12}|11\rangle_{34}) \tag{3.27}$$

Alice and Bob exchange qubits, so that Alice will have 1 and 4 qubits, and, Bob 2 and 3.

We rewrite the state (3.27) rearranging terms so that we can have together qubits 1 and 4, respectively, 2 and 3.

$$|\beta_{00}\rangle_{12}|\beta_{00}\rangle_{34} = \frac{1}{2}(|00\rangle_{14}|00\rangle_{23} + |01\rangle_{14}|01\rangle_{23} + |10\rangle_{14}|10\rangle_{23} + |11\rangle_{14}|11\rangle_{23}) \tag{3.28}$$

But:

$$|\beta_{00}\rangle_{14}|\beta_{00}\rangle_{23} = (\frac{|00\rangle_{14} + |11\rangle_{14}}{\sqrt{2}})(\frac{|00\rangle_{23} + |11\rangle_{23}}{\sqrt{2}}) =$$

$$= \frac{1}{2}(|00\rangle_{14}|00\rangle_{23} + |00\rangle_{14}|11\rangle_{23} + |11\rangle_{14}|00\rangle_{23} + |11\rangle_{14}|11\rangle_{23}) \tag{3.29}$$

Write product states as follows:

$$|\beta_{00}\rangle_{12}|\beta_{00}\rangle_{34} = \frac{1}{2}(|00\rangle_{14}|00\rangle_{23} + |01\rangle_{14}|01\rangle_{23} + |10\rangle_{14}|10\rangle_{23} + |11\rangle_{14}|11\rangle_{23} +$$

$$+|00\rangle_{14}|00\rangle_{23} + |11\rangle_{14}|00\rangle_{23} - |00\rangle_{14}|11\rangle_{23} - |11\rangle_{14}|00\rangle_{23}) =$$

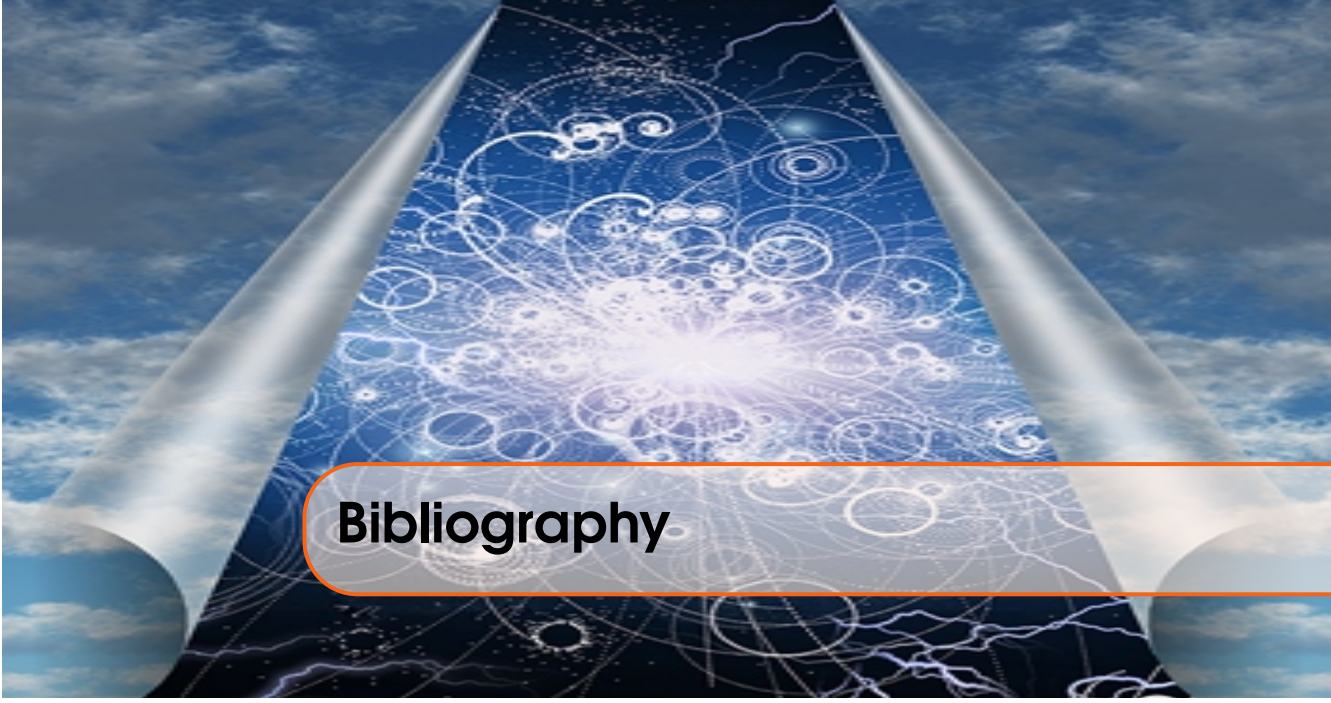
$$= \frac{1}{2}|\beta_{00}\rangle_{14}|\beta_{00}\rangle_{23} + |01\rangle_{14}|01\rangle_{23} + |10\rangle_{14}|10\rangle_{23} - |00\rangle_{14}|11\rangle_{34} - |11\rangle_{14}|00\rangle_{34}$$

At the end, we obtain:

$$|\beta_{00}\rangle_{12}|\beta_{00}\rangle_{34} = \frac{1}{2}(|\beta_{00}\rangle_{14}|\beta_{00}\rangle_{23} + |\beta_{10}\rangle_{14}|\beta_{10}\rangle_{23} + |\beta_{01}\rangle_{14}|\beta_{01}\rangle_{23} +$$

$$+|\beta_{11}\rangle_{14}|\beta_{11}\rangle_{23}$$

As we know, Alice possesses qubits 1 and 4. This provides a measurement of the Bell state of the pair $(1,4)$. Possible outcomes are $|\beta_{00}\rangle_{14}$, $|\beta_{10}\rangle_{14}$, $|\beta_{01}\rangle_{14}$ and $|\beta_{11}\rangle_{14}$, each with probability $\frac{1}{4}$. Depending on the measurement result obtained by Alice, Bob's state collapses into one of the Bell states $|\beta_{00}\rangle_{23}$, $|\beta_{10}\rangle_{23}$, $|\beta_{01}\rangle_{23}$ or $|\beta_{11}\rangle_{23}$. Now particles 2 and 3 are entangled.



Bibliography

[1] Ardehali A., Chau H.F. and Lo H,K. Efficient Quantum Key Distribution *http://quant-ph/9803007*, 2008.

[2] Bandyopadhyay S. *Physical Review A 62*, 012308, 2000.

[3] Barenco A., Bennett C.H., Cleve R., DiVincenzo D.P., Margolus N., Shor P., Sleator T., Smolin J.A. and Weinfürter H. Elementary gates for quantum computation. *Physical Review A 52.*, pp.3457-3467, 1995.

[4] Barnett S.M. and Phoenix S.J.D. Information theoretic limits to quantum cryptography. *Physical Review A, 48*, pp.R5-R9, 1993.

[5] Barni M. and Bartolini F. Watermarking Systems Engineering - Enabling Digital Assets Security and Other Applications. *Marcel Dekker, Inc*, pp.485, ISBN 0-8247-4806-9, 2004.

[6] Bengtsson I. and Zyczkowski K. Geometry of Quantum States: An Introduction to Quantum Entanglement. *Cambridge University Press*, pp.479, ISBN 978-0-511-19174-9, 2006.

[7] Bennett C.H. Logical Reversibility of Computation. *IBM Journal of Research and Development, 6*, pp.525-532, 1973.

[8] Bennett C.H. and Brassard G. *Proceedings IEEE Int. Conference on Computers, Systems and Signal Processing*, IEEE, New York, 1984.

[9] Bennett C.H., Bessette F., Brassard G., Salvail L. and Smolin J. *Journal of Cryptology*, 5, 3, 1992. Preliminary version in Advances in Cryptology-Eurocrypt'90 Proceedings Springer Verlag, pp. 253-265, 1990.

[10] Bennett C.H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68, pp. 3121-3124, 1992.

[11] Bennett C.H., Brassard G., Crépeau C., Jozsa R., Peres A. and Wootters W.K. *Physical Review Letters 70*, 1895-1899, 1993.

[12] Bennett C.H., DiVincenzo D.P., Smolin J.A. and Wootters W.K. *Physical Review A*, 54, 3824, 1996.

[13] Bechmann-Pasquinucci H. and Peres A. Quantum Cryptography with 3-state systems. *Physical Review Letters 85*, 3313, 2000.

[14] Bernstein E. and Vazirani U. Quantum Complexity Theory. *SIAM Journal on Computing*, vol.26, pp.11-20, 1997.

[15] Biham E., Huttner B. and Mor T. *Physical Review Letters A*, 2651, 1996.

[16] Blakley G.R. *Proceedings of the American Federation of Information Processing*, pp.313-317, 1979.

[17] Bloch F. and Staub H. Fission Spectrum. *Los Alamos Scientific Lab*, 1943.

[18] Bloom J.A. et al. Copy Protection for DVD Video. *Proceedings of the IEEE vol.87, no.7*, 1999.

[19] Boneh D. and Shaw J. Collusion-Secure Fingerprinting for Digital Data. *Advances in Cryptology, Proceedings of CRYPTO '95*, vol.963 of Lecture Notes in Computer Science, Springer, pp.452-465, 1995.

[20] Boneh D. and Shaw J. Collusion-Secure Fingerprinting for Digital Data. *IEEE Transactions on Information Theory vol.44, no.5*, pp.1897-1905, 1998.

[21] Bruss D. and Macchiavello C. Optimal eavesdropping in cryptography with three-dimensional quantum states. *http://arxiv.org/abs/quant-ph/0106126v2*, 2002.

[22] Burlakov A.V., Chekhova M.V., Karabutova O.A., Klyshko D.N. and Kulik S.P. *Physical Review A*, 60, R4209, 1999.

[23] Büzek V. and Hillery M. *Physical Review A 54*, 1844, 1996.

[24] Calderbank A.R., Rains E.M., Shor P.W. and Sloane N.J.A. Quantum Error Correction and Orthogonal Geometry. *Physical Review Letters 78*, pp.405-408, 1997.

[25] Cerf J.N., Thomas D. and Gisin N. Cloning a qutrit. *http://quant-ph/pdf/0110*, 2001.

[26] Cleve R., Gottesman D. and Lo H.K. *Physical Review Letters 83*, 648, 1999.

[27] Cole E. Hiding in Plain Sight: Steganography and the Art of Covert Communication. *Wiley Publishing, Inc., Indianapolis, Indiana*, pp.363, ISBN 0-471-44449-9, 2003.

[28] Dirac P.A.M. A New Notation for Quantum Mechanics. *Proceedings of the Cambridge Philosophical Society, vol.35*, pp.416, 1939.

[29] Dirac P.A.M. The principles of quantum mechanics (Fourth Edition ed.). *Oxford University Press*, UK, ISBN: 0198520115, 1982.

[30] Deutsch D. The Structure of the Multiverse. *http://arXiv:quant-ph/0104033v1*, 2001.

[31] Deutsch D. Three connections between Everetts Interpretation and experiment. *Quantum concepts in space and time*, 1985.

[32] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society, London*, A400:97-117, 1985.

[33] Deutsch D. and Jozsa R. *Proceedings of the Royal Society, London*, A439, 553, 1992.

[34] Deutsch D., Ekert A., Jozsa R., Macchiavello C., Popescu S. and Sanpera A. *Physical Review Letters*, 77, 2818, 1996.

[35] Einstein A., Podolsky B. and Rosen N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review, vol.47*, pp.777 - 780, 1935.

[36] Ekert A.K. *Physical Review Letters*, 67, 661, 1991.

[37] Ekert A.K., Rarity J.G., Tapster P.R. and Palma G.M. Practical quantum cryptography based on two photon interferometry. *Physical Review Letters 69*, pp.1293-1295, 1992.

[38] Ekert A.K. Quantum cryptography based on Bell's theorem. *Physical Review Letters 67*, pp.661-663, 1991.

[39] Fan H., Imai H., Matsumoto K. and Wang X-B. Phase-covariant quantum cloning of qudits. *http://arxiv.org/abs/quant-ph/0205126*, 2002.

[40] Gottesman D. A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound. *Physical Review A 54*, 1996.

[41] Grover L.K. A fast quantum machanical algorithm for databases search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pp.212-219, Philadelphis, PA, 1996.

[42] Grover L.K. Quantum computers can search rapidly by using almost any transformation. *Physical Review Letters 80*, pp.4329-4332, 1998.

[43] Grudka A. and Wöjcik A. How to encode the states of two non-entangled qubits in one qutrit. *http://quant-ph/0303168*, 2003.

[44] Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathématiques, vol.17*, pp.240-246, 1893.

[45] Heisenberg W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik, 43*, pp.172-198, 1927.

[46] Hilbert D., Nordheim L. and von Neumann J. Über die Grundlagen der Quantenmechanik. *Mathematische Annalen 98*, pp.1–30, 1927

[47] Hillery M., Büzek V. and Berthiaume A. *Physical Review A 59*, 1829, 1999.

[48] Hsu L.Y. *Physical Review A 68*, 022306, 2003.

[49] Imai H. and Hayashi M. Quantum Computation and Information - From Theory to Experiment. *Springer-Verlag*, pp.284, ISBN 3-540-33132-8, 2006.

[50] Imre S. and Bálazs F. Quantum Computing and Communications - An Engineering Approach. *John Wiley and Sons Ltd*, pp.316, ISBN 0-470-86902-X, 2005.

[51] Ivanovic I.D. *Journal of Physics A: Mathematical and General*, 14, 3241, 1981.

[52] Kalker T. Considerations on watermarking security. *Proceedings MMSP*, pp.201-206, 2001.

[53] Kuchment P. Quantum graphs: an introduction and a brief survey. *Analysis on Graphs and its Applications", Proc. Symp. Pure. Math., AMS 2008*, pp.291-314, 2008.

[54] Kutter M. and Petitcolas F.A.P. Fair Benchmarking for Image Watermarking Systems. *Proceedings of the SPIE 3657, Security and Watermarking of Multimedia Contents*, pp.226-239, 1999.

[55] Laflamme R., Miquel C., Paz J.P. and Zürek W.H. Perfect Quantum Error Correction Code. *http://arXiv:quant-ph/9602019v1*, 1996.

[56] Lance A.M., Symul T., Bowen W.P., Sanders B.C. and Lam P.K. *Physical Review Letters*, 92, 177903, 2004.

[57] Lanyon B.P., Weinhold T.J., Langford N.K., O'Brien J.L., Resch K.J., Gilchrist A. and White A.G. Manipulating Biphotonic Qutrits. *Physical Review Letters 100*, 060504, 2008.

[58] Linnartz J.P.M.G. The "TicketÇoncept for Copy Control Based on Embedded Signalling. *Computer Security-5th European Symposium on Research in Computer Security*, vol.1485 of Lecture Notes in Computer Science, Springer, pp.257-274, 1998.

[59] Liu X.S., Long G.L., Tong D.M. and Li F. *Physical Review A*, 65, 022304, 2002.

[60] Lo H.K. and Chau H.F. Quantum Cryptographic System with Reduced Data Loss *US patent No.5732139*, granted March 24, 1998.

[61] Lo H.K. and Chau H.F. *Science*, 283, 2050, 1999.

[62] Mayers D. *Journal of ACM* 48, 351, 2001.

[63] Melikidze A., Dobrovitski V.V., De Raedt H.A., Katsnelson M.I. and Harmon B.N. Parity effects in spin decoherence. *Physical Review B 70*, 014435, 2004.

[64] Monroe C., Meekhof D.M., King B.E., Itano W.M. and Wineland D.J. Demonstration of a Fundamental Quantum Logic Gate. *Physical Review Letters 75*, pp.4714-4717, 1995.

[65] Muller A., Breguet J. and Gisin N. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1km. *Europhysics Letters, vol.23 no.6*, pp.383-388, 1993.

[66] Mütze U. Quantum Image Dynamics - an entertainment application of separated quantum dynamics. *www.ma.utexas.edu/mp arc/c/08/08-199.pdf*, 2008.

[67] Neumann von J. Mathematical Foundations of Quantum Mechanics. *Princeton University Press*, 1955.

[68] Nielsen M.A. and Chuang I.L. *Quantum Computation and Quantum Information*, UK, 2000.

[69] Nielsen M.A. and Chuang I.L. Quantum Computation and Quantum Information. *Cambridge University Press*, ISBN 0-521-63235-8, 2000.

[70] Papanikolaou N.K. Techniques For Design And Validation Of Quantum Protocols. *University of Warwick*, 2004.

[71] Parthasarathy K.R. Lectures on Quantum Computation and Quantum Error Correcting Codes. *Indian Statistical Institute, Delhi Center*, 2001.

[72] Petitcolas F.A.P., Andreson R.J. and Kuhn M.G. Information Hiding - A Survey *Proceedings of IEEE*, pp. 1062-1078, July, 1999.

[73] Petz D. Quantum Information Theory and Quantum Statistics - Theoretical and Mathematical Physics. *Springer-Verlag*, pp.219, ISBN 978-3-540-74634-8, 2008.

[74] Preskill J. Lecture Notes for Physics 229: Quantum Information and Computation. *CIT*, 1998.

[75] Prugovećki E. Quantum mechanics in Hilbert space. *Academic Press*, pp.334, ISBN 75-117639, 1971.

[76] Rarity J.G., Owens P.C.M. and Tapster P.R. Quantum random number generation and key sharing. *Journal of Modern Optics*, 1993.

[77] Reid K.B. and Brown E. Doubly regular tournaments are equivalent to skew Hadamard matrices. *Journal of Combinatorial Theory A 12*, pp.332-338, 1972.

[78] Scheck F. Quantum physics. *Springer-Verlag*, pp.741, ISBN 978-3-540-25645-8, 2007.

[79] Schneider M. and Chang S.F. A Robust Content Based Digital Signature for Image Authentication. *Proceedings IEEE International Conference on Image Processing 1996*, Lausanne, Switzerland, 1996.

[80] Schrödinger E. An Undulatory Theory of the Mechanics of Atoms and Molecules. *Physical Review 28*, pp.1049–1070, 1926.

[81] Schrödinger E. Über das Verhaltnis der Heisenberg-Born-Jordanschen Quantenmechanik zu der meinen. *Annalen der Physik*, Leipzig, 1926.

[82] Schumacher B. Quantum coding. *Physical Review A 51*, pp.2738-2747, 1995.

[83] Seevinck M. and Svetlichny G. *Physical Review Letters 89*, 060401, 2002.

[84] Sencar H.T., Ramkumar M. and Akansu A.N. Data Hiding Fundamentals and Applications. *Elsevier Academic Press*, pp.269, ISBN 0-12-047144-2, 2004.

[85] Sergienko A.V. Quantum communications and cryptography. *CRC Press, Taylor and Francis Group*, pp.249, ISBN 0-8493-3684-8, 2006.

[86] Shamir A. *Communications of the ACM*, 22, 612, 1979.

[87] C. E. Shannon. *A Mathematical Theory of Communication*, 1948.

[88] Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, 1994.

[89] Shor P.W. Scheme for reducing decoherence in quantum computer memory. *Physical Review A 52*, R2493 - R2496, 1995.

[90] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing 26*, 1484, 1997.

[91] Shor P. and Preskill J. *Physical Review Letters*, 85, 441, 2000.

[92] Simon D.R. On the power of quantum computation. *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science*, IEEE Press, pp.116-123, 1994.

[93] Simmons G.J. The Prisoners' Problem and the Subliminal Channel. *Advances in Cryptology, Proceedings of CRYPTO '83, Plenum Press*, pp. 51-67, 1984.

[94] Stoke J.and Suter D. Quantum Computing - A Short Course from Theory to Experiment. *Wiley-VCH Verlag GmbH and Co. KGaA*, pp.246, ISBN 3-527-40438-4, 2004.

[95] Toffoli T. Reversible Computing. *Technical Report MIT/LCS/TM-151*, 1980.

[96] Townsend P.D., Rarity J.G. and Tapster P.R. Single photon interference in a 10 km long optical fibre interferometer. *Electronics Letters vol.29 no.7*, pp.634-635, 1993.

[97] Townsend P.D., Rarity J.G. and Tapster P.R. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel. *Electronics Letters vol.29 no.14*, pp.1291-1293, 1993.

[98] Towsend P.D. *Nature*, 385, 47, 1997.

[99] Uffink J. *International Journal of Theoretical Physics. 33*, 199, 1994.

[100] Vedral V. Introduction to Quantum Information Science. *Oxford University Press*, pp.177, ISBN 0-19-9215707, 2006.

[101] Werner R.F. *Physical Review A 40*, 4277, 1989.

[102] Wiesner S. Conjugate coding. *Sigact News 15*, pp.78-79, 1983. original manuscript written circa 1970.

[103] Wootters W.K. *Foundations of Physics*, 16, 391, 1986.

[104] Wootters W.K. and Zürek W.H. A Single Quantum Cannot be Cloned. *Nature 299*, pp.802-803, 1982.

[105] Xiao L., Long G.L., Deng F.G. and Pan J.W. Efficient Multi-Party Quantum Secret Sharing Schemes. *Physical Review A 69*, 052307, 2004.

[106] Xie L. and Arce G.R. A Blind Wavelet Based Digital Signature for Image Authentication. *Proceedings of the European Signal Processing Conference*, Rhodes, Greece, 1998.

[107] Zizzi P.A. Holography, Quantum Geometry and Quantum Information Theory *The 8th UK Foundations of Physics Meeting*, 13-17 September, London, UK, 1999.

[108] Zukowski M., Horne M., and Ekert A.K. Event-Ready-Detectors"Bell State Measurement via Entanglement Swapping. *Phys. Rev. Lett. 71*, pp.4287, 1993.

"You have to learn the rules of the game.
And then you have to play better than anyone else."

Albert Einstein

ISBN: 978-9942-21-517-8

This work was financed by the Prometeo Project of the Ministry of Education Superior, Science, Technology and Innovation of the Republic of Ecuador.

QUANTUM COMPUTING AND COMMUNICATION
GABRIELA MOGOS