FUNDAMENTALS OF INFORMATION AND COMPUTATION IN THE REALM OF THE QUANTA

Por

John H. Reina*+

Resumen

Reina J. H.: Fundamentals of information and computation in the realm of the quanta. Rev. Acad. Colomb. Cienc. **33**(127): 201-242, 2009. ISSN 0370-3908.

La información es un ente físico. Los sistemas físicos registran y procesan información. El reconocimiento de estos hechos desde el punto de vista de la teoría de información y su relación directa con aplicaciones a nuevas tecnologías cuánticas ha sido crucial en el desarrollo reciente la física tanto básica como aplicada, al mismo tiempo que de otras áreas tales como ciencias de la computación, matemáticas e ingenierías, donde el reto de construir dispositivos que permitan el procesamiento de información a nivel cuántico es objetivo primordial. En los trabajos de Deutsch (**Deutsch,** 1985) y Shor (**Shor,** 1994), la noción de *bit* clásico de la teoría de información fue conceptualmente extendida a un marco físico radicalmente diferente con la introducción del *bit cuántico*, donde fue demostrado que los efectos de interferencia cuántica de muchas partículas pueden permitir una forma nueva y fundamental de cómputo, donde es posible la ejecución de tareas computacionales irresolubles tales como la factorización de números primos muy grandes o la simulación exacta de sistemas cuánticos multipartitos. Así, la investigación en física de la información y cómputo cuántico se ha convertido en un foco de desarrollo básico de la fenomenología cuántica, análisis y revisión del cual se presenta en este trabajo.

Empezamos con la definición formal de qubit, registrador cuántico, y de conjunto universal de compuertas lógicas empleado en la construcción de un computador cuántico, desde la perspectiva de un modelo de computación de red cuántica. A partir de este, se enfatiza en la versatilidad de la representación de circuito cuántico para *intrincar* y *desintrincar* estados cuánticos. De aquí se introduce el "teorema de no clonación" y sus aplicaciones a criptografía cuántica. Se describen dos alternativas a la formulación 'tradicional' o usual de cómputo cuántico: i) computación cuántica geométrica, y ii) computación cuántica unidireccional. Se realiza la caracterización, y cuantificación de intrincamiento cuántico, en particular de sus usos como *recurso* físico en protocolos de comunicación cuántica tales como teleportación, criptografía, codificación superdensa, y compresión de datos. Se introduce el concepto de paralelismo cuántico de Deutsch y se analiza su aplicación a la resolución eficiente de tareas algorítmicas irresolubles clásicamente. La decoherencia cuántica se introduce como proceso inherente y central en el procesamiento de información cuántica. Se plantean mecanismos para corregirla o evitarla, en particular, se analiza en detalle el proceso de corrección de errores cuánticos. Finalmente, se desciben algunas de las implementaciones físicas de cómputo y comunicación cuántica, y de la forma como un qubit puede ser representado físicamente en una gran variedad de nanosistemas.

* Profesor Asistente, Facultad de Ciencias Naturales y Exactas, Departamento de Física. Universidad del Valle, A.A. 25360, Cali.

+ Electronic address: jhreina@univalle.edu.co

Palabras clave: Computación e información cuántica, intrincamiento cuántico, comunicación, algoritmos, decoherencia cuántica, corrección de errores cuánticos, qubits y nanosistemas.

Abstract

Information is physical. Physical systems register and process information. These facts have generated enormous interest in the development of novel quantum technologies, especially because the construction of smaller electronic devices ultimately leads to a consideration of quantum mechanical effects in electronic and computer designs. The notion of the classical *bit* of information theory was formally pushed into the realm of the quanta with the introduction of the quantum bit or *qubit*, in the seminal works of Deutsch (**Deutsch,** 1985) and Shor (**Shor,** 1994). They demonstrated that, indeed, controlled multipartite qubit interference effects could provide the means for a radical new way of computing, allowing the computation of many intractable computational problems, such as the factoring of large numbers or the exact simulation of large quantum systems. The field of experimental and theoretical research in quantum information and computation has emerged as a very important player in the understanding of quantum phenomena at both the basic and technological levels. This has attracted the attention of numerous reasearchers with backgrounds ranging from computer science, mathematics and engineering, to the physical sciences, and we now have an interdisciplinary field where great efforts are being made in order to build devices that allow the processing of information at a quantum level.

A concise introduction to the field of quantum information and quantum computation is presented. This starts with the basic definitions of bits, quantum registers, through to the universal gate-set for building the universal quantum computer, from a quantum network model of computation. The work shows how two-qubit gates suffice for quantum computation, emphasing the power of the quantum circuit representation for *entangling* and *disentangling* quantum states. This leads to the "no-cloning theorem," which leads us to many interesting applications, such as quantum cryptography. Two alternative approaches for performing quantum computation are also described: i) the one-way or measurement based quantum computer method, and ii) holonomic or geometric quantum computation. Following this, quantum entanglement quantification is highlighted, particularly its usefulness as a communication resource, in order to describe some of its most celebrated practical applications to date: quantum teleportation, cryptography, dense coding, and data compression. Deutsch's concept of quantum parallelism is emphasized in order to gain insight into the potential for efficiently solving certain classically intractable algorithms. A subject central to the field of QIP - quantum decoherence - is then introduced. Possible ways to overcome it, in particular quantum error correction, are discussed. A description of some of the currently available hardware for the practical implementation of quantum computation is provided with a discussion of the main physical quantum bits that are currently employed (or proposed) for such a purpose.

Keywords: Quantum computation, entanglement, communication, algorithms, decoherence, error correction, qubits, and nanostructures.

Contents

I. INTRODUCTION

The ways in which quantum theory can tell us about nature have been the subject of long periods of debate throughout its history since its foundation, a century ago (**d'Espagnat,** 1976; **Mermin,** 1985; **Peres,** 1993). Some of the very same issues that revealed most of the 'difficulties' (**Einstein *et al.*,** 1935; **Schrödinger,** 1935) of this theory have come to be of great practical use for technological purposes in the emerging field of quantum information processing (QIP) (**Bennett & DiVincenzo,** 2000; **Steane,** 1998; **Bennett,** 1995)[1].

In 1935, Einstein, Podolsky, and Rosen (EPR) (**Einstein *et al.*,** 1935), and Schrödinger (**Schrödinger,** 1935) pointed out that one such aspect of quantum theory is the phenomenon of *entanglement*. By means of predictions associated with an entangled (EPR-pair) state, EPR argued that quantum mechanics is an 'incomplete' physical theory because of the violation of "local realism," a description of the world where the physical properties of spatially separated subsystems of a composite system are characterised by an 'independent' and 'objective reality.' This was the subject of many fundamental discussions concerning the basic structure of quantum theory. This conflict had to wait for almost 30 years for its resolution, when Bell reported, in his celebrated 1964 paper (**Bell,** 1964; **Bell,** 1987), that this local realism leads to constraints on the predictions of spin correlations (Bell's inequalities), which can be *violated* by quantum theory for a system in the singlet (Bell) state $|\uparrow\rangle\,|\downarrow\rangle - |\downarrow\rangle\,|\uparrow\rangle$, being $|\uparrow\rangle$ ($|\downarrow\rangle$) a particle's spin "up" ("down") state along a given axis (**Peres,** 1993). After this breakthrough, several experiments (**Aspect *et al.*,** 1982; **Selleri,** 1989; **Tittel *et al.*,** 1998; **Weihs *et al.*,** 1998) were performed in support of Bell's findings. This feature—*nonlocality*—reveals quantum entanglement at its best, an outstanding phenomenon of quantum physics. As we shall see below, quantum entanglement has led to several important practical applications for QIP, where it has been recognised as a valuable *resource* for communication at both classical and quantum levels.

After these theoretical developments, there was a further long period until we arrived to the point which settled the foundations of the field of quantum information processing. It was realised that quantum mechanical principles are not just exotic theoretical statements but fundamental for a new technology of practical information processing. This is based on the ideas of Feynman (**Feynman,** 1982; **Feynman,** 1985) and Benioff (**Benioff,** 1982(A); **Benioff,** 1982(B)) presented in 1982, and a few years later, in 1985, by Deutsch (**Deutsch,** 1985). These findings have developed in concrete practical applications: quantum computation (**Feynman,** 1982; **Feynman,** 1985; **Benioff,** 1982(A); **Benioff,** 1982(B); **Deutsch,** 1985), quantum cryptography (**Ekert,** 1991; **Bennett *et al.*,** 1992(A); **Bennett *et al.*,** 1992(B)), quantum teleportation (**Bennett *et al.*,** 1993), quantum dense coding (**Bennett & Wiesner,** 1992; **Barenco & Ekert,** 1995), and quantum games (**Meyer,** 1999; **Meyer,** 2000; **Eisert *et al.*,** 1999; **Eisert & Wilkens,** 2000; **Benjamin & Hayden,** 2001(A); **Benjamin & Hayden,** 2001(B)), all of which represent exciting new arenas in which to exploit such intrinsic quantum mechanical correlations.

The discovery of algorithms for which a computer based on the principles of quantum mechanics (**Deutsch & Jozsa,** 1992; **Simon,** 1994; **Shor,** 1994; **Shor,** 1997(A); **Grover,** 1997) should beat any modern digital computer has triggered intense research into realistic controllable quantum systems. Since the seminal idea of Feynman (**Feynman,** 1982; **Feynman,** 1985) and Benioff (**Benioff,** 1982(A); **Benioff,** 1982(B)), and the work of Deutsch (**Deutsch,** 1985), both pure and applied research in the field of quantum information processing have blossomed. In 1994, Shor (**Shor,** 1994; **Shor,** 1997(A); **Ekert & Jozsa,** 1996; **Cleve *et al.*,** 1998) opened the way to new fast quantum searching algorithms: he discovered that a quantum computer can factorize large integers. Two years later the proof that quantum error-correcting codes exist arrived (**Shor,** 1995; **Shor,** 1997(B); **Steane,** 1996(A); **Steane,** 1996(B); **Steane,** 1996(C)).

Regarding the physical implementations of quantum computation and information, the main areas of research include ion traps (**Cirac & Zoller,** 1995; **Cirac & Zoller,** 2000; **Monroe *et al.*,** 1995; **Molmer *et al.*,** 1999; **Sackett *et al.*,** 2000; **Blatt & Wineland,** 2008), quantum electrodynamics cavities (**Pellizzari *et al.*,** 1995; **Turchete *et al.*,** 1995; **Cirac *et al.*,** 1996; **Cirac *et al.*,** 1997; **Imamoglu *et al.*,** 1999; **Rauschenbeutel *et al.*,** 1999; **Rauschenbeutel *et al.*,** 2001; **Greiner *et al.*,** 2002; **Leuenberger *et al.*,** 2005), nuclear magnetic resonance (**Gershenfeld & Chuang,** 1997; **Chuang *et al.*,** 1998(A); **Chuang *et al.*,** 1998(B); **Cory *et al.*,** 1997; **Knill *et al.*,** 1998; **Jones *et al.*,** 1998(A); **Jones & Mosca,** 1998(B); **Vandersypen *et al.*,** 2001;

[1] See also the special issue of Physics World, March (1998). Note that most of the literature in the field can be found at the Los Alamos National Laboratory e-print archive, http://xxx.lanl.gov/archive/quant-ph.

Kane, 1998), optical lattices and Bose-Einstein condensation (**Brennen *et al.*,** 1999; **Jacksch *et al.*,** 1999; **Greiner *et al.*,** 2002; **Mandel *et al.*,** 2003; **Giamarchi *et al.*,** 2008; **Bloch,** 2008), Josephson junctions (**Shnirman *et al.*,** 1997; **Makhlin *et al.*,** 1999; **Nakamura *et al.*,** 1999; **Averin,** 1998; **van der Wal *et al.*,** 2000; **Makhlin *et al.*,** 2001; **Clarke & Wilhelm,** 2008; **Montes *et al.*,** 2009), molecular magnets (**Leuenberger *et al.*,** 2001; **Leuenberger *et al.*,** 2002), nanotubes and fullerenes (**Ardavan *et al.*,** 2003), single molecule arrays (**Reina *et al.*,** 2004), graphene quantum dots (**Trauzettel *et al.*,** 2007), organic polymers (**Mujica *et al.*,** 2009), and quantum dots (**Barenco *et al.*,** 1995(B); **Loss & DiVincenzo,** 1999; **Burkard *et al.*,** 1999; **Reina *et al.*,** 2000(A); **Reina *et al.*,** 2000(B); **Quiroga & Johnson,** 1999; **Biolatti *et al.*,** 2000; **Troiani *et al.*,** 2000; **Lovett *et al.*,** 2003(A); **Lovett *et al.*,** 2003(B); **Nazir *et al.*,** 2005; **Fushman *et al.*,** 2008; **Robledo *et al.*,** 2008). This is, by no means, and extensive list and many more proposals and implementations can be found in the literature. This gives an idea of the broadness of the field and of the current experimental and theoretical activity.

All of the above proposals and/or implementations have decoherence and operational errors as the main obstacles for their experimental realisation: these, as we shall see throughout this work, pose much stronger problems here than in conventional digital computers. The main challenge we face in order to process information at a quantum level is to identify a physical system with an appropriate internal dynamics and corresponding external driving forces, which enables one to selectively manipulate quantum superpositions and entanglements. A fundamental requirement for the experimental realisation of such proposals is the successful generation of highly entangled quantum states. In particular, coherent evolution of two quantum bits (qubits) in an entangled state of the Bell type (**Bell,** 1987; **Bell,** 1964; **Aspect *et al.*,** 1982) is relevant to both quantum cryptography and quantum teleportation. Maximally entangled states of three qubits, such as the so-called GHZ states (**Greenberger *et al.*,** 1989; **Greenberger *et al.*,** 1990), are not only of intrinsic interest but are also of great practical importance in such proposals.

Besides the capability to control and manipulate entanglement, a high level of isolation from the environment is required to reach a full unitary evolution. Quantum information processing will be a reality when optimal control of quantum coherence in noisy environments can be achieved. The various communities typically rely on different hardware methodologies. It is therefore extremely important to clarify the underlying physics and limits for each type of physical realisation of QIP systems. This work aims to give a basic introduction of the main results concerning the processing of information at a quantum level. It is *not* intended to provide a historical review of the development of classical information theory and computer science, and the way they were linked to fundamental aspects of quantum physics to give birth to the field of quantum information theory. Instead, the background and the necessary concepts of quantum computing and quantum information are presented to further establish the framework to some physical realizations such as those of the solid-state.

For the purpose of the implementations discussed in the final part of this work, the network model of computation is adopted. Here one can imagine a quantum computer (QC) as a physical device that takes an initial state (input) into some final state (output) via a set of quantum networks that evolves in a unitary fashion. Next, the methods to build such networks are presented.

II. FROM BINARY DIGITS TO UNIVERSAL QUANTUM COMPUTATION

A. Bits and quantum registers

A binary digit, or *bit*, is the basic unit of information in classical communication and information theory. This has only two possible states: 0 and 1 in the binary system generally used in digital computers (in a proper electromechanical device, this basis can be represented by an "on-off," or "open-closed," or "go-no go" states). The relevance of this base–2 representation to computer technology arises from the reliable compact manner in which data can be digitally stored. For example, the year 2002 (decimal system) can be written in binary system as 11111010010. At first glance, this number appears to be more compact in base–10 than in its binary equivalent; however, a physical representation of a four digit number in base 10 requires 10^4 states, while its binary representation 'only' requires $2^{11} = 2048$ states: it is clear that the binary system appears to be the most convenient one for the storage and processing of the information. Therefore, we shall hereafter assume that information is stored in registers in a binary form[2].

[2] A binary string can be represented in any base b as: $c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b^1 + c_0 b^0$, where c_i are 'place-value' coefficients. Usually, the number representing this expansion is written as $c_n c_{n-1} \cdots c_2 c_1 c_0$ (base b). For example, in the decimal system, the number 2002 is the compact way of writing $2 \times 10^3 + 0 \times 10^2 + 0 \times 10^1 + 2 \times 10^0$. Its binary equivalent is 11111010010, i.e., $1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$, while for the Mayans (vigesimal number system) this should read 502.

In contrast to the binary digit, or classical bit, the elementary unit for the processing of quantum information is the quantum bit or *qubit*, a term coined by Schumacher (**Schumacher,** 1995). In this case the Boolean states 0 and 1 are represented by a pair of normalised and orthogonal quantum states labelled as $\{|0\rangle, |1\rangle\}$ (**Schumacher,** 1995). These states form a 'computational basis', that we shall name the $\mathcal{B}_1$-basis, so that any other state of the qubit can be written as a linear superposition $\alpha\,|0\rangle+\beta\,|1\rangle$, with $|\alpha|^2+|\beta|^2=1$, $\alpha,\beta\in\mathbf{C}$. Typical examples of qubits are nuclei with spin 1/2, two-level atoms, polarised photons, etc.

A *quantum register* (QR) of size n, is a quantum system of n qubits with a 2^n dimensional Hilbert space, and hence with 2^n mutually orthogonal quantum states available, which can be written compactly as $\{|j\rangle\}$, where j is an n-bit binary number ($j=2^{n-1}j_{n-1}+2^{n-2}j_{n-2}+\cdots+2^1j_1+2^0j_0$, $j_m\in\{0,1\}$), and $|j\rangle$ denotes the tensor product $|j_{n-1}\rangle\otimes|j_{n-2}\rangle\cdots|j_1\rangle\otimes|j_0\rangle$, or $|j_{n-1}j_{n-2}\cdots j_1j_0\rangle$ for short. Though a qubit is a prescribed two-state system, it is fundamentally different from a classical bit. A given quantum physical system that serves for the storage, processing, and readout of a computational process by using a qubit has to deal with a microscopic system that is to be "switched *on* or *off*" by appropriately manipulating its interaction with an external driving source, bearing in mind its interaction with the other qubits of the system and also with the surrounding environment. This has an additional ingredient: the dynamics of a qubit is ruled by the principles of quantum physics. This means that while a binary string of n classical bits can store *only* one number at a given time, say

$$\underbrace{1}_{j_{n-1}}\underbrace{0}_{j_{n-2}}\underbrace{0}_{j_{n-3}}\cdots\underbrace{0}_{j_1}\underbrace{0}_{j_0}\ , \tag{1}$$

an n-quantum register can store a superposition of all of the 2^n mutually orthogonal quantum states $\{|j\rangle\}$ simultaneously: this is the computational power of quantum interference, which led to the so-called quantum parallelism (see below). To see this, we need to prepare the register in such a way that each qubit is in a superposition state, say $(|0\rangle+|1\rangle)/\sqrt{2}$. Hence we are left with a quantum register in the state

$$\tfrac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)_{j_{n-1}}\otimes\tfrac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)_{j_{n-2}}\otimes\cdots\otimes\tfrac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)_{j_0}$$

which in binary notation is the sum of 2^n quantum states $|j\rangle$,

$$\begin{aligned}\sum_{j\in\{0,1\}^n}|j\rangle \ &=\ |00\cdots00\rangle+|00\cdots01\rangle+|00\cdots10\rangle+\cdots+\\ &\quad |100\cdots00\rangle+\cdots+|11\cdots10\rangle+|11\cdots11\rangle,\end{aligned} \tag{2}$$

where the normalisation factor $2^{-n/2}$ has been omitted. Eq. (2) can be written in base-10 as

$$\begin{aligned}\frac{1}{\sqrt{2^n}}\Big\{\ &|0\rangle+|1\rangle+|2\rangle+|3\rangle+\cdots+\overbrace{|2^{n-1}\rangle}+\cdots\\ &+|2^n-1\rangle\Big\}\equiv\frac{1}{\sqrt{2^n}}\sum_{m=0}^{2^n-1}|m\rangle\ \ ,\end{aligned}$$

where the overbraced state is the quantum representation (in decimal notation) of the binary string represented by Eq. (1). Hence, it is clear that due to the quantum superposition principle, a quantum computer can, in principle, be prepared in a superposition of (and as we shall see below, can process) 2^n states in a given n-QR at once. Here, there is an important issue to be highlighted: a qubit is an extremely fragile physical system and its reliability to store and process information at will is going to be limited by the interactions that it might have with the environment that surrounds it—the problem of noise at a quantum level. This QR-environment coupling, known as *decoherence*, produces an undesirable effect over the register: it makes superpositions such as $|0\rangle+|1\rangle$ lose their phase, and therefore their ability to interfere reliably, which results in the destruction of the quantum computation. This can also be viewed as a loss of the unitarity of the quantum evolution of the QR, an essential requirement for quantum computation to occur.

B. Quantum logic and the universal quantum computer

Building blocks of a quantum computer are now introduced. As in the case of the processing of classical information in digital computers, logic gates and networks for the processing of quantum information (**Deutsch,** 1989) are introduced. A *quantum logic gate* is a device that performs a prescribed unitary operation on selected qubits in a definite time t and a *quantum network* is a device built of quantum logic gates whose computational steps are synchronised in time (**Deutsch,** 1989). Such quantum networks are to be represented by a circuit notation that accounts for the action of the logic gates. Here, a qubit is represented by a horizontal line—"wire"— that evolves in time from left to right, and single and two qubit gates are represented respectively by a prescribed symbol on one wire, and by symbols on two wires connected by a vertical line. The qubit associated with the filled dot is usually called the "control" (or source), and the other one is called the "target." An example is shown in the following network of *size* 4 (Fig. 1):

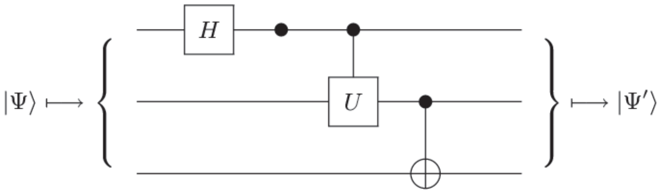


FIG. 1 A quantum network containing 4 gates. From left to right, the QR state $|\Psi\rangle$ experiences the action of the following quantum logic gates: i) Hadamard (H), ii) phase shift [$P(\varphi)$], iii) Controlled-U (U), and iv) controlled-NOT (CNOT or XOR). The network produces the final state "output" $|\Psi'\rangle \equiv XOR_{23}U_{12}P(\varphi)_1H_1\,|\Psi\rangle$. In this operational notation, the subscripts denote the qubits to be addressed, and in any two-qubit gate U_{ij}, i, and j denote the control and target bits respectively. Note that the first two unitary transformations are single qubit gates while the remaining ones are two qubit gates.

It turns out that *any* possible unitary transformation to be performed by a quantum computer can be simulated by an appropriate combination of the set of quantum logic gates shown in Fig. 1, i.e., by performing arbitrary single qubit rotations and two-qubit XOR (or U) gates. Thus, the sets of gates $\{P(\varphi), H, \text{XOR}\}$, and $\{P(\varphi), H, U\}$ are universal for quantum computation: *all logic gates* to be performed on a given quantum register can be constructed by composing the gates of either of these sets. These are the so-called *universal quantum logic gates* (**Deutsch,** 1989; **Deutsch *et al.*,** 1995; **Barenco,** 1995; **DiVincenzo,** 1995; **Lloyd,** 1995).

A quantum system capable of realising and manipulating at will a given set of universal quantum gates is said to perform *universal quantum computation.* Such a machine is the so-called universal quantum computer, a concept first introduced by Deutsch in 1985 (**Deutsch,** 1985; **Deutsch *et al.*,** 1995).

The main result to be emphasized here is that *two-qubit gates are sufficient for quantum computation.* As can be imagined, there are many combinations of gates that can be built to perform elementary 'quantum arithmetical operations' such as binary addition and multiplication. However, it is not the purpose of this section to describe in detail such quantum networks. Many basic constructions can be found in (**Barenco *et al.*,** 1995(A); **van der Wal *et al.*,** 2000). We are now ready to define the building blocks from which one can assemble a circuit that can evaluate any *arbitrary* Boolean function:

1. The *phase-shift gate* $P(\varphi)$ is a single qubit gate that performs the unitary operation $P(\varphi)(|m\rangle) \mapsto e^{im\varphi}\,|m\rangle$, where $m \in \{0,1\}$, or $P(\varphi) \equiv |0\rangle\langle 0| + e^{i\varphi}\,|1\rangle\langle 1|$.

2. The *Hadamard gate* H is also a single qubit gate that performs the unitary operation known as the Hadamard transform $H(|m\rangle) \mapsto \frac{1}{\sqrt{2}}[(-1)^m\,|m\rangle + |1-m\rangle]$, or $H \equiv \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]$. These gates are schematically represented in the language of quantum circuits as shown in Fig. 1. It is easy to show that by combining the set of transformations $\{P(\varphi), H\}$, any single qubit rotation can be generated. Hence, the Hadamard and the phase shift gates suffice to perform any unitary transformation on a single qubit.[3] Other relevant single qubit gates are the identity $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$; the quantum NOT gate, which in analogy with the classical NOT gate transforms $|0\rangle$ to $|1\rangle$ and vice versa: $\text{NOT} \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$; and the V-gate $V \equiv P(\pi/2)$.

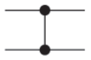
3. The *controlled-U* gate is a two-qubit gate that performs the operation $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$, where U is some prescribed single-qubit unitary transformation. This gate leaves the target qubit unchanged or applies the U gate depending on whether the control qubit is $|0\rangle$ or $|1\rangle$: $|0\rangle\,|m\rangle \mapsto |0\rangle\,(I\,|m\rangle)$, and $|1\rangle\,|m\rangle \mapsto |1\rangle\,(U\,|m\rangle)$. The network representation corresponding to this gate is shown in Fig. 1. This two-qubit gate comprises a general family of quantum gates, each of them, together with $P(\varphi)$, and H, being universal for quantum computation.

4. The *controlled*-NOT (CNOT or XOR) gate is an important example of a U gate[4]: it flips the target bit if the control bit is in the state $|1\rangle$ and acts trivially otherwise. This action can be formally written as: $\text{CNOT}(|j\rangle\,|m\rangle) \mapsto |j\rangle\,|j \oplus m\rangle$, where $j, m \in \{0,1\}$, and $\oplus$ denotes addition modulo 2 or XOR operation. This is why the symbol $\oplus$ is schematically used to represent such a gate, as seen in Fig. 1.

[3] To see this, compose the network $P(\varphi + \pi/2)\,H\,P(2\theta)\,H\,|m\rangle$, $m \in \{0,1\}$. This gives the most general rotation of a single qubit:

$$V(\theta,\varphi) \equiv e^{i\theta}\begin{pmatrix} \cos\theta & e^{i\varphi}\sin\theta \\ \sin\theta & e^{i\varphi}\cos\theta \end{pmatrix}. \qquad (3)$$

[4] Another common two-qubit gate is the controlled phase shift gate $B(\varphi)$, which performs the unitary transformation: $|m\rangle\,|n\rangle \mapsto e^{imn\varphi}\,|m\rangle\,|n\rangle$, $m, n \in \mathcal{B}_1$. In the language of networks, this gate is represented as

$|\Psi\rangle_{1,2} \mapsto \Big\{$  $\Big\} \mapsto |\Psi'\rangle_{1,2}$.

The CNOT gate is usually termed as a *measurement gate* due to the fact that it maps $|m\rangle_1 |0\rangle_2 \mapsto |m\rangle_1 |m\rangle_2$, i.e., if the purpose is to measure the final state of 'qubit 1,' then a measurement of the output state of 'qubit 2' reveals the answer. The advantage of this procedure over a direct measurement of qubit 1 is that it is a "non-demolition" measurement: the original quantum state of qubit 1 remains the same after the measurement. However, this is only valid if the qubit 1 is originally in one of the two states of the computational basis $\mathcal{B}_1 \equiv \{|0\rangle, |1\rangle\}$: if $|m\rangle_1$ is initially in a superposition of the states of this basis, then the state is "collapsed" by the measurement. This is because it is impossible to build a universal quantum "cloning machine" $|\Psi\rangle |0\rangle \mapsto |\Psi\rangle |\Psi\rangle$, with $|\Psi\rangle$ being the arbitrary superposition state $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$, $\alpha, \beta \neq 0$. This important result is known as the *no-cloning theorem* (**Wootters & Zurek,** 1982); see Appendix A. In fact, if we 'run' the CNOT$_{12}$ gate over the initial state $|\Psi\rangle_1 |0\rangle_2$, we transform $(\alpha|0\rangle + \beta|1\rangle)|0\rangle \mapsto \alpha|00\rangle + \beta|11\rangle$. This output state is known as an *entangled state* because it cannot be written as a direct product of quantum states for the two qubit register, i.e., $\alpha |00\rangle + \beta |11\rangle \neq |\Psi_1\rangle \otimes |\Psi_2\rangle$. Hence, a measurement of the output of qubit 2 should collapse the state of qubit 1. This is to be contrasted with the case of single qubit gates, where the input and the output of a general n-QR can always be expressed as a *product* or *separable state* $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \cdots \otimes |\Psi_n\rangle$, for arbitrary superpositions $|\Psi_i\rangle$.

The fact that the CNOT gate takes superpositions of the control qubit into entanglement of the corresponding output qubits is an outstanding property. In addition to this, the CNOT gate is a *reversible* gate: from its output we can reconstruct its input. It suffices to repeat the same gate, i.e., CNOT$_{1,2}$(CNOT$_{1,2}$$(|\Psi_1\rangle |\Psi_2\rangle)) \equiv |\Psi_1\rangle |\Psi_2\rangle$. Thus, the CNOT can be used to perform *reversible computation.* As we shall see below, *quantum entanglement* is at the very heart of any quantum computational process and also a fundamental ingredient of most of the 'spooky' technological applications that quantum information brings as a byproduct.

For illustrative purposes, let us go back to the network presented in Fig. 1. By making $U \equiv$ CNOT, we are left with the *entangling* quantum network $\widehat{N}_{\text{GHZ}} \equiv$ CNOT$_{23}$CNOT$_{12}$
$P(\varphi)_1 H_1$, which in the most elementary case performs the transformation

$$\widehat{N}_{\text{GHZ}}(|\Psi\rangle \equiv |000\rangle) \longmapsto |\Psi'\rangle \equiv \tfrac{1}{\sqrt{2}}(|000\rangle + \mathrm{e}^{i\varphi}|111\rangle)\,, \tag{4}$$

thus producing a highly entangled state of three qubits known as the *maximally* entangled Greenberger-Horne-Zeilinger state (**Greenberger *et al.*,** 1989; **Greenberger *et al.*,** 1990). In Fig. 1, the action of the first single qubit gates H, and $P(\varphi)$ is to rotate and to 'phase-shift' the state $|0\rangle_1$ into $\frac{1}{\sqrt{2}}(|0\rangle_1 + \mathrm{e}^{i\varphi}|1\rangle_1)$ while the other qubits remain unaffected. As expected at this stage, the three-QR state is still a separable state. Next, we enter the CNOT$_{12}$ gate. Since its control qubit is in a superposition state, it is clear that this gate will entangle the qubits 1 and 2 of the register. Indeed, after this XOR gate operation we are left with the state $\frac{1}{\sqrt{2}}(|00\rangle + \mathrm{e}^{i\varphi}|11\rangle) \otimes |0\rangle$, the product state of the maximally entangled (Bell or EPR) state of two qubits $|\Psi_{\text{BELL}}\rangle$ (**Bell,** 1987; **Bell,** 1964; **Einstein *et al.*,** 1935), and the qubit state $|0\rangle$. The last action of the network leaves the quantum register in the output GHZ state $|\Psi_{\text{GHZ}}\rangle \equiv |\Psi'\rangle$ of Eq. (4). The subject of quantum entanglement and the issue of how to quantify the degree of entanglement of a given entangled state is addressed in the Section III.

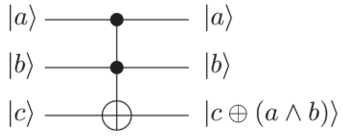
In the physical implementations to be described below, the universal set of gates $\{P(\varphi), H, \text{CNOT}\}$ shall be referred to. The logic gates $P(\varphi)$, and H, can be written in the $\mathcal{B}_1$-basis, and the CNOT gate in the computational basis of two-qubits $\mathcal{B}_2 \equiv \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ as follows:

$$P(\varphi) \equiv \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\varphi} \end{pmatrix}, \qquad H \equiv \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5}$$

$$\text{CNOT} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{6}$$

Another fundamental logic gate, whose classical version is universal for *reversible computation*, is the "*controlled-controlled*-NOT" (c^2-NOT) gate or Toffoli gate (**Toffoli,** 1980); a three-qubit gate that maps $|a\rangle |b\rangle |c\rangle \mapsto |a\rangle |b\rangle |c \oplus (a \wedge b)\rangle$. Hence, the third qubit experiences a flip or a NOT operation if and only if the control qubits $|a\rangle$, and $|b\rangle$ are in the state $|1\rangle$. By contrast, if the third qubit is prepared in the state $|0\rangle$ then this gate computes the AND of the first two qubits: $|a\rangle |b\rangle |0\rangle \mapsto |a\rangle |b\rangle |a \wedge b\rangle$. In addition, if we prepare $|a\rangle = |1\rangle$, then the c^2-NOT gate becomes a CNOT gate with $|b\rangle$, and $|c\rangle$ as inputs. This means that the Toffoli gate is capable of generating operations such as NOT, AND, and CNOT in such a way that all the information about the input is 'preserved'. Thus, the Toffoli gate provides us with a complete operator set: any gate can be generated with just a c^2-NOT gate, thus giving the logical connectives for performing quantum arithmetic and the evaluation of functions in general.

The Toffoli gate is schematically represented as



where the filled dots indicate the control qubits while the target qubit, denoted by $\oplus$, is negated if and only if the control bits are in the state $|1\rangle|1\rangle$. The action of this gate can be written operationally as c^2-NOT_{ijk}, where i, j (k) stand for the control (target) qubits. The Toffoli gate can be built from the controlled-V (C-V), CNOT, and Hadamard gates as follows: $c^2\text{-NOT}_{123} \equiv H_3V_{13}\text{CNOT}_{12}V_{23}^{\dagger}\text{CNOT}_{12}V_{23}H_3$, where C-$V^{\dagger} \equiv$ C-V^{-1}. Similarly, the CNOT gate can be constructed by applying a simple network of H, and C-V gates as follows: $\text{CNOT}_{12} \equiv H_2V_{12}V_{12}H_2$. There are, of course, plenty of quantum networks that can be built to represent the above-mentioned gates, but there is a main concern when building such networks: it is desirable and almost necessary to minimise the number of gates required to perform a given quantum computational task.

Quantum parallelism

The fact that a quantum system is capable of performing a computation was first pointed out by Feynman (**Feynman,** 1982; **Feynman,** 1985) and Benioff (**Benioff,** 1982(B); **Benioff,** 1982(A)) in 1982. However, it was Deutsch (**Deutsch,** 1985), in 1985, who made this idea more concrete by establishing that a quantum computer can perform the best of its computational potential by realising a process that he termed "quantum parallelism." By doing this, it is easy to see that a quantum computer can perform certain computational tasks much faster than any classical digital computer. This observation turns out to be the first quantum algorithm, known as the Deutsch-Josza algorithm (**Deutsch & Jozsa,** 1992), where physical principles such as quantum interference and quantum entanglement were made evident as a powerful computational resource.

To see why this is so, suppose we are given a device "*oracle*" that computes the Boolean function $f: x \in \{0,1\} \mapsto f(x) \in \{0,1\}$ in a single step. The problem is to determine whether $f(x)$ is *constant* (i.e., $f(0) = f(1)$), or *balanced* $(f(0) \neq f(1))$, with the minimum possible number of queries. It is clear that any attempt at solving this by using classical means invokes the oracle twice. In contrast, we note that with the help of a quantum strategy, a "quantum oracle $\mathcal{U}_f$" that performs the unitary transformation $\mathcal{U}_f: |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ in a single step, this problem is easily solved with only one query. Here $x, y \in \mathcal{B}_1$. Imagine a two wire network that is given with the input $|\Psi_0\rangle = |0\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. The following algorithm shows how to solve this (Deutsch's) problem efficiently:

1. Apply the Hadamard transform to the first qubit:

$$H: |\Psi_0\rangle \rightarrow |\Psi_1\rangle, \quad |\Psi_1\rangle \equiv \tfrac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \qquad (7)$$

2. Send the two-qubit state $|\Psi_1\rangle$ through the quantum oracle. This gives you the result

$$\mathcal{U}_f: |\Psi_1\rangle \rightarrow \tfrac{1}{2}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle](|0\rangle - |1\rangle) \equiv |\Psi_2\rangle \qquad (8)$$

   Note that the generic action of this function evaluator $\mathcal{U}_f$ over a state of the type $|x\rangle(|0\rangle - |1\rangle)$ gives the output $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$.

3. Apply H to the first qubit of $|\Psi_2\rangle$. Then perform a measurement in the $\mathcal{B}_1$-basis of qubit 1 final output. The result of this measurement reveals the answer to our problem.

Note that the state of qubit 1 in Eq. (8) can be written as

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle = \begin{cases} \pm(|0\rangle + |1\rangle) & \text{if } f \text{ is constant} \\ \pm(|0\rangle - |1\rangle) & \text{if } f \text{ is balanced} \end{cases} \qquad (9)$$

Hence, after step 3 of this protocol, we shall always find qubit 1 in the state $|0\rangle$ if the function is constant and $|1\rangle$ is the function is balanced. Also note that qubit 2 remains in the same state throughout this protocol. Thus, by using quantum superpositions instead of classical evaluations, we have solved this problem with just one query (throughout the whole process we have assumed a coherent evolution of the qubit states). The power of quantum parallelism becomes even more evident when we try to solve the same problem but for large registers, i.e., when $x \in \{0,1\}^n$. This will be discussed later in Subsec. III.H. Thus, Deutsch pointed out one of the most outstanding properties of a quantum computer and paved the way for the development of the field of quantum information processing.

So far, we have been concerned only with the formal framework that allows an introduction of all the elements required to perform universal quantum computation. However, nothing has been said about concrete physical implementations that may lead to a practical demonstration of the quantum logic gates introduced above. This point shall be returned to later, to briefly describe the experimental hardware currently used for a few qubit quantum computation and possible future prospects. As you may imagine, the extremely fragile nature of the quantum states used as qubits means that the requirements necessary for any hardware useful for quantum computation are rather stringent. As we have pointed out, the dynamics of a qubit physical evolution on a quantum computer is ruled by the laws of quantum physics. Thus, we should expect any unitary transformation or quantum gate U (e.g., the matrix operator $U \equiv \textsc{cnot}$ given in Eq. (6)) to be represented by an operator $U(t)$

$$U(t) = \mathcal{T} \exp\left(-\frac{i}{\hbar}\int \mathcal{H}(t)dt\right), \tag{10}$$

such that $U(t) \equiv U$. Here, $\mathcal{T}$ denotes time-ordering, and $\mathcal{H}$ is the Hamiltonian that describes the physical system used to represent the qubits. Thus, the dynamic action of a quantum gate can be viewed in terms of the time evolution of the unitary matrix $U(t)$ which, according to the quantum mechanical Schrödinger's equation, connects the initial wavefunction coefficients to the final ones: mapping on the qubit basis states uniquely specifies the dynamics of an *arbitrary* initial quantum state. Hence, it should be possible to identify a Hamiltonian $\mathcal{H}$, acting over a definite time t, that produces the desired U-gate. This is the main idea behind any intended physical implementation of quantum computation. In practice, there are different quantum hardwares that exploit different types of Hamiltonians in order to implement such quantum logic gates.

Quantum hardware requirements

The building of hardware for a quantum computer implies the processing of quantum information in a *coherent* fashion (see Sec. IV). Regardless of the chosen technology, we need the feasibility to reliably perform the following experimentally:

1. Preparation and Storage: We must be able to *prepare* an n-quantum register in a definite state such as $|00\cdots 00\rangle$, and to *store* the information used while processing the quantum computation for a time long enough to perform an arbitrarily complex computational task[5].
2. Isolation: The quantum register must be well isolated from the environment, so that we can minimize the errors due to decoherence.
3. Measurement: We must be able to efficiently measure the QR states in the basis $\mathcal{B}_1$.
4. Unitary operations: We must be able to manipulate individual qubit states, and to have control over the interactions among qubits, so that we can perform universal quantum gates over any subset of gates of the quantum register.
5. Precision: We must be able to control the unitary evolution of the register in such a way that the gates are implemented with high precision.

Some aspects of this prescription shall be made more precise below, especially when discussing the subject of 'quantum errors' that need to be taken into account when performing practical quantum computation (see Sec. IV). The subject of quantum hardware practicalities will be returned to in Section V, where different physical systems that may serve as quantum registers are explored.

C. Global control quantum computation

Aside of the traditional '*local*' control (LC) mechanism for the implementation of localized multi-qubit gates in a quantum register, there is the so-called '*global*' control (GC). As described above, in LC quantum computation (LCQC), an induced evolution in the system requires the *direct* individual localization of the computational qubits. This fact can pose a difficulty regarding the physical implementation of the computing process, especially at scales where the manipulation invokes more than a few qubits register. By contrast, in GC quantum computing (GCQC) the induced evolution of the system doesn't require direct individual localization of the computational qubits to be targeted by the logic gates; and we can induce a localized gate by using the instructions stored in the register's initial configuration (**Lloyd,** 1993; **Benjamin,** 2000, 2002; **Benjamin *et al.*,** 2005; **Jaramillo & Reina,** 2008). Thus, from the viewpoint of quantum information technologies, it may be more promising to be able to realize unitary manipulations within the quantum register in a global fashion.

The GCQC models are arrays of two level quantum systems interacting, in first approximation, with their nearest neighbours. There exists a finite number of "qubit species" distributed in an alternate manner within the arrays, as shown schematically in Fig. 2(a). Here, each species can be collectively manipulated in an independent way. An example of a physical realization of such architectures is a periodic and finite set of frequencies $(\omega_B\omega_A\omega_B\cdots)$ manipulated through resonant radiofrequency (RF) pulses. Between the '*computational*' qubits, those effectively involved in the computation, there are auxiliary qubits or "ancillae", with purely operative functions which are initialized in the computational state $|0\rangle^{\otimes m}$. Besides the ancillae, there is a "special qubit", the

[5] In practice, this time is bounded by *decoherence* of the register states (see Sec. IV).

"control unit", whose role is to localize and 'transport' information between the computational qubits. One qubit gates, for example, are performed in two steps: first, the control unit is taken near enough to the computational qubit to be modified, and then the desired gate is performed over the computational qubit, as a controlled gate, where the control unit acts as the control qubit.

We next introduce some interesting architectures and their respective operative protocols.

i) **Model 1** (*BM1*). Proposed by Benjamin (**Benjamin,** 2002), this is one of the simplest models for GCQC; it consists of two species of *physical* qubits, A and B, as shown in Fig. 2. The computational qubits are encoded in physical qubits ($|0\rangle \equiv |\uparrow\rangle$ and $|1\rangle \equiv |\downarrow\rangle$) belonging exclusively to a given species with the exception of the "special qubit" or "control unit", which is initialized in a different species at the computational state $|1\rangle$. There are arrays of three and five ancillae qubits alternately distributed between the computational qubits (see Fig. 2(b)). The generic Hamiltonian for this system is given by $H = \sum_{j=1}^{n} H_j^s + \sum_{j=1}^{n} H_{j,j+1}^{\text{int}}$, where the first term is associated with the individual qubit energy and the latter with the interaction energy between neighbouring qubits. The particular characteristics of the system reduce the total Hamiltonian to the form (**Benjamin,** 2002):

$$\begin{aligned} H_{2j} &= H^A, \\ H_{2j+1} &= H^B, \\ H_{2j,2j+1} &= H^{AB}, \\ H_{2j+1,2j} &= H^{BA}. \end{aligned} \tag{11}$$

This model works as long as the following conditions are fulfilled: a) it has to be possible to control the supression of the interaction process due to H^{BA}, in a way that the system reduces to a set of pairs A-B interacting identically through H^{AB}; b) any quantum gate must be able to be realized, in the A-B pairs, through the manipulation of the remaining terms: H^A, H^B and H^{AB}; c) as in the requirements a) and b), but this time supressing the interaction H^{AB}. These conditions may, however, pose a challenge from an experimental point of view (**Benjamin *et al.*,** 2005). To alleviate such difficulties, a strategy that incorporates a third energy level as part of one of the qubit species (a "barrier"), has been put forward in (**Benjamin *et al.*,** 2005), at the cost of increasing the number of species in the array.

As an illustration, in Fig. 2(c) we show how to perform a one computational qubit gate: the control unit is located at an adjacent cell from the target qubit (**Y**). Making sure that the interacting Hamiltonian between the target and the control unit is turned on (H^{AB}), any arbitrary controlled gate ($Ctrl - \mathcal{U}$) can be performed by means of using the species where the control unit is located as the *control* qubit and the species where the target computational qubit is located as the *target*.

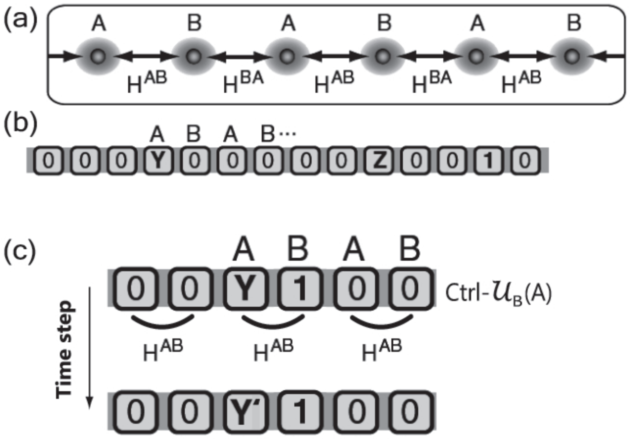


FIG. 2 (a) Schematic of a periodic array of two types of qubits (A and B), present in the architectures *BM1* and *BM2* (see text) for quantum computation based on global control. (b) Array of ancillae and computational qubits in architecture *BM1*. (c) One qubit gate $\mathcal{U}$ acting selectively on qubit **Y**. The gate is indirectly performed using the controlled quantum gate $Ctrl_B(A)$, which uses the H^{AB} interaction Hamiltonian. The "control unit" acts as the control qubit and assures the localized action of $\mathcal{U}$ (**Jaramillo & Reina,** 2008).

ii) **Model 2** (*BM2*). This model actually precedes *BM1* (**Benjamin,** 2000). It has the same Hamiltonian configuration specified in Eq. (11). Unlike *BM1*, this model doesn't require the ability to independently control the interacting Hamiltonians, H^{AB} and H^{BA}. This benefit doesn't come free; in this case the computational qubits are encoded in four physical qubits, as follows: $|0\rangle \equiv |\uparrow\uparrow\downarrow\downarrow\rangle$ and $|1\rangle \equiv |\downarrow\downarrow\uparrow\uparrow\rangle$. Between every encoded computational qubit there are four ancillae qubits. The "control unit" is also encoded, but in a different configuration: $|\uparrow\uparrow\downarrow\downarrow\uparrow\uparrow\rangle$ and $|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$, representing the computational states $|1\rangle$ and $|0\rangle$, respectively. The complete array is shown in Fig. 3(a). The operational gates which, applied sequentially, perform any *computational gate*, are symmetric three qubit gates of the generic form

$$\begin{aligned} M(u_{00}, u_{01}, u_{10}, u_{11}) = & \; |00\rangle\langle 00| \otimes u_{00} + |01\rangle\langle 01| \otimes u_{01} + \\ & |10\rangle\langle 10| \otimes u_{10} + |11\rangle\langle 11| \otimes u_{11} \;, \end{aligned} \tag{12}$$

where M acts simultaneously over every physical qubit of a given species and the symmetric condition $u_{01} = u_{10}$ is fulfilled. This condition is compatible with the fact that neighbouring qubits are of the same species and therefore only symmetric gates are physically feasible.

Both models, *BM1* and *BM2*, perform *computational* two-qubit controlled gates using the control unit as the carrier of information from the "control" qubit to the "target" qubit. This is done through the entanglement between the control unit and the control qubit, as illustrated in Fig. 3(b). In (**Jaramillo & Reina,** 2008), we show that in order to perform a more general two-qubit gate under the former protocol, two controlled gates are required; a fact that triples the computational time. To see why this is so, consider the case where a general two-qubit gate is performed through the scheme depicted in Fig. 3(b). In this case, the state of the control unit (dark gray) approaching step (c) may carry information about qubit state **V**, given the action of the general two-qubit gate performed at step (b). This disables the possibility of recovering the original localized qubit state **Y** through the step (c) where the entanglement is destroyed.

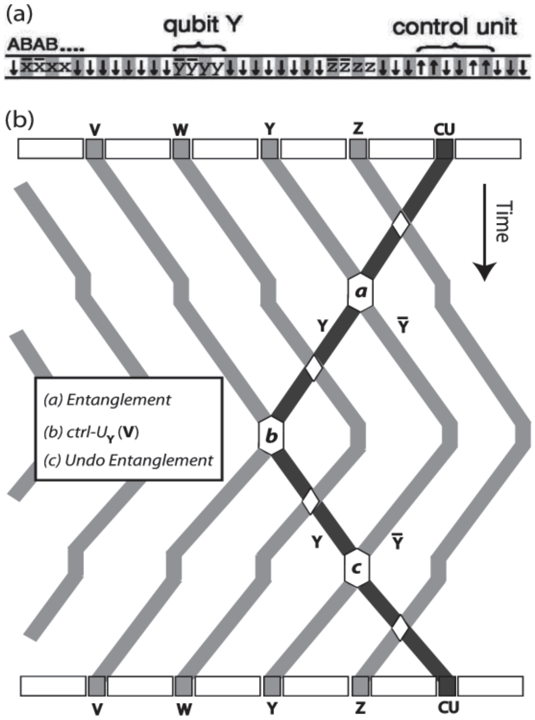
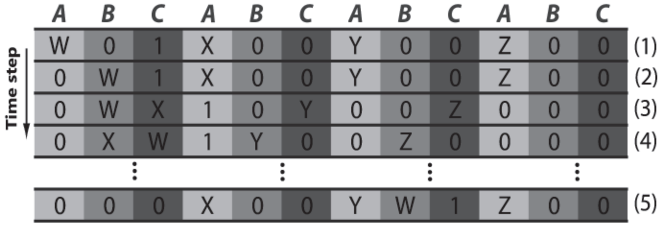


FIG. 3 (a) Array of ancillae and computational qubits in architecture *BM2*. (b) Heuristic protocol for two-qubit (**V** and **Y**) computational gates in models *BM1* and *BM2*. Computational qubits are in light gray and distinguished by letters. The white space between computational qubits corresponds to ancillae qubits, and the line in dark grey corresponds to the control unit path (**Jaramillo & Reina,** 2008).

iii) **Model 3** (*LM3*). Introduced by Lloyd (**Lloyd,** 1993), this model is perhaps the first proposal for GCQC. It has three different species distributed in a periodic array $ABCABCABC$. Here, there's no need to control interacting Hamiltonians and computational qubits are encoded in physical qubits belonging exclusively to a given species, just as in *BM1*. There are two ancillae qubits between the computational qubits.



A	B	C	A	B	C	A	B	C	A	B	C	
W	0	1	X	0	0	Y	0	0	Z	0	0	(1)
0	W	1	X	0	0	Y	0	0	Z	0	0	(2)
0	W	X	1	0	Y	0	0	Z	0	0	0	(3)
0	X	W	1	Y	0	0	Z	0	0	0	0	(4)
	⋮			⋮			⋮			⋮		
0	0	0	X	0	0	Y	W	1	Z	0	0	(5)

FIG. 4 Protocol for a two-qubit quantum gate between arbitrary computational qubits **W** and **Z**, in architecture *LM3*. Every computational qubit is initiated at qubit species A. (1) The control unit is located at the neighbourhood of **W**, in this case **W** is at species A, while the control unit is at species C. (2) A controlled *SWAP* gate between species A and B is applied by using qubits at species C as the control qubits. Given the location of the control unit, only the computational qubit **W** will be transferred to species B. (3) A *SWAP* gate is applied between species A and C. (4) A *SWAP* gate is applied between species B and C. (5) Steps 2, 3, and 4 are applied again. The register is ready to implement a two-qubit gate between computational qubits **W** and **Z** using the control unit. This is done after applying a controlled two-qubit gate between species A and B, where the species C acts as the control qubit. Any other operation can be reverted so that the modified computational qubits **W** and **Z** can go to their initial locations in the register (**Jaramillo & Reina,** 2008).

The operative gates that add up to perform computational gates are non-symmetric three qubit gates of the generic form given by Eq. (12). Unlike the models above, two-qubit gates are performed by the transportation of one of the computational qubits to a position adjacent to the second computational qubit involved in the two-qubit gate. This process, illustrated in Fig. 4, is performed by using the control unit to exclusively transport the first computational qubit (**W**) through the register. Once the control unit and the two computational qubits (**W** and **Z**) are all in the same neighbourhood, ABC, the system is ready to apply any two-qubit computational gate, where only the former computational qubits are involved. This is assured given that the control unit acts as a control qubit for the action of the two-qubit gate over the former computational qubits.

Recently, a proposal that uses organic polymers to encode the qubits in the global scheme proposed in (**Benjamin *et al.*,** 2005) has been put forward in molecular architectures for GCQC (**Mujica *et al.*,** 2009).

D. One-way quantum computation

Aside of the standard local and global quantum computation described above, which are performed through a series of unitary quantum logic gates as part of a multipartite quantum interference circuit, there is another method which is based on a radically different concept. This is the so-called *one-way* quantum computing proposal of Raussendorf and Briegel (**Raussendorf & Briegel,** 2001). In this view, the requirements for performing conventional QC are reformulated. In the one-way or measurement based quantum computer method, the qubits are initially prepared in the form of a highly entangled *resource* state: a cluster or a graph state; see Appendix B (**Raussendorf & Briegel,** 2001; **Briegel & Raussendorf,** 2001). After this, the computation follows the implementation of a sequence of single-qubit measurements with classical feedforward of their outcomes, and therefore, the resource state is destroyed by the measurements and the one-way quantum computer becomes irreversible (hence the term "one-way"). As a consequence, the order and choices of measurements determine the algorithm computed. As a general rule, the choices of basis for later measurements *do depend* on the results of the earlier ones, and hence the measurements cannot all be performed at the same time (**Raussendorf & Briegel,** 2001).

There exist an *equivalence* between the one-way computation and the quantum circuit model: the former can be made into a quantum circuit by using quantum gates to prepare the resource state. For cluster and graphresource states, this requires only one two-qubit gate per bond, so is efficient. It turns out that any quantum circuit can be simulated by a one-way computer using a two-dimensional cluster state as the resource state, by laying out the circuit diagram on the cluster: Z measurements ($\{|0\rangle, |1\rangle\}$ basis) remove physical qubits from the cluster, while measurements in the X-Y plane ($\{|0\rangle \pm e^{i\theta}|1\rangle\}$ basis) teleport the logical qubits along the "wires" and perform the required quantum gates (**Raussendorf *et al.*,** 2003). This is also polynomially efficient, as the required cluster size scales as the size of the circuit (qubits × timesteps), while the number of measurement timesteps scales as the number of circuit timesteps.

In (**Walther *et al.*,** 2006), the experimental realisation of four-qubit cluster states encoded into the polarization state of four photons has been reported. They characterized the quantum state by implementing experimental four-qubit quantum state tomography. Using this cluster state, they demonstrated the feasibility of one-way quantum computing through the construction of a universal set of one- and two-qubit logic gates. Furthermore, Walther *et al.* (**Walther *et al.*,** 2006), succeeded in implementing a basic Grover's search algorithm. More recently, the same group (**Prevedel *et al.*,** 2007) has demonstrated, by running the two-qubit Grover's algorithm on a 2 × 2 cluster state of photons, the execution of one-way quantum computation. This shows that indeed, one-way QC can be suited for such computing tasks. In addition, a *linear optics* quantum computer based on one-way computation has been proposed in (**Brown & Rudolph,** 2005), and cluster states have also been created in *optical lattices* (**Mandel *et al.*,** 2003).

Next, another way to realise quantum computation is discussed, the so-called *geometric* or *holonomic quantum computation* (**Zanardi & Rasetti,** 1999; **Pachos *et al.*,** 1999; **Pachos & Chountasis,** 2000).

E. Quantum computation by geometric means

It is interesting that there is an alternative way of performing quantum computations. This is built on the results of Berry (**Berry,** 1984; **Wilczek & Zee,** 1984; **Shapere & Wilczek,** 1989), who showed that a quantum system under cyclic evolution acquires, besides the dynamic phase induced by the time evolution of the system, a *geometric phase*, the so-called Berry phase. It can be shown (**Zanardi & Rasetti,** 1999; **Pachos *et al.*,** 1999; **Pachos & Chountasis,** 2000; **Ekert *et al.*,** 2000(A)) that universal quantum gates can be implemented by purely geometric means, i.e., by using Abelian and non-Abelian geometric computations (holonomies) (**Berry,** 1984; **Wilczek & Zee,** 1984; **Shapere & Wilczek,** 1989) rather than dynamic ones. The holonomies can be either Abelian phase factors (Berry phases) or general non-Abelian operations, depending on whether the eigenspace of the system's Hamiltonian is nondegenerate or degenerate. An interesting feature of the holonomic quantum computation is its potential robustness to certain types of computational errors, hence offering a natural way of performing *fault-tolerant* quantum computation. Let us formally establish the idea of a cyclic evolution to build the geometric phase and the non-Abelian Berry phase (non-adiabatic state evolution):

Cyclic evolution

The concept of a cyclic evolution is based on the adiabaticity (**Galindo & Pascual,** 1990) of the quantum state evolution of a given physical system, say the vector state $|\Psi\rangle$. In quantum mechanics, a basic goal is to calculate amplitudes, and then square them to obtain the probability of an event. Formally, in a Hilbert space $\mathbf{H}$, we have $|\langle\Psi|\Psi\rangle|^2 = 1$. However, this implies an ambiguity: there is no physical distinction between the two states $|\Psi\rangle$, and $\mathrm{e}^{i\varphi}|\Psi\rangle$. To fix this, the projective space $\mathbf{P}$ is introduced, in which vectors are grouped into equivalence classes such that we map $\mathbf{\Pi}: \mathbf{H} \to \mathbf{P}$, where $|\Psi\rangle \mapsto [|\Psi\rangle] = \{|\Psi'\rangle : |\Psi'\rangle = r\mathrm{e}^{i\varphi}|\Psi\rangle\}$, for any $r > 0$ and real φ (**Ekert *et al.*,** 2000(A)). Hence, a cyclic evolution of the system's state $|\Psi\rangle$ translates into a closed curve $\mathbf{\Pi}(\mathcal{C}) \in \mathbf{P}$ covered in a period τ. In $\mathbf{H}$ the situation is rather different: at $t = \tau$, the path $\mathcal{C} \in \mathbf{H}$ followed by the initial state $|\Psi(0)\rangle$ no longer coincides with the final state $|\Psi(\tau)\rangle$ of the system: there is a phase difference of $\mathrm{e}^{i\varphi}$ between them. This phase can be determined by making the following (adiabatic) approximation: for each point $|\Psi(t)\rangle$ on $\mathcal{C}$, $t \in [0,\tau]$, we can choose a $|\Psi_\Pi(t)\rangle$ from $\mathbf{\Pi}(\Psi(t))$ in such a way that $|\Psi_\Pi(0)\rangle = |\Psi_\Pi(\tau)\rangle$. Hence we can write

$$|\Psi(t)\rangle = \mathrm{e}^{if(t)}|\Psi_\Pi(t)\rangle \ , \tag{13}$$

where the phase change of $|\Psi(0)\rangle$ is now given through the function $f(t)$: $\varphi = f(\tau) - f(0)$.

Calculating geometric and dynamic phases

Let us start by writing the system's Schrödinger equation

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\Psi(t)\rangle = \mathcal{H}(t)|\Psi(t)\rangle \ , \tag{14}$$

where $\mathcal{H}(t)$ represents the system's Hamiltonian. From Eqs. (13), and (14) we obtain

$$\begin{aligned}\varphi = \int_0^\tau \mathrm{d}f(t) \ &= \ -\frac{1}{\hbar}\int_0^\tau \langle\Psi(t)|\,\mathcal{H}\,|\Psi(t)\rangle\,\mathrm{d}t + \\ & i\int_0^\tau \langle\Psi_\Pi(t)|\,\tfrac{\mathrm{d}}{\mathrm{d}t}\,|\Psi_\Pi(t)\rangle\,\mathrm{d}t \ . \end{aligned}\tag{15}$$

Hence, we end up with a total phase φ which is built of a *dynamic phase* δ that depends on the Hamiltonian $\mathcal{H}(t)$, and a *geometric phase* γ that depends only on the path $\mathcal{C}$, and is independent of the rate at which $|\Psi(t)\rangle$ completes $\mathcal{C}$, the Hamiltonian, or the choice of reference $\{|\Psi_\Pi\rangle\}$ (**Ekert *et al.*,** 2000(A)). These geometric and dynamic phases can be calculated as:

$$\gamma \ = \ i\oint_{\mathcal{C}} \langle\Psi_\Pi|\,\mathrm{d}\,|\Psi_\Pi\rangle \tag{16}$$

$$\delta \ = \ -\frac{1}{\hbar}\int_0^\tau \langle\Psi(t)|\,\mathcal{H}\,|\Psi(t)\rangle\,\mathrm{d}t \ . \tag{17}$$

A particular case of the geometric phase γ is the Berry's phase (**Berry,** 1984), which occurs when the system's dynamics is performed under adiabatic conditions. This imposes restrictions over the rate at which $|\Psi(t)\rangle$ completes a given cyclic evolution. A fundamental characteristic of the Berry phase is that the energy eigenspace of the instantaneous Hamiltonians is non-degenerate along the path $\mathcal{C}$. As a model example, it can be shown, by using Eq. (16), that the Berry phase of a spin-half particle located in an external oscillating field gives the result

$$\gamma = -\pi(1-\cos\theta) \ , \tag{18}$$

where θ is the angle between the Bloch vector and the z-axis (**Ekert *et al.*,** 2000(A)). As said, it is assumed that through the qubit cyclic evolution, the Hamiltonian parameters are changed adiabatically. The generalization of this result to any closed path gives $\gamma = \Omega/2$, where Ω is the solid angle enclosed by $\mathcal{C}$ on the Bloch sphere (**Berry,** 1984). Thus, the Berry phase depends only on the area covered by the motion of the system, and is independent of the details of how this motion is executed.

The results explained above constitute an alternative approach to quantum computation. Here, quantum gates can be built by using purely holonomies. A procedure to perform this is outlined in (**Ekert *et al.*,** 2000(A)) for the case of a nuclear magnetic resonance (NMR) system via the use of the Abelian Berry phase. Experimental work has combined the above results to perform a first step towards geometric quantum computation (**Jones *et al.*,** 2000). The Abelian geometric phase has been used to experimentally demonstrate the controlled phase shift gate $B(\varphi)$ in an NMR system (**Jones *et al.*,** 2000). There is also another proposal for doing this via a Josephson junction system (**Falci *et al.*,** 2000). However, to be able to perform universal geometric quantum computation we need to combine this particular geometric gate (or any other two-qubit entangling gate) with single qubit gates. The proposals reported in (**Jones *et al.*,** 2000; **Falci *et al.*,** 2000) are restricted to Abelian holonomies only, which due to adiabatic conditions, have the disadvantage of being too slow if compared with typical dynamical time-scales, making it very difficult for any realistic realisation of quantum computation.

A leap has been taken towards the implementation of holonomic quantum computation. The adiabaticity difficulty has been overcome in (**Duan *et al.*,** 2001; **Xiang-Bin & Keiji,** 2001; **Xiang-Bin *et al.*,** 2001), by using non-Abelian holonomies to perform geometric quantum gates in a set of trapped ions (**Duan *et al.*,** 2001), and in an NMR system (**Xiang-Bin & Keiji,** 2001; **Xiang-Bin *et al.*,** 2001). The use of *non-adiabatic* state evolution implies two main differences from what was said for the Abelian Berry phase: i) After a time $t = \tau$, the state vector evolution is *non-cyclic*, and ii) The geometric phase Γ acquired over the period τ is different from the one found for the adiabatic evolution, $\Gamma \neq -\pi(1 - \cos\theta) = \gamma$. Details concerning these new results, and the way they can be used to perform conditional quantum dynamics (e.g., the controlled phase shift gate) can be found in (**Duan *et al.*,** 2001; **Xiang-Bin & Keiji,** 2001; **Xiang-Bin *et al.*,** 2001). As a bottom line, any scheme attempting to perform quantum computation using only geometric phases has to *eliminate the dynamic phase*. In NMR this can be done by using a refocussing technique known as spin-echo (**Ekert *et al.*,** 2000(A); **Jones *et al.*,** 2000).

Regarding the robustness of the geometric QC to errors, and the way decoherence may affect the geometric phases during the quantum computation, the following results are in order. By means of a quantum-jump approach, Carollo *et al.* (**Carollo *et al.*,** 2003) have calculated the geometric phase associated with the evolution of a system subjected to decoherence. They considered dephasing and spontaneous decay as the two main sources of decoherence, and showed that the geometric phase is completely insensitive to the number of jumps determined by the dephasing operator; that is, insensitive to dephasing. By using the same approach, Carollo *et al.* (**Carollo *et al.*,** 2004) have also calculated the geometric phase of a spin-1/2 system driven by one and two mode quantum fields subject to decoherence: they have shown that the corrections to the phase in the no-jump trajectory are different when considering adiabatic and nonadiabatic evolutions. Finally, it has also been shown in (**Carollo *et al.*,** 2006) that in the limit of a strongly interacting environment a system initially prepared in a decoherence-free subspace (DFS) coherently evolves in time, adiabatically following the changes of the DFS. If the reservoir cyclicly evolves in time, the DFS states acquire a holonomy.

So far, there has been an experimental demonstration of the two-qubit gate $B(\varphi)$ in an NMR setup (**Jones *et al.*,** 2000), and some other physical implementations in systems such as trapped ions (**Blatt & Wineland,** 2008), quantum dots (**Fushman *et al.*,** 2008; **Robledo *et al.*,** 2008), Josephson junctions (**Clarke & Wilhelm,** 2008), and other solid-state setups.

III. QUANTUM ENTANGLEMENT: A COMMUNICATION RESOURCE

Entanglement is a central concept in quantum information theory. In a system consisting of n quantum subsystems, it shows a form of correlations between such subsystems that cannot be understood or explained in any "classical" fashion because it points out exactly what distinguishes the quantum from the classical world. These correlations imply that each subsystem carries some knowledge, some degree of information, about the other parts. This degree of knowledge can be quantified, as is shown below. This section introduces the basic elements and definitions that are used to characterise the degree of entanglement of a given quantum system. A detailed review of the current developments regarding the subject of entanglement can be found in (**Horodecki *et al.*,** 2001; **Plenio & Virmani,** 2007; **Horodecki *et al.*,** 2007; **Amico *et al.*,** 2008; **Vedral,** 2008).

A. Quantifying quantum entanglement

It is well known how to quantify entanglement in the case of a bipartite system (a system consisting of two subsystems, namely A and B) in a total pure state. For more than two subsystems, or mixed states, the situation is not so clear (for a survey of recent developments see, e.g., (**Horodecki *et al.*,** 2001; **Plenio & Virmani,** 2007; **Horodecki *et al.*,** 2007; **Amico *et al.*,** 2008). Next, the basic tools and definitions are given. Consider a bipartite system composed of subsystems A, and B. The state vector for this system is in the finite dimensional Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. This is to be referred to as an $n \otimes m$ system, where n and m are the dimensions of the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. A general *pure* state of the system can be written as

$$|\Psi\rangle_{AB} = \sum_{i,j} c_{ij} \, |i\rangle_A \otimes |j\rangle_B \ , \tag{19}$$

where $\{|i\rangle_A\}$, and $\{|j\rangle_B\}$ are a complete orthonormal basis set for each subsystem.

Theorem (Schmidt decomposition): For any given pure state $|\Psi\rangle_{AB}$ it is always possible to find a complete set of orthonormal vectors $\{|n\rangle_A\}$, and $\{\widetilde{|n\rangle}_B\}$, in spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ such that

$$|\Psi\rangle_{AB} = \sum_{n=1}^{k} \alpha_n \, |n\rangle_A \otimes \widetilde{|n\rangle}_B \ , \tag{20}$$

where the coefficients $\alpha_n > 0$, and $k \leq \dim \mathcal{H}_{AB}$. Eq. (20) is called the Schmidt decomposition of $|\Psi\rangle_{AB}$.

Note that this decomposition contains only one index, in contrast to Eq. (19). The proof of this theorem is almost straightforward (see, e.g., (**Peres,** 1993)). Note: i) There is no Schmidt decomposition for a system of more than two subsystems. ii) A bipartite pure state is said to be *entangled* if at least two cofficients of the α_n's do not vanish (the number of non-vanishing coefficients is called the Schmidt number of $|\Psi\rangle_{AB}$)[6].

Degrees of entanglement: The entanglement of a given quantum state can be defined in terms of the concept of separability: if a given state does not satisfy the separability criterion, then the state is said to be entangled. However, it is not so easy to find a unique separability criterion that solves the problem of determining with certainty whether a given quantum state is entangled or not. In fact, this question has led to a very active field of research: manipulation of entanglement, where quantifying, concentrating and distilling entanglement, and using mixed-state entanglement as a resource for quantum communication are central subjects (**Horodecki *et al.*,** 2001; **Plenio & Virmani,** 2007; **Horodecki *et al.*,** 2007; **Amico *et al.*,** 2008). One separability criterion is based on the violation of Bell inequalities (**Werner,** 1989), where separable states are required to satisfy all Bell inequalities (**Werner,** 1989). However, this is not a very strong criterion since there are some entangled states that also satisfy all standard Bell inequalities (**Popescu,** 1994; **Popescu,** 1995; **Zukowski *et al.*,** 1998). A stronger and more useful criterion is based on the concept of partial transposition of Peres (**Peres,** 1996; **Peres,** 1999), in which he noted that a separable state remains a positive operator if subjected to partial transposition. For a detailed discussion of these criteria, see, e.g., (**Horodecki *et al.*,** 2007; **Amico *et al.*,** 2008) and references therein. Here, it is necessary to introduce some definitions concerning the degree of entanglement of a given quantum system. It follows from the Schmidt theorem that for a bipartite system (each subsystem having a two-dimensional Hilbert space)

$$|\Psi\rangle_{AB} = \alpha\,|0\rangle_A\,|0\rangle_B + \beta\,|1\rangle_A\,|1\rangle_B \ . \tag{22}$$

Suppose that any present phase is absorbed by the Schmidt vectors, such that we can define α, $\beta \in \mathbf{R}$, with $|\alpha| \leq |\beta|$. Then, the following terminology is introduced:

Product state: A state is a product state if and only if $\alpha = 0$.

Entangled state: A state is entangled if and only if $\alpha \neq 0$.

Maximally entangled state: A state is maximally entangled if and only if $|\alpha| = |\beta|$.

The most famous entangled states are the maximally entangled states $|\phi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle \pm |1\rangle\,|1\rangle)$, and $|\psi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle \pm |1\rangle\,|0\rangle)$. These four mutually orthogonal states are so important because they exhibit the strongest possible Bell-EPR correlations (**Peres,** 1993; **Braunstein *et al.*,** 1992), the reason they are known as the Bell-basis states. Also, as will be seen below, these states are crucial to many communication protocols. It was shown in Section II that these entangled states can be generated and manipulated in terms of universal quantum logic gates: suppose, for example, that a two qubit state is initialised in the state $|\Psi_0\rangle = |0\rangle\,|0\rangle$. Then, by applying the two successive quantum gates $\textsc{cnot}_{12}H_1$ to $|\Psi_0\rangle$, the Bell state $|\phi^+\rangle$ is generated (the same sort of unitary transformations can be applied to n-qubit systems in order to generate, for example, "Schrödinger cat states"-like). In (**Quiroga & Johnson,** 1999; **Reina *et al.*,** 2000(B)), a solid-state based setup for producing maximally entangled states of the Bell and Greenberger-Horne-Zeilinger type is proposed; also, in (**Reina & Johnson,** 2000(D)), a quantum teleportation protocol of quantum dot excitonic states has been proposed. It is interesting that once $|\phi^+\rangle$ has been generated, the remaining states of the Bell basis can be also generated by applying *only* single qubit gates to it.

B. Entanglement measures

Two main questions are: Given an arbitrary state, can we decide whether it is entangled? Given two quantum states, can we decide which of them has more entanglement?

As discussed above, the first question was partially solved initially by Peres (**Peres,** 1996) and refined by the Horodeckis (**Horodecki *et al.*,** 1996): Peres observed that if a matrix is entangled, it remains positive after being partially transposed; subsequently, the Horodeckis limited the criteria to the 2×2 and 2×3 case. For higher dimensions, the problem remains open (**Horodecki *et al.*,** 2007; **Amico *et al.*,** 2008) . The recognition of the partial transpose positivity property would later lead to

[6] In a bipartite system, subsystems A and B are described by *density operators* ρ_A and ρ_B. It turns out that these operators have the same non-vanishing eigenvalues: they are equal to the square of the Schmidt numbers. A state acting on Hilbert space $\mathcal{H}_{AB}$ is called *separable* (**Horodecki *et al.*,** 2001) if it is of the form

$$\rho = \sum_{i=1}^{k} c_i \rho_i^A \otimes \rho_i^B \ , \tag{21}$$

for some k, where ρ_i^A and ρ_i^B are states on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. If ρ is a *pure* state, i.e., $\rho = |\Psi_{AB}\rangle\,\langle\Psi_{AB}|$, then it is easy to see whether is entangled or not: indeed, it is separable if and only if $|\Psi\rangle_{AB} = |\Psi\rangle_A \otimes |\Psi\rangle_B$.

an important measure of entanglement called *Negativity* (**Vidal & Werner,** 2002). Later, the formalism of entanglement witnesses appeared (**Terhal,** 2000), based on the structure of the density matrix space. This formalism is of particular interest because it relies on operators called "witnesses of entanglement" which take negative expectation values whenever the state is entangled and with positive values on separable states. They are, however, not effective as quantifiers of entanglement.

The second question, as to how to quantify entanglement, is also quite an involved one, and it has been the object of extensive research over the past decade. We now give a brief review of several strategies that have been adopted towards its solution. One could try to solve this problem by using a particular protocol and measuring the entanglement of the chosen state by the success of the involved protocol or task. However, using this method, different protocols would yield different hierarchies of states, hence a different strategy should be adopted.

The observation that local operations and classical communication (LOCC) don't create entanglement suggests that if a state A can be transformed to B by LOCC then A is at least as entangled as B. This leads to a natural hierarchy of entangled states in the bipartite (two qubits) case in the form of the majorization process (**Nielsen & Kempe,** 2001). However, in the qudit case, or the multipartite (many qudits) case, one faces difficulties because of the existence of incomparable states, namely states which cannot be transformed into each other by LOCC means. These limitations can in principle be overcome in the asymptotic limit where many copies are used (**Popescu & Rohrlich,** 1997), or even when the transformation among states is not required to be fully certain (SLOCC) (**Bennett,** ***et al.***, 2001; **Dür,** ***et al.***, 2000). However, establishing a hierarchy gets very complicated even in low dimensional cases. Despite this, the LOCC hierarchy discussion has raised several measures of entanglement, such as the distillable entanglement (**Rains,** 1999; **Bennett,** ***et al.***, 1996), the entanglement cost (**Hayden,** ***et al.***, 2001), and the entanglement of formation (**Bennett,** ***et al.***, 1996).

Plenio and Virmani (**Plenio & Virmani,** 2007) have proposed an axiomatic approach to entanglement. They established the conditions that a quantity should exhibit in order to quantify entanglement, which must be satisfied even if one chooses to measure entanglement in a "protocol-based" fashion (**Horodecki** ***et al.*****,** 2007; **Amico** ***et al.*****,** 2008). This axiomatic approach is convenient as it not only incorporates the operational approach to entanglement, but goes further, avoiding the incomparability limitations, and even set bounds for them. Such basic conditions are (**Plenio & Virmani,** 2007)

§ *There are states with no entanglement.*—Separable states, i.e., states that can be written as

$$|\Psi\rangle_{1,\dots,N} = \sum p_i \, |\psi\rangle_1^i \otimes \dots \otimes |\psi\rangle_N^i \, , \tag{23}$$

have no entanglement. This is so because these states can be created by local operations and classical communications, namely they are classically correlated states which do not violate any Bell inequality.

§ *Non-separable states are entangled.*—Essentially this means that for any non-separable state there is a protocol in which the states outperform a separable state.

§ *Entanglement cannot increase under Local Operations and Classical Communications.*—This follows from Bennett's observation (**Bennett & DiVincenzo,** 2000): entangled states are those which can perform tasks that states generated by local operations and classical communications cannot; thus, LOCC cannot create entanglement because it would imply that LOCC could be used to perform the above mentioned tasks. Mathematically, this means that given a measure of entanglement $\mathcal{X}$,

$$\mathcal{X}(\rho) \geq \sum p_i \mathcal{X}\left(\frac{M_i \rho M_i^\dagger}{p_i}\right), \tag{24}$$

where $\sum M_i M_i^\dagger = 1$ and $p_i = Tr[M_i \rho M_i^\dagger]$. In the bipartite qubit case, LOCC establishes a full hierarchy in this sense: if a state can be transformed into another by LOCC then it is at least as entangled as the other one. The general qudit and/or multipartite case has some subtleties, as there are states which cannot be transformed into each other by LOCC operations with certainty, and thus, are incomparable using this criteria. However, this condition must still be satisfied. This is, in general, the most difficult property to test, although there are some simplifications (**Vidal,** 2000; **Horodecki,** 2005).

§ *Entanglement is invariant under Local Unitary (LU) operations.*—This reflects the freedom in the choice of basis for every subsystem, entanglement is independent of that choice and thus any measure of entanglement should also satisfy this invariance condition. Also, as local unitaries are invertible then, by the LOCC condition, both states must have the same entanglement.

§ *Maximally entangled states exist.*—This follows, as it can be shown that an arbitrary two-qubit state can be built by LOCC from an EPR pair (**Bennett,** ***et al.*****,** 1996). In the qudit/multipartite case, there is no notion of a unique maximally entangled state in the

LOCC sense, because of the existence of incomparable states, as discussed above; however Bell inequalities multipartite generalizations, such as the one by Greenberger, Horne, and Zeilinger (**Greenberger, *et al.*,** 1989), lead to the notion of maximal multipartite entanglement and generalize the EPR pair to higher numbers of qubits.

A quantity satisfying the above-mentioned conditions is called an *entanglement monotone*. There are some other properties which can be demanded of entanglement monotones when thinking in terms of axiomatic measures, i.e., when obtaining the optimal conditions for an entanglement measure. We give some of them that are of relevance to the entanglement monotones proposed in Paz-Silva and Reina (**Paz-Silva & Reina,** 2008; **Paz-Silva & Reina,** 2009).

[ADD] *Additivity.* Given two arbitrary states denoted by ρ_A and ρ_B,

$$\mathcal{X}(\rho_A \otimes \rho_B) = \mathcal{X}(\rho_A) + \mathcal{X}(\rho_B)\ . \qquad (25)$$

[SSA] *Strong super additivity.* Given a generic N-partite state $\rho^{1,\ldots,N}$,

$$\mathcal{X}(\rho^{1,\ldots,N}) \geq \mathcal{X}(\rho^{1,\ldots,m}) + \mathcal{X}(\rho^{m+1,\ldots,N})\ . \qquad (26)$$

[CONT]*Asymptotic continuity.* There are $c, c' \geq 0$ such that for all ρ, σ with $\delta(\rho,\sigma) \leq \epsilon$

$$|\mathcal{X}(\rho) - \mathcal{X}(\sigma)| \leq c\,\epsilon \log d + c'. \qquad (27)$$

Another multipartite entanglement measure formulated from pure geometric considerations has been proposed in (**Paz-Silva & Reina,** 2007).

C. Examples

We now review some measures of entanglement which have been extensively used and which are of great value because of their implications, properties and relation to quantum information.

***Entanglement of Formation* (EoF)**.— This is the most cited and prominent measure of entanglement, since for the bi-partite scenario it allows an exact, ambiguity free, analytical expression. It is defined as

$$\mathcal{E}_F^b(\rho_{AB}) = \min \sum p_i \mathcal{E}^b(\rho_i), \qquad (28)$$

$\mathcal{E}^b(\rho_{AB}) = S(Tr_B[\rho_{AB}]) = -Tr_B[\rho_{AB}]\log[Tr_B[\rho_{AB}]]$, and the minimization is intended over pure state decompositions (pure-convex-roof (**Uhlmann,** 1998)). Further, note that it can be rewritten as

$$\mathcal{E}_F^b(\rho_{AB}) = \min \sum p_i\ \tfrac{1}{2} I(\rho_A^i : \rho_B^i), \qquad (29)$$

where $I(\rho_A : \rho_B)$ is the quantum mutual information (**Cerf & Adami,** 1997). Although the minimization is, in general, non-trivial, it has an analytic solution for the two-qubit case (**Wooters,** 1998).

Consider, in decreasing order, the eigenvalues λ_i of the matrix $\sqrt{\rho_{AB}\tilde{\rho}_{AB}}$, where $\tilde{\rho}_{AB} = (\sigma_y \otimes \sigma_y)\bar{\rho}_{AB}(\sigma_y \otimes \sigma_y)$, $\bar{\rho}_{AB}$ is the elementwise complex conjugate of ρ, and σ_y is the Pauli matrix. The Concurrence is defined as $C(\rho_{AB}) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, and hence the EoF reads

$$\begin{aligned}\mathcal{E}_F^b(\rho_{AB}) \;=\; & -\frac{1+\sqrt{1-C^2}}{2}\log_2\frac{1+\sqrt{1-C^2}}{2} - \\ & \frac{1-\sqrt{1-C^2}}{2}\log_2\frac{1-\sqrt{1-C^2}}{2}. \qquad (30)\end{aligned}$$

The general multipartite EoF is currently conjectured to be additive, but a formal proof of it has, so far, been elusive (**Bennett, *et al.*,** 1997; **Shor**, 2002; **Shor**, 2004).

As pointed out in (**Plenio & Virmani,** 2007), due to the fact that the two-qubit $\mathcal{E}_F^b(\rho)$ and the two-qubit Concurrence $C(\rho)$ are monotonically related, some authors prefer to characterise entanglement using only the Concurrence (instead of $\mathcal{E}_F^b(\rho)$). This said, it should be stressed that it is only the entanglement of formation that is an entanglement measure, and the Concurrence gets its meaning via its relation to the EoF, and not the other way around.

Squashed entanglement.— It is defined as (**Christandl & Winter,** 2004)

$$E_{sq} := \inf\left[\tfrac{1}{2} I(\rho^{ABE} : Tr\left[\rho^{ABE}\right] = \rho^{AB}\right], \qquad (31)$$

where $I(\rho^{ABE}) = S(\rho^{AE}) + S(\rho^{BE}) - S(\rho^{ABE}) - S(\rho^E)$ is the quantum conditional mutual information, which essentially measures how correlated two parties are, according to a third one. This measure is important because it was the first additive entanglement measure, bounded by the entanglement of formation and the distillable entanglement.

Relative entropy of entanglement.— Defined as (**Vedral & Plenio,** 1998)

$$E_R^X(\rho) = \inf_{\sigma \in X} S(\rho\|\sigma), \qquad (32)$$

where X is a set of states, usually the set of separable states, distillable states, or positive partial transposed states, chosen according to the definition of separable states, such that LOCC maps X into X. It is not an additive quantity.

For other entanglement measures and a more detailed treatment of entanglement quantification, the reader is referred to (**Plenio & Virmani,** 2007; **Horodecki *et al.*,** 2007; **Amico *et al.*,** 2008).

As we mentioned before, the LOCC constraint is very strong in the bi-partite case. In the multipartite case, however, there are complications. The main issue is the existence of non LOCC-interconvertible states, which implies the existence of incomparable states and thus the impossibility of applying the LOCC constraint to obtain a hierarchy. The LOCC non-increasing condition must still hold for any measure of entanglement. This complication is strongly related to the issue of having many elements which can be entangled in different ways. For instance, in the four qubit case we can have an $|\Omega\rangle = |\phi^+\rangle_{12} \otimes |\phi^+\rangle_{34}$ state, which cannot be LOCC compared to a GHZ state, say $|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$, and thus the problem of characterizing its entanglement arises. Here, the axiomatic approach is valuable, as we can build a quantity characterizing the entanglement of a system. This liberty, however, implies that different monotones may manifest different hierarchies, which, in turn, means that each monotone characterizes a different type of entanglement (**Plenio & Virmani,** 2007). Of course, the more properties we require will narrow our search space further.

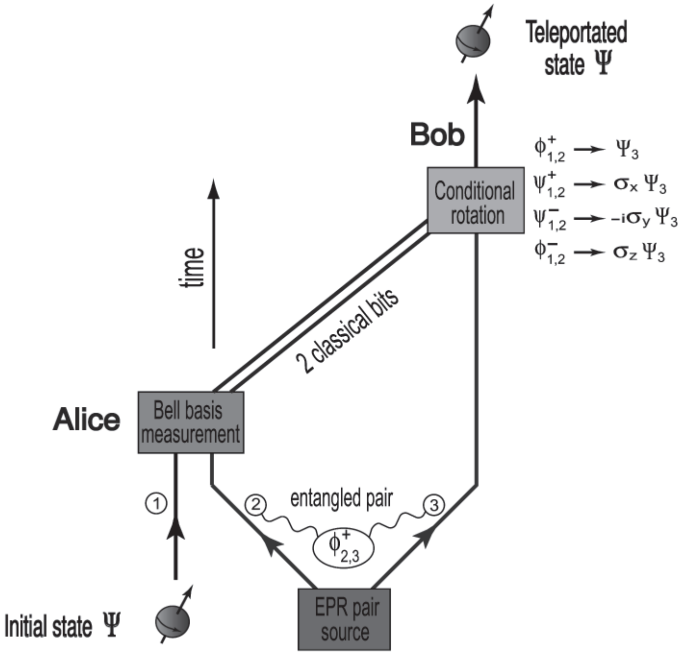

Teleportated state Ψ
Bob
$\phi^+_{1,2} \rightarrow \Psi_3$
$\Psi^+_{1,2} \rightarrow \sigma_x \Psi_3$
$\Psi^-_{1,2} \rightarrow -i\sigma_y \Psi_3$
$\phi^-_{1,2} \rightarrow \sigma_z \Psi_3$
Conditional rotation
time
2 classical bits
Alice
Bell basis measurement
①
②
entangled pair
③
$\phi^+_{2,3}$
EPR pair source
Initial state Ψ

FIG. 5 Schematics of the quantum teleportation process. For simplicity the kets notation for the quantum states associated with the 3-particle system has been omitted (see text).

A study of non-equilibrium multipartite entanglement dynamics in an externally driven Dicke model has been reported in (**Bastidas *et al.*,** 2009). This has been done for the driven single-mode Dicke model in the thermodynamic limit, when the field is in resonance with the atoms. There, the correlations for the atoms-field ground state, and the linear entropy have been analytically calculated as entanglement quantifiers. A strong relation between the stability of the dynamical parameters and the reported entanglement has been found in (**Bastidas *et al.*,** 2009).

Now that the basic framework to entanglement quantification has been introduced, we discuss the main practical applications of entanglement as a *communication resource*.

D. Quantum teleportation

This is arguably the most striking application of quantum entanglement. Here, the quantum state $|\Psi\rangle$ of a system can be transmitted from one spatial location to another with neither physical transportation of the system itself nor previous knowledge of $|\Psi\rangle$. This apparently impossible task invokes only the use of a two-particle maximally entangled state (e.g., $|\phi^+\rangle$)[7]— that has to be shared beforehand between the two parties that wish to transmit $|\Psi\rangle$— assisted by the communication of two classical bits of information. The details of the whole teleportation protocol, as originally formulated in (**Bennett *et al.*,** 1993), are given below. This is perhaps the most evident of the demonstrations of quantum entanglement as a *resource* for the transmission of quantum information. In (**Reina & Johnson,** 2000(D)), a prescription for the teleportation of excitonic states in a quantum dot molecule, and the generalization of the original protocol in terms of using an N-partite Schrödinger cat state has been reported.

The protocol that performs the teleportation process is sketched in Fig. 5. In this scenario, the "arrow of time" indicates how to carry out the protocol:

(t_0) At $t = t_0$ the EPR source prepares *one* of the *entangled* states of the Bell basis $\mathcal{B}_{\mathrm{B}} = \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ between particles 2 and 3, let's say, the state $|\phi^+\rangle_{2,3}$.

(t_1) At $t = t_1$ Alice sends the particle 3 of the EPR-pair to Bob, and unites the other particle of the entangled pair with the unknown qubit state $|\Psi\rangle_1 \equiv \alpha|0\rangle_1 + \beta|1\rangle_1$ ($|\alpha|^2 + |\beta|^2 = 1$) that she wants to transmit to Bob. After this, she performs a Bell measurement on the (uncorrelated) particles 1 and 2, which projects onto one of the states of the $\mathcal{B}_{\mathrm{B}}$-basis (see Fig. 5). As this stage, the whole system's state can be written as follows:

$$|\Psi\rangle_1|\phi^+\rangle_{2,3} = \tfrac{1}{2}\Big[|\phi^+\rangle_{1,2}(\alpha|0\rangle_3{+}\beta|1\rangle_3) + |\psi^+\rangle_{1,2}(\alpha|1\rangle_3{+}\beta|0\rangle_3) + |\psi^-\rangle_{1,2}(\alpha|1\rangle_3{-}\beta|0\rangle_3) + |\phi^-\rangle_{1,2}(\alpha|0\rangle_3{-}\beta|1\rangle_3)\Big]. \quad (35)$$

(t_2) Next, Alice sends the result of her measurement, two classical bits of information, to Bob via a classical channel. These classical bits are represented by two straight lines in Fig. 5. Eq. (35) can then be rewritten as

$$\begin{aligned}|\Psi\rangle_1|\phi^+\rangle_{2,3} \;=\; & \tfrac{1}{2}\Big[|\phi^+\rangle_{1,2}|\Psi\rangle_3 + |\psi^+\rangle_{1,2}(\sigma_{\mathbf{x}})|\Psi\rangle_3 + \quad (36)\\ & |\psi^-\rangle_{1,2}(-i\sigma_{\mathbf{y}})|\Psi\rangle_3 + |\phi^-\rangle_{1,2}(\sigma_{\mathbf{z}})|\Psi\rangle_3\Big] ,\end{aligned}$$

where the σ_i operators are the Pauli matrices in the $\{|0\rangle, |1\rangle\}$ basis[8].

(t_3) After receiving Alice's classical information, Bob performs one of the following unitary operations [see Eq. (37)] in order to transform the state of his particle[9] into $|\Psi\rangle$:

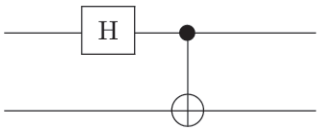
$$\begin{aligned}
|\phi^+\rangle_{1,2} &\longrightarrow I && \text{(do nothing)} ,\\
|\psi^+\rangle_{1,2} &\longrightarrow \sigma_{\mathbf{x}} && \text{(do bit flip)} ,\\
|\psi^-\rangle_{1,2} &\longrightarrow \sigma_{\mathbf{x}}\sigma_{\mathbf{z}} && \text{(do bit- and phase-flip)} ,\\
|\phi^-\rangle_{1,2} &\longrightarrow \sigma_{\mathbf{z}} && \text{(do phase flip)} . \qquad (37)
\end{aligned}$$

Hence, Bob only needs to apply one of the unitary transformations of Eq. (37), conditional on the outcome of Alice's measurement, in order to obtain the initial state $|\Psi\rangle$ of particle 1 on his qubit (particle 3). Thus, the process works without actual physical transportation nor previous knowledge of the state $|\Psi\rangle$. A few remarks regarding this teleportation process: i) The Bell measurement establishes a correlation between the two initially uncorrelated particles 1 and 2. The outcome of this measurement is completely random, as can be seen from Eq. (37). ii) The protocol is consistent with the no–cloning theorem, since the "copy" of the state $|\Psi\rangle$ obtained by Bob requires the previous Bell basis measurement of particles 1 and 2 which destroys the original state $|\Psi\rangle_1$. iii) Since Bob has to wait for a classical signal to be sent to him in order to perform the quantum state transmission, the process has not been accomplished faster than light.

Teleportation as a quantum circuit

Next, it is shown that the above quantum teleportation protocol can be described in terms of elementary gates for quantum computation. In order to implement the quantum operations needed for the description of the practical teleportation scheme proposed here, two elements are employed: i) the Hadamard gate H, and ii) the CNOT (measurement) gate. As explained in Section II, in the language of quantum circuits, qubits are denoted by horizontal lines ("wires"), and the above-mentioned gates are schematically represented as in Fig. (1), where the basis states $i, j = 0$ or 1. In addition, if the above set of gates is to be used for universal quantum computation, another single qubit gate, the *phase shift* $P(\varphi)$ gate must be introduced. This transforms: $|0\rangle \mapsto |0\rangle$, and $|1\rangle \mapsto \mathrm{e}^{i\phi}|1\rangle$, and is denoted as $|x\rangle \overset{\varphi}{—\!\!\bullet\!\!—}\ \mathrm{e}^{ix\varphi}|x\rangle$. The Hadamard and phase gates are sufficient to construct *any* unitary operation on a single qubit. Consequently, the Hadamard transform, all phase gates, together with the CNOT gate form an *universal* set of logic gates, i.e., any given n-qubit unitary transformation required in a certain quantum computation scheme can be exactly simulated with these gates (**Barenco,** *et al.,* 1995(A)). A pure state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbf{C}$, and $|\alpha|^2 + |\beta|^2 = 1$ is also introduced in this Hilbert space. The circuit notation is now used in order to provide a description of the quantum teleportation phenomenon in terms of quantum computation.

The *unitarity* of the Hadamard and the CNOT gates has interesting implications: consider the action of the following (Bell) circuit



This transforms the states of the (disentangled) computational basis of two qubits $\mathcal{B}_2$ into a set of maximally entangled states. This set is exactly the so-called Bell basis and, as we saw previously, is of fundamental relevance to quantum teleportation. As a result of the two-qubit register transformations of the circuit, we are left with the states:

$$|00\rangle \longmapsto \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\phi^+\rangle , \qquad (38)$$

$$|01\rangle \longmapsto \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv |\psi^+\rangle , \qquad (39)$$

$$|10\rangle \longmapsto \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv |\phi^-\rangle , \qquad (40)$$

$$|11\rangle \longmapsto \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv |\psi^-\rangle . \qquad (41)$$

[8] Recall that $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

[9] Note that originally ($t = t_0$), Bob's particle 3 was *maximally* entangled with particle 2.

Since the Hadamard transform is just a single qubit gate, it is obvious that the CNOT gate is the one responsible for the generation of the *entangled* basis $\mathcal{B}_{\text{B}} = \{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$. Interestingly, the same CNOT gate can be used to disentangle the Bell basis states: just apply the circuit $\text{CNOT}_{12}\text{H}_1$ to the $\mathcal{B}_{\text{B}}$-basis states and you shall end up with the disentangled basis $\mathcal{B}_2$! As discussed in Sec. II, this is because of the reversibility of this entangling gate. In an n-qubit register, the Schrödinger's cat state $|\Psi_{\text{N-CAT}}\rangle = \frac{1}{\sqrt{2}}\big(|00\ldots0\rangle_{1,\ldots,n} + |11\ldots1\rangle_{1,\ldots,n}\big)$ can be produced, for example, starting from the trivial input state $|00\ldots0\rangle_{1,\ldots,n}$, and then applying a sequence of $n+1$ CNOT gates (**Reina & Johnson,** 2000(D)).

Figure 6(a) shows the computational approach, which is based on the work reported in (**Brassard *et al.,*** 1998). As usual, two parties are referred to, Alice and Bob. Alice wants to teleport an arbitrary, unknown qubit state $|\Psi\rangle$ to Bob. Alice prepares two qubits in the state $|0\rangle$ and then gives the state $|\Psi 00\rangle$, as the *input* to the system. By performing the series of transformations shown in Fig. 6(a), Bob receives as the *output* of the circuit the state $\frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a)\frac{1}{\sqrt{2}}(|0\rangle_b + |1\rangle_b)|\Psi\rangle_c$. This circuit by itself is not a quantum teleportation machine, we next show how to transform it into a quantum teleportation device.

The circuit shown in Fig. 6(a) comprises the teleportation protocol given above. As before, this uses three qubits. The unitary transformations that are applied during the computation process in Fig. 6(a) (from left to right) are:

(t_1) Preparation of the input state: this is initialized as the direct product of the unknown state to be teleported, $|\Psi\rangle_1 = \alpha\,|0\rangle_1 + \beta\,|1\rangle_1$, and the basis state of qubits 2, and 3, $|00\rangle_{23}$.

(t_2) Realization of the first two quantum gates gives

$$\frac{1}{\sqrt{2}}\,(\,\alpha\,|0\rangle + \beta\,|1\rangle\,)\,(\,|00\rangle + |11\rangle\,) = \qquad (42)$$
$$\frac{1}{\sqrt{2}}\,(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle)$$

(t_3) The CNOT_{12} gate produces

$$\frac{1}{\sqrt{2}}\,(\,\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle\,) \qquad (43)$$

(t_4) After the Hadamard transform H_1 one gets

$$\frac{\alpha}{2}\,\{\,|000\rangle + |100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle\,\} + \qquad (44)$$
$$\frac{\beta}{2}\,\{\,|010\rangle - |110\rangle + |001\rangle - |101\rangle\,\}\ ,$$

which can be rewritten as

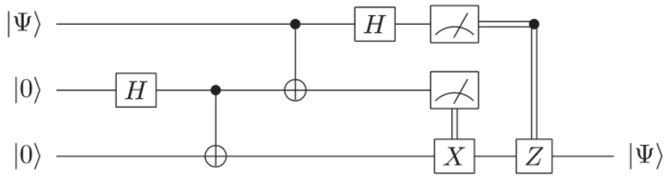
$$\tfrac{1}{2}\{|00\rangle\,(\,\alpha\,|0\rangle + \beta\,|1\rangle\,) + |01\rangle\,(\,\alpha\,|1\rangle + \beta\,|0\rangle\,) + \qquad (45)$$
$$|10\rangle\,(\,\alpha\,|0\rangle - \beta\,|1\rangle\,) + |11\rangle\,(\,\alpha\,|1\rangle - \beta\,|0\rangle\,)\} =$$
$$\tfrac{1}{2}\,\{\,|00\rangle\,|\psi\rangle + |01\rangle\,\widehat{\sigma}_x\,|\psi\rangle + |10\rangle\,\widehat{\sigma}_z\,|\psi\rangle + |11\rangle\,(\,-\boldsymbol{i}\sigma_y\,)\,|\psi\rangle\,\}$$

and we are done, since now we only need to make a measurement in the computational basis over qubits 1 and 2 (at the dashed line) and the outcome will reveal the transformation that Bob needs to perform over qubit 3 in order to obtain the desired quantum state $|\psi\rangle$. Note that for the circuit to work as a teleportation device: i) two bits of classical information have to be transmitted from Alice to Bob, and ii) we have used the computational basis $\mathcal{B}_2$ which can be significantly easier to realise in the laboratory than the Bell basis originally used in (**Bennett *et al.,*** 1993).

(t_5) If we were to perform the second part of the circuit (after the dashed line) the final result or outcome of the computation is given at the right hand-side of Fig. 6(a). This process, however, can be simplified if we notice that after Alice's measurement (at the dashed line), the four possible outcomes (left-hand side of Eq. (46)) explicitly indicate the route of action to be followed by Bob over his qubit (right-hand side of Eq. (46)) in order to recover Alice's original quantum state:

$$\begin{aligned}
|00\rangle &\longmapsto \widehat{\mathbb{I}}(\alpha\,|0\rangle + \beta\,|1\rangle) = |\Psi\rangle_3\\
|01\rangle &\longmapsto \widehat{\sigma}_x(\alpha\,|1\rangle + \beta\,|0\rangle) = |\Psi\rangle_3\\
|10\rangle &\longmapsto \widehat{\sigma}_z(\alpha\,|0\rangle - \beta\,|1\rangle) = |\Psi\rangle_3\\
|11\rangle &\longmapsto \widehat{\sigma}_z\widehat{\sigma}_x(\alpha\,|1\rangle - \beta\,|0\rangle) = |\Psi\rangle_3 \qquad (46)
\end{aligned}$$

This process can be summarised, in the language of quantum circuits, as shown below. Each 'detector box' and double line means, respectively, the measurement and communication of one bit of information:



In Fig. 6(b), the analysis of the teleportation process is extended to the case of a four qubit circuit (**Reina & Johnson,** 2000(D)). As before, Alice wants to teleport the state $|\Psi\rangle_1$ to Bob. She prepares three qubits in the state $|0\rangle$ and gives the state $|\Psi 000\rangle$ as the input to the system. From Fig. 6(b) it is clear that the function of the first three gates performed by Alice is to obtain the maximally entangled GHZ state $|\Psi_{\text{GHZ}}\rangle \equiv \frac{1}{\sqrt{2}}(|000\rangle +$

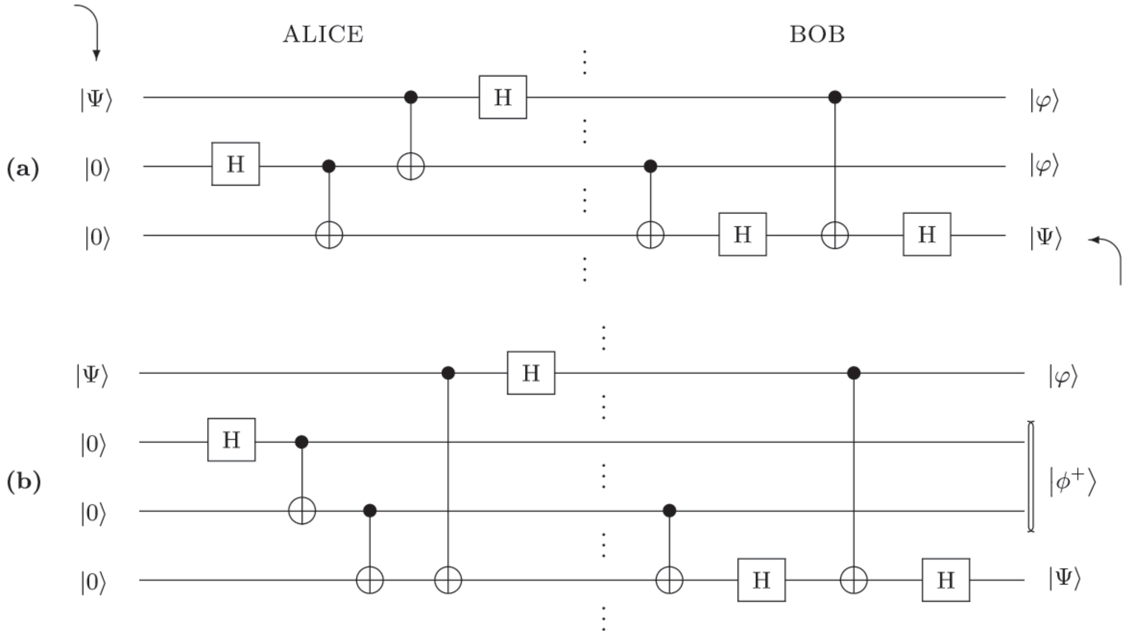


FIG. 6 Circuit schemes to teleport an unknown quantum state from Alice to Bob using an arrangement of (a) 3, and (b) 4 qubits. The method employs (a) Bell, and (b) GHZ states respectively.

$|111\rangle$) (**Greenberger *et al.*,** 1989). The next two gates realised by Alice (before the dotted line in Fig. 6(b)) leave the system in the state

$$\tfrac{1}{2}\Big\{|000\rangle(\alpha|0\rangle+\beta|1\rangle)+|011\rangle(\beta|0\rangle+\alpha|1\rangle)+ \\ |100\rangle(\alpha|0\rangle-\beta|1\rangle)+|111\rangle(-\beta|0\rangle+\alpha|1\rangle)\Big\}. \quad (47)$$

By performing the operations shown after the dotted line in Fig. 6(b), Bob gets as the output of the circuit the state $\frac{1}{\sqrt{2}}(|0\rangle_1+|1\rangle_1)|\phi^+\rangle_{2,3}|\Psi\rangle_4$. Again, for this to work as a teleportation circuit, we notice from Eq. (47) that a measurement (in the computational basis) of qubits 1 and 2 and its communication to Bob, who then realises a unitary transformation over qubit 4 (as detailed for the circuit of Fig. 6(a)), completes the process. A generalisation to the case of an n-QTC using Schrödinger's cat states is given in (**Reina & Johnson,** 2000(D)).

After the seminal work of (**Bennett *et al.*,** 1993), some remarkable experimental demonstrations of teleportation have been achieved. The first one (**Bouwmeester *et al.*,** 1997), teleported the polarization state of a photon by using an additional pair of entangled photons. Here, the measurement process explained above took place in such a way that the second photon (that of Bob) of the entangled pair acquired the polarization of the initial photon (that of Alice). The deterministic teleportation of a quantum state between two single material particles (trapped ions or atomic qubits) has now also been achieved (**Riebe *et al.*,** 2004; **Barrett *et al.*,** 2004). Remarkably, also the experimental quantum teleportation of a two-qubit composite system has been achieved (**Zhang *et al.*,** 2006).

The experimental teleportation between objects of a different nature—light and matter, which respectively represent flying and stationary media has also been reported (**Chen *et al.*,** 2008; **Sherson *et al.*,** 2006). In (**Sherson *et al.*,** 2006), a quantum state encoded in a light pulse is teleported onto a macroscopic object (an atomic ensemble of caesium atoms). Here, the authors point out that the use of a macroscopic atomic ensemble is relevant for the practical implementation of a quantum repeater. It is well known that an important factor for the implementation of quantum networks is that the teleportation between transmitter and receiver can be carried out over long distances. In this experiment, the distance achieved was 0.5 metres. The authors claim that their approach should be scalable to longer distances since their experiment uses propagating light to achieve the entanglement of light and atoms. In a more recent experiment, (**Chen *et al.*,** 2008) have achieved, following the spirit of the teleportation between light and matter states, a memory-built-in teleportation between photonic (flying) and atomic (stationary) qubits. They succeeded in teleporting an unknown polarization state of a single photon over a distance of 7 metres onto a remote atomic qubit that also served as a readable quantum memory. Interestingly, the teleported state was stored and successfully read out for up to 8 μs. As pointed out in (**Chen *et al.*,** 2008), the combination of quantum teleportation and quantum memory of photonic qubits paves the road for future implementations of large-scale quantum communication, and measurement-based quantum computation.

E. Dense coding

Classical information can be transmitted by means of a quantum channel, i.e., via the use of qubits. In principle, the task is very simple: if a sender, Alice, wants to transmit a classical binary string, say 0110, to a physically distant receiver Bob, via quantum means, she simply prepares the state $|0110\rangle$ and send it to Bob who can then extract the information by measuring the qubits in the $\mathcal{B}_1$-basis, therefore obtaining four bits of classical information, precisely the message sent by Alice. However, communicating one bit per qubit is obviously not the best thing that one can do with qubits. In fact, this way of sending classical bits is actually more expensive than sending them via a proper classical channel. It turns out, however, that the qubits offer an additional advantage over the classical bits: *one can communicate two classical bits by sending only one qubit*.

Once more, the trick relies on the possibility of generating entangled states: suppose Alice and Bob are given one particle each which has been previously prepared in the maximally entangled state $|\phi^+\rangle$. They don't know each other and have never interacted previously, before this entangled pair is given to them. Alice then can communicate to Bob two classical bits by sending him only one qubit. This is the so-called dense coding, an idea proposed by Bennett and Wiesner (**Bennett & Wiesner,** 1992; **Barenco & Ekert,** 1995). This is based on the fact that the four Bell-basis states can be projected onto the computational basis to convey two classical bits of information. This can clearly be seen in terms of the unitarity of the studied quantum logic gates. First, after receiving the qubit that Alice has sent to Bob, he performs $\text{CNOT}_{12}(|\phi^+\rangle)$, hence generating the disentangled state $|\psi_1\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$. Second, he realises the operation $H_1(|\psi_1\rangle)$, thus obtaining the state $|0\rangle_1\,|0\rangle_2$. From this output, qubit 1 is referred to as the *phase* bit (+ or −), and qubit two as to the *parity* bit (this tells whether the spins are aligned or anti-aligned: $|\phi\rangle$ or $|\psi\rangle$). Hence, a measurement of this output in the computational basis should give the result 00: Bob finishes with two classical bits of information. In the same way, by using any of the remaining states of the Bell-basis $|\phi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$, Bob should obtain the following two classical bits output: 10, 01, and 11 respectively; thus, in any case, transmitting two classical bits per qubit. Note that this process can be seen as a way of performing *secure communication*: the qubit trasmitted by Alice will convey two classical bits of information only if the receiver has the other qubit of the *apriori* distributed entangled pair. This is an example of the information content of quantum entanglement and the way it can be exploited for classical communication.

F. Quantum key distribution

Suppose that Alice and Bob now need to communicate an extremely confidential message, such that the information is not to be deciphered by a dangerous eavesdropper "Sal." This task can be accomplished with certainty only if Alice and Bob are allowed to share a private cryptographic *quantum key* K, a secret random bit string known only to them, in order to encode and protect the original message. The problem assumes that Alice and Bob have at their disposal a public classical channel, and a quantum channel that is insecure. Hence, the original problem of communicating a message has been converted into a cryptographic key exchange problem. This is often referred to in the literature as *quantum cryptography*.

As in the previous cases of entanglement-assisted communication, the key exchange can only be accomplished with certainty by means of quantum entanglement. It is to be added to this problem that Sal is an efficient eavesdropper: he can interact with the quantum information carriers used by Alice and Bob, and he can also tap, without disturbing, any classical communication that Alice and Bob may transmit during the process of sharing the private key. The quantum key distribution schemes are based on the no-cloning theorem, since, in contrast to the situation of classical communication, the message sent from Alice to Bob cannot be tapped and faithfully copied by an eavesdropper. Any 'excess' of Sal's eavesdropping should be easily detected by Alice and Bob, who can then abort the protocol and create a new key. Thus, any attempt by an eavesdropper to obtain relevant information about K and remain undetected should be negligible.

Let's see how to establish such a secured shared random key. Suppose that Alice and Bob share a supply of entangled (singlet) Bell states $|\psi^-\rangle$. Then, they perform the following protocol. Alice and Bob measure either σ_x or σ_z over each qubit they have[10]. Hence, each choice

[10] Here, σ_i denote the Pauli matrices. These are single qubit transformations that can be used for phase shifting and flipping the qubits of the Bell basis: i) Apply σ_z to qubit 1: $|\phi^+\rangle \leftrightarrow |\phi^-\rangle$,

occurs with probability 1/2. Once these measurements are performed, the observables they measure are publicly announced, but the obtained outcomes are not revealed. If their qubits are measured along different axes, the outcomes are uncorrelated, hence Alice and Bob discard their results. In contrast, if their qubits are measured along the same axis, their results, though random, are perfectly correlated, thus establishing a shared random key. It is easy to check that this protocol is robust against Sal's attacks to the quantum information carriers, where he can try, for example, to entangle his qubits with those transmitted between Alice (A) and Bob (B) and then perform a measurement of his qubits (after knowing the results announced by Alice and Bob). The result is that Sal (S) does not obtain any significant information from Alice's and Bob's and his own measurement results. Hence, the generated random key K is secure.

To see why this is so, suppose that Sal has indeed attacked the quantum channel in order to extract information from that of Alice and Bob. The most general possible state that describes A, B, and the intervention of S can be written as

$$\begin{aligned} |\aleph\rangle_{ABS} \;=\; & |00\rangle_{AB}\,|e_{00}\rangle_S + |01\rangle_{AB}\,|e_{01}\rangle_S + \\ & |10\rangle_{AB}\,|e_{10}\rangle_S + |11\rangle_{AB}\,|e_{11}\rangle_S \;, \end{aligned} \tag{48}$$

where we can imagine the states e_{ij} as the states of a surrounding environment—Sal (see Section IV). As $|\psi^-\rangle$ is an eigenstate of both $\sigma_x^A\sigma_x^B$, and $\sigma_z^A\sigma_z^B$ (eigenvalue -1), hence Alice and Bob can verify that effectively $\sigma_z^A\sigma_z^B = -1$ (the phase bit). Then, they must have

$$|\aleph\rangle_{ABS} = |01\rangle_{AB}\,|e_{01}\rangle_S + |10\rangle_{AB}\,|e_{10}\rangle_S \;, \tag{49}$$

and $\sigma_x^A\sigma_x^B = -1$ (the parity bit), which implies

$$|\aleph\rangle_{ABS} = \tfrac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})\,|e\rangle_S \;. \tag{50}$$

Comparing Eqs. (48), (49), and (50), it is clear that Sal's qubits must be unentangled from Alice's and Bob's if their pair (or any of the Bell-basis) is to be an eigenstate of $\sigma_i^A\sigma_i^B$, $i = x, z$. This means that despite Sal's efforts, the shared key is safe: even his knowledge of quantum mechanics does not allow him to learn anything about the secret random key! In contrast, if Alice and Bob measure a part of the shared key and find that the results are not perfectly correlated, then Sal may have been successful, in which case they have to abort this key and try to generate a new secure one. Once more, it is evident that the capability to successfully perform a quantum key distribution protocol relies on the generation and distribution at will of particles in a highly entangled pair (**Ekert,** 1991; **Bennett *et al.*,** 1992(B); **Bennett *et al.*,** 1992(A)). Any state of the Bell-basis could serve for this purpose.

This is not the only available quantum protocol. In fact, the so-called BB84 protocol of Brassard and Bennett (**Bennett & Brassard,** 1984) does not require the entangled pairs to be shared by Alice and Bob: here, Alice can prepare the pairs herself, from which she measures one qubit of each pair and sends the other qubit to Bob. Then Bob can measure and verify his results with Alice as explained above. This scheme is as secure as the former. The corresponding security proofs can be found in Refs. (**Mayers,** 1998; **Lo & Chau,** 1999). The effects of the insecurity of the quantum channel can also affect the results of Alice's and Bob's measurement. However, it can be shown that the errors due to possible imperfections in the channel can be distinguished from the errors that occur because of Sal's eavesdropping (**Mayers,** 1998; **Lo & Chau,** 1999). Experimental demonstrations of quantum key distribution are far more advanced than any other QIP task. For an account of the main experimental achievements in this subject see, e.g., Refs. (**Bennett & Brassard,** 1989; **Hughes *et al.*,** 1995; **Phoenix & Townsend,** 1995; **Gisin *et al.*,** 2002).

G. Quantum data compression

A qubit is a useful measure of quantum information content. Jozsa and Schumacher have shown that given a system of n qubits, it is possible to find a subspace of Hilbert space in which one can describe any state vector of the system, and that the dimension of this subspace is $2^{nS(\rho)}$, for $S(\rho) < 1$ (**Schumacher,** 1995; **Jozsa & Schumacher,** 1994). Hence, only $nS(\rho)$ qubits are required to represent the quantum information content, where $S(\rho)$ is the von Neumann entropy of the quantum source,

$$\begin{aligned} S(\rho) \;&=\; -\,\mathrm{Tr}\rho\log_2\rho \;, \\ \rho \;&=\; \sum_i p_i\,|\Psi_i\rangle\,\langle\Psi_i| \;. \end{aligned} \tag{51}$$

Here, ρ is the density matrix representing the system, $|\Psi_i\rangle$ are the states trasmitted by the source and p_i their probability of transmission. The von Neumann entropy is a measure of the minimum asymptotic number of qubits that are required to compress the initial state of a system that is to be faithfully transmitted and finally recovered

and $|\psi^+\rangle \leftrightarrow |\psi^-\rangle$. ii) Apply σ_x to qubit 1: $|\phi^+\rangle \leftrightarrow |\psi^+\rangle$, and $|\phi^-\rangle \leftrightarrow -|\psi^-\rangle$. The Bell-basis states can be characterized as the simultaneous eigenstates of the commuting observables $\sigma_x^A\sigma_x^B$, and $\sigma_z^A\sigma_z^B$, where the eigenvalue of $\sigma_x^A\sigma_x^B$ is the parity bit, and the eigenvalue of $\sigma_z^A\sigma_z^B$ is the phase bit. These operators can in principle be measured simultaneously.

by a decoder. As can be seen, $nS(\rho) < n$, hence the name quantum data compression.

This is to be compared with classical data compression, where redundant data can also be compressed and then faithfully decoded. The main difference between the two is that classical compression has allowed only orthogonal states, while *any* superposition of states is allowed quantum-mechanically. Hence, a general quantum compression that involves non-orthogonal states does not have any classical analogue. In fact, if the quantum states to be compressed and transmitted are non-orthogonal, the encoder cannot make a copy of them because of the no-cloning theorem. The snag here is that a practical implementation of these 'compressions' and 'decodings' is extremely demanding. As pointed out in Ref. (**Steane,** 1998), this is the ultimate compression allowed by the laws of physics.

H. Quantum algorithms and quantum games

Quantum algorithms

Deutsch's *quantum parallelism* is an outstanding property of a quantum computer. It points out that a quantum computer can perform certain computational tasks faster than any modern digital computer. This was rigorously stated in the 'Deutsch problem,' whose solution gave birth to the first quantum algorithm, the so-called Deutsch-Josza algorithm (**Deutsch & Jozsa,** 1992), where the interplay between interference effects and quantum entanglement gives rise to a celebrated speed up of the quantum computational process: this leads to an exponential gap between the complexity class of the quantum problem and the corresponding complexity class of the classical problem. In other words, the quantum parallelism leads to the solution of problems that are otherwise intractable by any classical means. After Deutsch's, other quantum algorithms have been discovered, the most remarkable one being Shor's algorithm for efficient factorisation of large numbers (**Shor,** 1994; **Shor,** 1996; **Ekert & Jozsa,** 1996). This finding is one of the main breakthroughs in the subject of quantum information theory. It established a solution to a problem that, from the complexity point of view, was thought to be intractable, and brings practical uses as a byproduct, because it is exactly the same difficulty of factoring a large number that holds up modern schemes for public key cryptography, such as the RSA scheme (**Rivest *et al.*,** 1978; **Cocks,** 1973). Other relevant algorithms are those of Simon (**Simon,** 1994), and Grover's search algorithm (**Grover,** 1997). A common element to all these algorithms is the use of the quantum parallelism property, where the linear superposition principle plays a remarkable role when extracting a 'global' information of a given function f. In this section we shall concentrate on a generalisation of Deutsch's algorithm (**Deutsch & Jozsa,** 1992; **Cleve *et al.*,** 1998). A detailed analysis of Shor's algorithm can be found in Ref. (**Ekert & Jozsa,** 1996).

Generalised Deutsch's problem: Suppose we are given a device *oracle* that computes the Boolean function $f : x \in \{0,1\}^n \rightarrow f(x) \in \{0,1\}$ that takes any n-binary string x as input and produces a single bit $f(x) \in \mathcal{B}_1$ as output, in a single step. The problem assumes that the function f is either *constant* or *balanced* depending on whether the result of the 2^n possible evaluations gives the same output (0 or 1) or a situation where half of them are 0's and the other half 1's. The problem is to determine whether f is constant or balanced (we previously analysed the simplest case $n = 1$, where $f(0) = f(1)$ or $f(0) \neq f(1)$, in Subs. II(B)).

Before we give the solution to this problem, let us first analyse its complexity class: if we attempt to solve this problem with a classical computing device in the worst possible scenario, we shall have to call the oracle $2^{n-1} + 1$ times. Thus, the number of oracle queries grows exponentially with n. But there is a much cleverer way to solve this problem. In doing so, we start by replacing the classical oracle "f" with a quantum oracle $\mathcal{U}_f$ which performs the unitary transformation $\mathcal{U}_f : |x\rangle |a\rangle \rightarrow |x\rangle |a \oplus f(x)\rangle$ in a single step, where $|x\rangle$ is an n-qubit state (input) such as the one given in Eq. (2), and $|a\rangle$ is an ancilla single qubit state ($a \in \mathcal{B}_1$). Thus, the solution of Deutsch's problem is straightforward: Suppose the n-QR and the ancilla are initialised in the states $|x\rangle = |0\rangle^{\otimes n}$, and $|a\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Next, perform the following protocol:

1. Apply the Hadamard transform H to $|x\rangle$. This leads to the state

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle (|0\rangle - |1\rangle) \ . \qquad (52)$$

   For the sake of clarity, the qubit $|x\rangle$ is explicitly given in Eq. (2).

2. Apply the quantum oracle to the quantum register: $\mathcal{U}_f(|\Psi_1\rangle)$. This yields

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) \ . \qquad (53)$$

3. Next, perform a measurent to determine whether f is constant or balanced. This measurement can be realised as follows: Apply the Hadamard transform to all of the first n-qubits of the register given by Eq. (53). This yields

$$|\Psi_3\rangle = \frac{1}{2^{n+\frac{1}{2}}} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)+(x\cdot y)} |y\rangle \left(|0\rangle - |1\rangle\right) . \quad (54)$$

This reduces the measurement problem to that of finding whether or not the first n qubits are in the state $|0\rangle$, thus solving Deutsch's problem.

The effect of the Hadamard transform over an arbitrary n-QR in a given state $|x\rangle$, $x \in \{0,1\}^n$, is

$$|x\rangle \;\mapsto\; \frac{1}{2^{n/2}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle \ , \qquad (55)$$

where the product $x \cdot y = (x_{n-1}y_{n-1} + \ldots x_1y_1 + x_0y_0)$. Here, $j = (j_{n-1}, \ldots, j_0)$, $j = x, y$. For example, if $|x\rangle = |010\rangle$, hence $H(|x\rangle) \equiv \frac{1}{2^{3/2}}\{|000\rangle + |001\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle - |111\rangle\}$.

To see why the third step solves the problem, note that the probability of finding the system's output $|\Psi_3\rangle$ in the initial state $|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |a\rangle$ is

$$\frac{1}{2^{2n}}\left| \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \right|^2 = \begin{cases} 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases} \qquad (56)$$

The term inside the delimiters gives $2^n(-1)^{f(0\cdots 0)} = \pm 2^n$ when f is constant. Thus, a measurement of the first n qubits output determines with a 100% success rate whether f is constant or balanced. As said, this is actually a generalisation of Deutsch's algorithm, which originally gave only a 50% of probability of success when solving this problem (**Cleve *et al.*,** 1998).

It is remarkable what has been done using this algorithm: its massive quantum parallelism led to the computation of all the 2^n possible values of $f(x)$ in one single run. This arises from the fact that the quantum oracle can perform its task for any linear combination of possible basis states in a single step: this is to be physically identified as an interference pattern. As to the complexity class of this quantised problem, we require only $O(n)$ steps to obtain the final answer. Hence, if we compare this result with that of the classical complexity class, it is found that Deutsch's algorithm leads to an *exponential speedup* of the computations. This is a wonderful property that only a quantum computer can provide.

Deutsch's and Grover's algorithms have been implemented in bulk liquid NMR experiments but only for a few qubit register (**Jones *et al.*,** 1998(A); **Jones & Mosca,** 1998(B)). More recently, there has been the more demanding implementation of Shor's factoring algorithm, also using NMR quantum computation. This has been done in the simplest scenario: factorisation of the number $N = 15$, by using $n = 7$ qubits (**Vandersypen *et al.*,** 2001).

Next, we examine very briefly the subject of game theory, and discuss the role that quantum computation may play when the players of a given 'game' are allowed to play "quantum strategies."

Quantum games

Game theory is a well established branch of mathematics whose tools and formalism, mainly developed by J. von Neumann (**von Neumann & Morgenstern,** 1953), aims to solve the conflict between two or more competing parties (players) that hold particular interests. This has a vast range of applications in many different subjects such as social sciences, biology, and economics[11]. By contrast, quantum game theory (**Meyer,** 1999; **Meyer,** 2000; **Eisert *et al.*,** 1999; **Eisert & Wilkens,** 2000; **Benjamin & Hayden,** 2001(A); **Benjamin & Hayden,** 2001(B)) has been born from motivations regarding QIP, where information has been recognised as a physical quantity. The usefulness of quantum games for 'practical applications' goes back to the idea that many physical, chemical, and biological quantum processes can be thought of as games.

The initial motivation is the recognition of new effects without classical analogue, which are associated with the quantum character of the 'games'. For example, a two-player game (**Meyer,** 1999; **Meyer,** 2000; **Eisert *et al.*,** 1999; **Eisert & Wilkens,** 2000) can show a vanishing of 'predominant strategies' when the allowed 'moves' are made quantum-mechanically: these strategies should reappear only under the degrading of the quantum coherence (**Meyer,** 1999; **Meyer,** 2000; **Eisert *et al.*,** 1999; **Eisert & Wilkens,** 2000). For multi-player quantum games (**Benjamin & Hayden,** 2001(A); **Benjamin & Hayden,** 2001(B)), it has been shown that when the resources controlled by competing agents are entangled, they can cooperate to perfectly exploit the 'game' (**Benjamin & Hayden,** 2001(A); **Benjamin & Hayden,** 2001(B)). This has been performed for multi-player quantum games in the cases of the "Minority game," and a game analogous to "Prisoner's Dilemma" (**Benjamin & Hayden,** 2001(A); **Benjamin & Hayden,** 2001(B)), with the interesting result that such games can exhibit forms of 'coherent' quantum equilibrium[12] which have no analogue in classical games, or even in two-player quantum games. Thus, quantum players can exploit their

[11] See, e.g., http://www.unifr.ch/econophysics/minority/.

[12] An equilibrium is understood here as a set of strategies, such that neither player can improve his probability of winning by changing his strategy while the others do not.

moves highly efficiently through the use of collaborative strategies.

Because of the computational and physical rewards when performing both quantum algorithms and quantum games, one might be tempted to try to establish a common framework that yields a connection between the two. Many situations in nature, e.g., in biology, can be thought of as games where the competing agents try to establish a strategy that allows them to maximise their pay-off (e.g., their energy efficiency). In this respect, quantum algorithms may play an important role. They could be viewed, for instance, as games played between classical and quantum agents (**Meyer,** 1999; **Meyer,** 2000). One can imagine that a deeper understanding of the underlying structure of certain "quantum strategies" for performing quantum games may lead to the possibility of finding a different approach to gain insight into some fundamental physical and chemical processes in the quantum regime. One may think, for example, of the decoherence phenomenon as a *dynamic* multi-agent quantum game where at any given time t, we ask whether or not a given quantum register has been driven by an "environment strategy" to a situation where the QR coherence is lost. From a QIP perspective, we would like to find a way to play this game such that the registers answer is always "no." This example is in contrast with the above proposals (**Meyer,** 1999; **Meyer,** 2000; **Eisert *et al.*,** 1999; **Eisert & Wilkens,** 2000; **Benjamin & Hayden,** 2001(A); **Benjamin & Hayden,** 2001(B)), where the quantum games are played 'statically,' in the sense that they are played only once, and hence there is no record of the players history. Dynamical quantum games should be an interesting issue to address in the future, in particular because it could give rise to a new view of addressing *quantum memory effects*, and hence of understanding decoherence. Currently, there is an intense search to find new quantum algorithms. Finding new elements of the repertoire of the advantages of a quantum computer over its classical counterpart would bring, along with the possible development of novel quantum strategies, new insight into the understanding of basic processes in the interdisciplinary field of QIP.

The developments that came after the discovery of efficient quantum algorithms call for the need to solve another outstanding matter: the stabilisation problem. It is clear that environmental influences disturb the quantum computers capability of generating reliable quantum interference and quantum entanglement, hence destroying the possibility of performing arbitrarily complex quantum computations such as quantum algorithms. Fortunately, it was shortly shown afterwards, by Shor (**Shor,** 1995) and Steane (**Steane,**1996(A); **Steane,** 1996(B); **Steane,** 1996(C)), that quantum error-correcting codes exist, thus alleviating this situation. Next, the environmental problem mentioned above, and possible ways to overcome it, including fault-tolerant quantum computation itself, shall be briefly discussed.

IV. QUANTUM DECOHERENCE AND QUANTUM ERROR CORRECTION

The list of quantum hardware requirements to build a quantum computer presented in Section II possess a common difficulty. This is the problem of stability, which spoils the unitarity of the register evolution, and hence compromises the usefulness of any given computational task. It can be defined by two main ingredients: *noise*, the coupling that may exist between the state of the computer and its surrounding environment, and *imprecision*, the inaccuracy with which elementary quantum gates are performed in an arbitrarily complex computation (**Preskill,** 1998). As has been discussed, in order to perform quantum computations, a *coherent* evolution of the qubits is required. Noise causes the quantum computer to evolve from a pure quantum state to a statistical mixture of quantum states that exhibit no phase difference between them, the so-called *decoherence* (**Zurek,** 1991). Thus, decoherence implies that two of the main properties of a quantum computer, say, i) the capability to maintain superpositions of its states, i.e., to perform quantum interference reliably, and ii) the capability to reliably perform entanglement between its qubits, are lost during a given computational process. This can be illustrated by stating that, e.g., if $|S\rangle$ is a superposition of states $|\Phi_i\rangle$ of the quantum computer, say

$$|S\rangle = \tfrac{1}{\sqrt{2}}(|\Phi_1\rangle + \mathrm{e}^{i\varphi}\,|\Phi_2\rangle)\ , \tag{57}$$

then, a *coherent* evolution of the QC state requires that the $|\Phi_i\rangle$'s *and* the phase φ of the superposition remain unchanged by both noise and imprecision[13]. In practice, these criteria are very difficult to match. It is easy to see that an imprecise operation could result in a rotation of the state such that the phase φ becomes undefined. Also, and perhaps more stringent, is the fact that the coupling of $|S\rangle$ to the environment can result in a state

[13] This can be seen in the case of quantum entanglement as follows: suppose that the state $|S\rangle$ is created in an entangled state, say $|\Phi_1\rangle = |01\rangle$, $|\Phi_2\rangle = |10\rangle$, and $\varphi = \pi$ (the singlet state $|01\rangle - |10\rangle$). Hence, its phase bit ("$-$") and its parity bit (spin states are antialigned, "$|\psi\rangle$") should be guaranteed throughout the computational process if the system is to evolve coherently.

of the type $\frac{1}{\sqrt{2}}(|\Phi_1\rangle\,|e_1\rangle + \,\mathrm{e}^{i\varphi}\,|\Phi_2\rangle\,|e_2\rangle)$, which also affects the phase φ when the states of the environment $|e_i\rangle$ become orthogonal, i.e., when $\langle e_1|e_2\rangle \to\ 0$. This system-environment coupling—decoherence—results in a leakage of the information such that superpositions of the system's states evolve into entanglements with the environmental degrees of freedom, thus spoiling the unitarity of the evolution.

In the case of a spin half quantum (qubit) system, where $|S\rangle$ can be represented as a general state $\alpha\,|0\rangle + \beta\,|1\rangle$, the qubit-environment interaction leads, in the worst scenario, to a state of the type

$$|e_i\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) \;\to\; \alpha\,(c_{00}\,|e_{00}\rangle\,|0\rangle + c_{01}\,|e_{01}\rangle\,|1\rangle) + \beta\,(c_{10}\,|e_{10}\rangle\,|1\rangle + c_{11}\,|e_{11}\rangle\,|0\rangle)\,,$$

where $|e_i\rangle$ is the initial state, $|e_{ij}\rangle$ are the final states of the environment (not necessarily orthogonal), and c_{ij} are noise coefficients. It is interesting that this evolution can be rewritten as

$$|e_i\rangle\,|S\rangle \to \{|e_{_I}\rangle\,I + |e_x\rangle\,\sigma_x - i\,|e_y\rangle\,\sigma_y + |e_z\rangle\,\sigma_z\}\,|S\rangle\,, \tag{58}$$

where $|S\rangle$ is the initial state of the qubit, $e_{_I} = c_{00}\,|e_{00}\rangle + c_{10}\,|e_{10}\rangle$, $|e_x\rangle = c_{01}\,|e_{01}\rangle + c_{11}\,|e_{11}\rangle$, and so on. The Pauli operators σ_i, and the identity I, are written in the computational basis B_1. Recall that $-i\sigma_y = \sigma_x\sigma_z$. It follows from the Pauli matrices in Eq. (58) that the errors involved on each qubit are basically of three types: "*bit flip*" (σ_x) errors, "*phase flip*" (σ_z) errors, or "*bit/phase flip*" ($\sigma_x\sigma_z$) errors (**Steane,** 1996(A); **Steane,** 1996(B); **Steane,** 1996(C)). Thus, the problem of qubits error correction is reduced to the problem of correcting the above-mentioned errors. In these terms, the physical processes of phase decoherence and spontaneous emission can be stated as:

i. *Phase decoherence*: $(\alpha\,|0\rangle + \beta\,|1\rangle)\,|e\rangle \;\to\; \alpha\,|0\rangle\,|e_0\rangle + \beta\,|1\rangle\,|e_1\rangle$. This is given by $\{\ |e_{_I}\rangle, |e_z\rangle \neq 0,\quad |e_x\rangle = |e_y\rangle = 0,\quad \langle e_{_I}|e_z\rangle = 0\ \}$.

ii. *Spontaneous emission*: $(\alpha\,|0\rangle + \beta\,|1\rangle)\,|e\rangle \to \alpha\,|0\rangle\,|e_0\rangle + \beta(|1\rangle\,|e_1\rangle + |0\rangle\,|e_2\rangle)$, $\langle e_{_1}|e_2\rangle = 0$. This is given by $\{\ |e_x\rangle = -\,|e_y\rangle\,,\quad \langle e_x|e_{_I}\rangle = -\langle e_x|e_z\rangle,\quad \langle e_{_I}|e_z\rangle = \langle e_x|e_x\rangle\ \}$. If Γ is the spontaneous emission rate, it is found that $\langle e_x|e_x\rangle = \langle e_y|e_y\rangle = \langle e_z|e_z\rangle = \frac{1}{4}(1-\mathrm{e}^{-\Gamma t})$, and $\langle e_{_I}|e_{_I}\rangle = \frac{1}{4}(1+3\mathrm{e}^{-\Gamma t})$.

This latter process is referred to in the NMR literature as the T_1 (relaxation) process, and the former as the T_2 (dephasing) process. In any case, it is clear that the decoherence interaction entangles qubits with the environment. To visualise, e.g., the case of *phase decoherence*, it is useful to write the qubit evolution in terms of its density matrix operator. Thus, tracing out the environment states yields the evolution

$$\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \;\longrightarrow\; \begin{pmatrix} |\alpha|^2 & \alpha\beta^*\langle e_0|\,e_1\rangle \\ \alpha^*\beta\langle e_1|\,e_0\rangle & |\beta|^2 \end{pmatrix}\,, \tag{59}$$

where the off-diagonal elements "*coherences*," vanish for $\langle e_0|e_1\rangle \to 0$, in agreement with item (i). This is the origin of the term *decoherence*. Now that the problem has been identified, it is necessary to find a way to avoid or correct decoherence. In so doing, there is a powerful though counter-intuitive method: quantum error correction. By using this technique, a quantum computer is able to compute an arbitrary number of quantum logic gates—a complex quantum interference network—and produce the right answer even though the qubits in the computer relax spontaneously many times during the computational process (**Steane,** 1996(A, B, C)). To understand why this is so, let's start by noting that the principles of quantum error correction (QEC) are based on two main elements: the quantum states to be processed and the type of noise to be corrected. In order to describe the method, we follow (**Steane,** 1996(A, B, C)).

Suppose the coupling between an m-quantum system (Q) and its environment (E) is described by

$$|e\rangle\,|\Phi\rangle \;\longrightarrow\; \sum_s |e_s\rangle\,M_s\,|\Phi\rangle\ \ , \tag{60}$$

where $|e\rangle$ ($|\Phi\rangle$) is the initial state of the environment (system). The action of the "error operators" M_s on the system is unitary. These M_s's are a tensor product of operators (one for each qubit of the whole register) that belong to the set $\{I, \sigma_x, -i\sigma_y, \sigma_z\}$. The final states of the environment $|e_s\rangle$ need not be orthogonal nor normalised, and it is clear that the noise process of Eq. (60) is irreversible because the environment cannot be controlled. To perform QEC, the system Q has to be coupled to another system "ancilla" (a), which is composed of $n-m$ qubits in the definite state $|0\rangle_a$ (the whole register "$Q{+}a$" contains n qubits). The interaction A between Q and a, the *syndrome extraction*, is unitary and satisfies

$$A(|0\rangle_a\,M_s\,|\Phi\rangle) = |s\rangle_a\,M_s\,|\Phi\rangle\quad \forall\ M_s \in \mathcal{S}\ . \tag{61}$$

Here, the ancilla states $|s\rangle_a$ are mutually orthogonal, and the syndrome s gives us information (bits) about the kind of noise the register is experiencing. The set $\mathcal{S}$ is the set of error operators M_s for which syndrome extraction works—the set of correctable errors. This depends on the encoding: a central part of QEC is to find the best syndrome extraction operators (**Steane,** 1996(A, B, C); **Knill & Laflamme,** 1997).

Next, the syndrome extraction A is applied to the composite noisy-ancillary "$Q + E + a$" state. This yields

$$A\left\{\sum_s |e_s\rangle\, |0\rangle_a\, M_s\, |\Phi\rangle\right\} \;\longrightarrow\; \sum_s |e_s\rangle\, |s\rangle_a\, M_s\, |\Phi\rangle \ . \tag{62}$$

The next step is remarkable: by measuring the ancilla state in the $\{|s\rangle_a\}$-basis, the ancilla is projected onto one particular state $|s\rangle_a$, and the outcome value s becomes known to us. Thus, the whole system "$Q+E+a$" is projected onto the state $|e_s\rangle\, |s\rangle_a\, M_s\, |\Phi\rangle$, where s is known. Furthermore, from the measurement result (value of s), one can identify the operator M_s[14], thus applying M_s^{-1} to "$Q+a$" in order to obtain the final state[15]

$$|e_s\rangle\, |s\rangle_a\, |\Phi\rangle \ . \tag{63}$$

This means that our problem has been solved: *the original (noise-free) state $|\Phi\rangle$ has been recovered.* Note: i) After the syndrome extraction operation, the ancilla state $|s\rangle_a$ depends on the noise but not on the quantum state to be corrected (see Eq. (61)). ii) After the projective measurement, instead of the general noise of Eq. (60), one is left with only one error operator, M_s, which is now known to us. iii) The ancilla a can be again prepared in the state $|0\rangle_a$ for further corrections, thus allowing the quantum computer to overcome decoherence and perform further complex computations. iv) The last step, measure of the ancilla, can be avoided: this can be accomplished by defining another unitary interaction, namely C, that acts between Q and a (after the syndrome extraction) as follows $C(|s\rangle_a\, |\Phi\rangle) = |s\rangle_a\, M_s\, |\Phi\rangle$. Then the final state of the whole register becomes $|\Phi\rangle \sum_s |e_s\rangle\, |s\rangle_a$, thus transferring the "$Q+E$" entanglement onto an "$a+E$" entanglement (this procedure is illustrated in the Example 2; Appendix C.2).

The unitary operation that completes the QEC process, namely *recovery* "$\mathcal{R}$," in general establishes that for any $|\delta\rangle\,, |\delta_s\rangle \in$ "$E+a$", $\mathcal{R}(|\delta\rangle\, M_s\, |\Phi\rangle) = |\delta_s\rangle\, |\Phi\rangle$. In this sense, the main goal of QEC is to identify the set $\{|\Phi\rangle\}$, and the syndrome extraction A, in order to correct the noise introduced by M_s. In so doing, it suffices to find an orthonormal set of recoverable states (a subspace of Hilbert space) to be able to have a recoverable Hilbert space "$\mathcal{RH}$". Thus, QEC can be viewed as a *projection* of Hilbert system's space onto the recoverable Hilbert space. A *quantum codeword* $\{|j\rangle\}$ is a set of orthonormal quantum states that spans $\mathcal{RH}$. It turns out that A and $\mathcal{R}$ are possible if and only if the codewords satisfy $\langle j|\, M_m^\dagger M_n\, |k\rangle = 0$, and $\langle j|\, M_m^\dagger M_n\, |k\rangle = \langle k|\, M_m^\dagger M_n\, |j\rangle$, $\forall\ M_s \in \mathcal{S}$, and $\langle j|k\rangle = 0$ (**Knill & Laflamme,** 1997); see Example 1 given in Appendix C.1. For concrete examples of QEC code constructions, see, e.g., (**Shor,** 1995; **Steane,** 1996(A, B, C); **Calderbank & Shor,** 1996; **Laflamme *et al.*,** 1996); see Example 2, Appendix C.2.

In Examples 1 and 2, the used codewords only allowed for the correction of either bit-flip (σ_x) or phase-flip (σ_z) errors. A general method that protects against a more general noise, say a combination of σ_x, σ_z, and $\sigma_x\sigma_z$ errors, has been described in (**Steane,** 1996(A, B, C); **Calderbank & Shor,** 1996; **Knill & Laflamme,** 1997), and is based on the 'dual code theorem.' Here, the essential point is to note that

$$\tilde{H} \sum_{i\in C} |i\rangle = \frac{1}{\sqrt{2^k}} \sum_{i\in C^\perp} |i\rangle \ , \tag{64}$$

where $\tilde{H} \equiv H_1H_2H_3\cdots H_n$ is the Hadamard transform applied to all the members, say n states, of a linear classical error correcting code C (**Steane,** 1996(A, B, C)). The observation is that the action of $\tilde{H}$ over C produces another linear classical error-correcting code, the superposition of all the members of the dual code $C^\perp$. The dual $C^\perp$ is defined as the set of all vectors v such that $v \cdot u = 0\ \forall u \in C$. Hence, as long as both C and $C^\perp$ have good classical error correction properties, it can be shown that it is possible to correct both σ_x and σ_z errors (and hence errors involving the two of them, i.e., $\sigma_x\sigma_z$) by using states of the type given in Eq. (64). For more details of this code construction, the reader is referred to (**Steane,** 1996(A, B, C); **Calderbank & Shor,** 1996); see Example 3, Appendix C.3.

In conclusion, the method of QEC is mainly a matter of finding sets of states $|\Phi\rangle$, and the syndrome extraction A that allows one to suppress the influence of noisy environments M_s. Most of this work has been done by revisiting existing classical error-correcting codes. The theory of quantum error-correcting codes has been established within a general framework in (**Knill & Laflamme,** 1997). Quantum error-correction and stabilisation schemes have been built on the work of Shor (**Shor,** 1995), Steane (**Steane,** 1996(A, B, C)), Calderbank and Shor (**Calderbank & Shor,** 1996), and the later work reported in (**Ekert & Macchiavello,** 1996; **Laflamme *et al.*,** 1996; **Gottesman,** 1996; **Calderbank *et al.*,** 1997). There is an important issue that has been left out of the discussion presented above: the effect of the proper quantum gates, ancilla, and measurements realised by the QEC method. How perfect must they be in order to do a proper job of error correction instead of introducing further noise and imprecision to the system $Q+a$? Fortunately, the answer to this problem has been dealt with satisfactorily in what has been termed fault-tolerant QEC (**Shor,** 1997; **Kitaev,** 1997; **Steane,** 1997;

[14] This is because s is in a one-to-one correspondence with M_s.

[15] The transformation M_s^{-1} is accomplished by means of a sequence of single qubit quantum gates originated from the set $\{\sigma_x$, σ_z or $-i\sigma_y\}$.

Preskill, 1998). It was initially proposed by Shor (**Shor,** 1997) and Kitaev (**Kitaev,** 1997), and the central idea was to perform a convenient design of all the required logic gates where the evolving states are verified wherever possible, and the syndrome extraction repeated. In this way it is guaranteed that the QEC method "corrects more noise than it introduces." These ideas have been conveniently reviewed in (**Preskill,** 1998), where it has been estimated that a requirement for reliable quantum fault-tolerant computation is that the quantum hardware used in the computations must have a decoherence per qubit per gate below a finite threshold. This has been estimated at 10^{-5} to 10^{-2} (**Steane,** 1997; **Preskill,** 1998) . In addition, fault-tolerant computation allows a quantum computer that is built from qubits that undergo spontaneous emission decay with lifetime τ_{rel} to perform a complex quantum computation: the quantum coherence can be preserved for a period of order $10^4\tau_{rel}$ (**Steane,** 1997). This counter-intuitive result means that quantum coherence is preserved even though the qubits may have relaxed (and been re-excited) 10^4 times during the execution of the computations (**Steane,** 1997).

Error-correction protocols have been implemented in nuclear magnetic resonance experiments, but the inherent limitations of this technique (see Sec. V for discussions) prevent its application to quantum information processing. In (**Chiaverini *et al.*,** 2004), an experimental realisation of quantum error correction using trapped ions has been reported. They demonstrated quantum error correction using three beryllium atomic-ion qubits confined to a linear, multi-zone trap. They used a three-qubit quantum error-correcting code in order to protect a one-qubit (primary ion) state against 'spin-flip' errors. In the experiment, the errors are induced simultaneously in all qubits at various rates, and the encoded state is decoded back to the primary ion one-qubit state, making error information available on the ancilla ions, which are separated from the primary ion and measured. Finally, the primary qubit state is corrected on the basis of the ancillae measurement outcome. The error correction is verified by comparing the corrected final state to the uncorrected state and to the initial state (**Chiaverini *et al.*,** 2004).

In this section, only the method of QEC for correcting quantum noise has been presented. However, there have been different, complementary, proposals for suppressing, e.g., dynamical methods, or avoiding decoherence, e.g., by resorting to the use of decoherence-free subspaces (**Reina *et al.*,** 2002). In the latter, the evolution of a quantum register in a noisy environment is studied in detail. In particular, it is shown that under certain conditions —the collective decoherence coupling— it is possible to find a subspace of Hilbert's system space whose states evolve in a decoherence-free fashion (**Reina *et al.*,** 2002). From this point of view, one can argue that for arbitrarily complex quantum computations to ever be implemented in the laboratory, a combination of stabilisation schemes, such as fault tolerant QEC, decoherence-free subspaces, and dynamical methods to overcome decoherence, must be incorporated to the quantum registers dynamical evolution. In (**Reina & Bririd,** 2008), a numerically exact real-time path-integral approach (**Makri & Makarov,** 1995) has been used in order to account for the non-Markovian dissipation of a solid-state qubit system.

Next, we comment on some of the practicalities regarding QIP implementations, with a particular emphasis on solid-state technology.

V. PHYSICAL QUBITS

A quantum computation demands a coherent quantum evolution, and an active control or manipulations of the qubits, which are to be performed via unitary operations. We next give a brief discussion of some of the first hardware proposals (and/or demonstrations) for quantum information processing.

Cavity QED: originally proposed in (**Pellizzari *et al.*,** 1995), this hardware design is based on the idea of trapping neutral atoms inside a small high finesse optical cavity. Here, the quantum information is stored in the internal states of the atoms, which interact with each other via the coupling to the normal modes of the electromagnetic field in the cavity. By means of pulsed lasers, a transition in one atom can be induced as a result of the internal state of another atom, thus performing conditional dynamics. The first experimental attempt at producing these type of quantum gates was realised by Turchete *et al.* (**Turchete *et al.*,** 1995). A variant of this scheme is that proposed by Cirac *et al.* (**Cirac *et al.*,** 1996; **Cirac *et al.*,** 1997), allowing a further step: quantum communication. Here, instead of using a photon to couple the atoms, the quantum information is stored in the polarisation of the photon, and the trapped atoms are used as mediators of the interaction amongst the photons via high-Q optical cavities and optical fibres (**Cirac *et al.*,** 1996; **Cirac *et al.*,** 1997): in this way, quantum information can be transferred between separated atoms (e.g., ion traps, see below), in order to produce photon based logic gates (e.g., phase shift gates, see Ref. (**Cirac *et al.*,** 1997)). More recently, other proposals involving QED effects for quantum logic have been given in (**Imamoglu *et al.*,** 1999; **Rauschenbeutel *et al.*,** 1999; **Rauschenbeutel *et al.*,** 2001; **Leuenberger *et al.*,** 2005).

Ion traps: proposed by Cirac and Zoller, this scheme has single ions confined in a linear Paul trap as the qubit system (**Cirac & Zoller,** 1995; **Cirac & Zoller,** 2000). Thus, the qubit states can be represented as $|g\rangle \equiv |0\rangle$, and $|e\rangle \equiv |1\rangle$, the ground state, and a (long-lived metastable) excited state respectively. This ion system is very well shielded from the environment: almost spontaneous decay is the main source of decoherence. The preparation and measurement of corresponding (initial and final) states is easily accomplished by methods of optical pumping and laser cooling, and by means of 'quantum jump' or 'electron shelving' measurement technique, respectively (**Monroe *et al.*,** 1995; **Blatt & Wineland,** 2008).

Single qubit gates are performed via individually addressing the ions with pulsed lasers tuned at the transition frequency ω. This originates Rabi oscillations between the qubit states $|0\rangle$, and $|1\rangle$. Thus, arbitrary single-qubit gates can be performed by an appropriate timing and choosing of the laser phase.

Conditional logic gates rely on a beautiful but rather more complicated effect. The interactions in the ion trap are mainly given by the Coulomb repulsion between the ions. This implies a spectrum of coupled normal modes of vibration for the trapped ions, and the absorption or emission of a laser photon by the ion can be tailored in such a way that a normal mode involving many ions recoils coherently. The lowest frequency vibrational mode (frequency μ) is the centre-of-mass (cm) mode. Via laser cooling, these ions can be kept at an energy $k_BT << \hbar\mu$, hence guaranteeing that each vibrational mode occupies its quantum ground state. The next step, the generation of a "cm phonon," is crucial to this scheme: by shining an ion, say the nth, with a properly timed laser pulse of frequency $\omega - \mu$, the state $|e\rangle_n$ can be made to evolve into $|g\rangle_n$ at a cost of the transition $|0\rangle_{cm} \to |1\rangle_{cm}$ of the cm oscillator. This operation transforms

$$|g\rangle_n |0\rangle_{cm} \to |g\rangle_n |0\rangle_{cm} \, ; \quad |e\rangle_n |0\rangle_{cm} \to -i\,|g\rangle_n |1\rangle_{cm} \, , \tag{65}$$

thus, inducing an interaction between the ions via the collective state of motion of all the ions (the produced cm phonon). Next, the quantum information must be transferred from the cm phonon to the internal state of one of the ions, thus completing the logic gate. This procedure must be tailored in such a way that the cm mode returns to its ground state by the end of the computational process. It has been shown that this hardware design requires 5 appropriately tailored laser pulses in order to produce conditional CNOT gates (**Cirac & Zoller,** 1995; **Cirac & Zoller,** 2000). The experimental preparation, single gate realisation, and measurement for a single trapped ion was first demonstrated in (**Monroe *et al.*,** 1995). Another ion trap-based scheme for quantum computation has led to the experimental demonstration of up to four qubits (atoms) entanglement (**Molmer & Sorensen,** 1999; **Sackett *et al.*,** 2000). In (**Blatt & Wineland,** 2008), the state-of-the-art, as well as some of the original contributions and developments of the ion traps computers are highlighted.

Nuclear magnetic resonance: this hardware design provided the first few-qubit quantum processors realised in the laboratory, and, up to some point, had the 'lead' as to the achievement of a coherent manipulation of qubits is concerned. One of the key experiments has involved 7 qubits, in order to demonstrate the simplest possible case of Shor's factoring algorithm (**Vandersypen *et al.*,** 2001). This hardware scheme uses nuclear magnetic resonance (NMR) technology. The qubits are now represented by the nuclear spins in a particular molecule, where the spin states "up" or "down" serve as qubits. By placing the molecule in a large magnetic field, these nuclei spin states can be manipulated by applying oscillating magnetic fields in pulses of controlled duration. These qubits have very long decoherence and relaxation times (see table below). As said, Rabi oscillations of the spin can be induced by applying a pulsed rotating magnetic field of frequency ω (the energy splitting between the spin-up and spin-down states). Arbitrary single-qubit gates can be realised by an appropriate timing of this pulse. This process works in the presence of all of the molecule spins because only the spins on resonance respond to such an excitation. Two-qubit gates can be performed via the dipole-dipole spin interaction. Since the energy splitting between qubit states $|\uparrow\rangle$, and $|\downarrow\rangle$ for one spin depends on the state of neighbouring spins, the application of a resonant pulse that affects one spin is conditioned on the state of another spin. This produces the required conditional dynamics. For experimental demonstrations, see, e.g., (**Gershenfeld & Chuang,** 1997; **Chuang *et al.*,** 1998(A); **Chuang *et al.*,** 1998(B); **Cory *et al.*,** 1997; **Knill *et al.*,** 1998; **Jones *et al.*,** 1998(A); **Jones & Mosca,** 1998(B); **Vandersypen *et al.*,** 2001).

Major drawbacks of the NMR computers stem from their intrinsic scalability problems (the ratio of the coherent signal to the background declines exponentially with the number of spins per molecule), and from the fact that individual qubits can neither be directly prepared nor measured (only the average state of many processors is detectable). In fact, most experts agree that there is no chance that NMR-based qubits would succeed as scalable systems for the implementation of the controlled large-scale multipartite interference required for quantum computing.

Optical lattices & Bose-Einstein condensates: the recent experimental observation of a quantum phase transition from a superfluid to a Mott insulator in an ultracold gas has opened the way to a new hardware prospectus (**Greiner *et al.*,** 2002; **Mandel *et al.*,** 2003; **Giamarchi *et al.*,** 2008; **Bloch,** 2008; **Brennen *et al.*,** 1999; **Jacksch *et al.*,** 1999). By creating an optical lattice (an array of microscopic trapping potentials formed by laser light), a light-wave interference pattern which gives rise to an energy landscape of mountains and valleys, a gas of rubidium atoms has been reversibly switched from a superfluid to an insulating phase (**Greiner *et al.*,** 2002), where the rubidium atoms of the condensate have two different behaviours. They can either i) share the same quantum state in the superfluid phase and move freely between valleys, or ii) remain trapped in an individual valley, as a result of an increase in the intensity of the laser beams, which force the gas into an insulating phase.

This phase transition was predicted to occur in an optical lattice by Jaksch *et al.* (**Jacksch *et al.*,** 1999), where conditional dynamics and quantum entanglement has been proposed in moving trap potentials as a result of cold controlled collisions between two atoms. The experimental possibility of switching back and forth between superfluid and insulating behaviour brings an exciting development and is the subject of intense experimental activity (**Bloch,** 2008; **Giamarchi *et al.*,** 2008). In particular, the ideal array of single atoms in the insulating phase has become useful for multipartite entanglement generation (**Bloch,** 2008). Here, the two internal states (magnetic moment) of the rubidium atoms can represent the qubit states $|0\rangle$, and $|1\rangle$. Scalability can be guaranteed due to the large number of rubidium atoms in the optical lattice, which can serve as a quantum memory (**Bloch,** 2008).

The storage of ultracold (nK temperatures) quantum gases in in perfect large arrays of atoms (optical lattices) has provided a good tool for investigating quantum coherence and generating large-scale entanglement, and thus also leading to quantum information processing tasks in such artificial crystal structures . These arrays can also function as versatile model systems for the study of strongly interacting many-body systems on a lattice (**Bloch,** 2008).

Quantum dots & solid-state qubits: There is much current excitement about the possibility of using solid-state based devices for the achievement of quantum computation tasks (**Fushman *et al.*,** 2008; **Robledo *et al.*,** 2008; **Clarke & Wilhelm,** 2008). In particular, quantum dots are advantageous due to the existing and well developed nanofabrication technology and the ease of incorporating them into current opto-electronic devices. The quantum mechanical nature, the high degree of engineering and quantum control of individual wavefunctions of solid-state systems, besides intrinsic scalability properties, make, for example, quantum dots (**Fushman *et al.*,** 2008; **Robledo *et al.*,** 2008) and Josephson junctions (**Makhlin *et al.*,** 2001; **Clarke & Wilhelm,** 2008) very promising candidates for the physical implementation of QIP.

There are several proposals that consider different physical degrees of freedom as representative of solid-state qubit systems. Below we mention only some of these design schemes for quantum computation proposed to date: Kane (**Kane,** 1998) has proposed a scheme which encodes information onto the nuclear spins of donor atoms (like P) in doped silicon electronic devices where externally applied electric fields are used to perform logical operations on individual spins. Privman *et al.* (**Privman *et al.*,** 1998) suggested controlling the hyperfine electron-nuclear interaction via the excitation of the electron gas in quantum Hall systems. Loss and DiVincenzo (**Loss & DiVincenzo,** 1999; **Burkard *et al.*,** 1999) have presented a scheme based on electron spin effects, in which coupled quantum dots are used as a quantum gate. This scheme is based on the fact that the electron spins on the dots have an exchange interaction J which changes sign with increasing external magnetic field. Vrijen *et al.* (**Vrijen *et al.*,** 2000) considered electron spin resonance transistors in Silicon-Germanium heterostructures: one and two qubit operations are performed by applying a gate bias.

The above proposals, however, require the attachment of electrodes or gates to the sample in order to manipulate the nuclear spin qubit. Such electrodes are likely to have an invasive effect on the coherent evolution of the qubit, thereby destroying quantum information. In reference (**Reina *et al.*,** 2000(A)), an NMR solid-state based mechanism for quantum computation free from these shortcomings is proposed.

Possible quantum gate implementations have also been proposed by Barenco *et al.* (**Barenco *et al.*,** 1995(B)) by considering electronic charge effects in coupled QDs, however this scheme has as the main disadvantage rapid phonon decoherence, as compared with the above proposals. Imamoglu *et al.* (**Imamoglu *et al.*,** 1999) have considered a quantum computer model based on both electron spins and cavity QED which is capable of realising controlled interactions between two distant QD spins. In their model, the effective long-range interaction is mediated by the vacuum field of a high finesse microcavity, and single qubit rotations and CNOT operations are realised using electron-hole Raman transitions induced by classical laser fields and the cavity mode.

A different scheme exploits the exciton degrees of freedom of a QD system in order to generate an entangling network setup by exploiting (Förster) resonant energy transfer processes between coupled QDs (**Reina *et al.*,** 2000(B); **Quiroga & Johnson,** 1999; **Lovett *et al.*,** 2003(A,B); **Nazir *et al.*,** 2005). Related schemes, that also exploit exciton degrees of freedom for quantum computation, have been put forward in (**Biolatti *et al.*,** 2000; **Troiani *et al.*,** 2000).

Quantum dots can be constructed from inorganic or organic semiconductors, the latter being of special interest since they can constitute actual molecular architecture arrays of organic heterostructures, the so-called block copolymers (**Mujica *et al.*,** 2009). They are easier to construct than the inorganic systems, since they do not require expensive pieces of equipment as required for molecular beam epitaxy or metal-organic chemical vapour deposition. In principle, it is possible to construct an unlimited variety of organic heterostructures, since the interface between the materials is a chemical carbon-carbon bond, in contrast to inorganic ones, where it is required that the materials exhibit similar lattice constants to avoid interfacial stress, which notably limits the variety of heterostructures that can be synthesised. In (**Mujica *et al.*,** 2009) a global quantum computing scheme that uses molecular architectures based on π-conjugated block copolymers has been reported.

Within the quantum dots range of proposals, there have been some recent experimental demonstrations of controlled qubit gates, such as controlled phase shifts (**Fushman *et al.*,** 2008), and controlled-phase gates (**Robledo *et al.*,** 2008). In (**Fushman *et al.*,** 2008), the coupling between a single quantum dot and a photonic crystal nanocavity has allowed controlled phase and amplitude modulation between two modes of light at the single-photon level. As a perspective of such an experimental realisation, the combination of quantum logic devices and quantum nondemolition measurements on a chip are expected (**Fushman *et al.*,** 2008). In (**Robledo *et al.*,** 2008), a demonstration of conditional dynamics for two coupled quantum dots is reported. Here, the logic gate dynamics is induced by means of a transition to an optically excited state which is controlled by the presence or absence of an optical excitation in the neighboring dot. The dots interact via a tunnel coupling between optically excited states and can be optically gated by applying a laser field. Other recent demonstrations already incorporate the design of robust optically programmable quantum dots electron spin memories (**Kroutvar *et al.*,** 2004), and molecular ensembles as quantum memories for solid state circuits in hybrid quantum processors (**Rabi *et al.*,** 2006) that are envisioned as devices for the generation, control, and communication of multipartite quantum entanglement and for the realisation of large scale conditional dynamics.

Superconducting circuits (see Fig. 7) are macroscopic devices in size which can exhibit quantum behaviour, such as quantized energy levels, superpositions, and entanglement of of states (**Makhlin *et al.*,** 2001; **Clarke & Wilhelm,** 2008). The building blocks of such circuits are the so-called superconducting qubits, and electric charge and magnetic flux degrees of freedom are used as quantum hardware for quantum computing (**Makhlin *et al.*,** 2001; **Clarke & Wilhelm,** 2008). Here, the quantum states can be manipulated by using electromagnetic pulses to control the flux, the charge or the phase difference across a Josephson junction (**Makhlin *et al.*,** 2001). A generic superconducting qubit can be described by the Hamiltonian $\widehat{H}_q = -\frac{1}{2}\epsilon\widehat{\sigma}_z - \frac{1}{2}\Delta\widehat{\sigma}_x$, where ϵ and Δ denote the 'longitudinal' and 'transversal' parameters of the corresponding qubit, and σ_i are the usual Pauli matrices (**Leggett *et al.*,** 1987). The charge qubit has the advantage of a more flexible controllability via external parameters: it can be conveniently controlled by a voltage gate or an applied magnetic flux (**Makhlin *et al.*,** 2001). These external control parameters appear in the longitudinal (σ_z) and transverse (σ_x) terms of the circuit's reduced Hamiltonian. For the flux qubit, the longitudinal term can be controlled by the applied magnetic flux, but it can be harder to control the transversal term via an external parameter (**Makhlin *et al.*,** 2001).

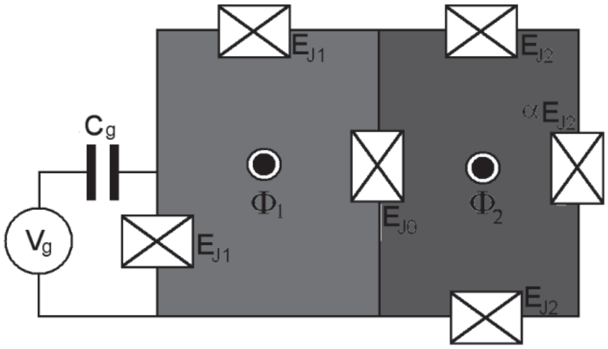


FIG. 7 Hybrid quantum circuit: charge (left) and flux (right) qubits are effectively coupled due to the Josephson junction E_{J0}. E_{Ji} denotes the Josephson energy of each junction (crossed boxes). The charge ($i = 1$) and the flux ($i = 2$) qubits are crossed by externally controlled magnetic fluxs Φ_i (**Montes *et al.*,** 2009).

In (**Montes *et al.*,** 2009), a hybrid quantum circuit, a system that couples a charge and a flux qubit, as schematically shown in Figure 7, has been studied. This exhibits an effective interaction due to a Josephson junction (a device with nonlinear inductance and no energy dissipation) that binds them. This system has been proposed in order to control the transversal term of the flux qubit with the charge qubit. The interaction between the qubits gives rise to an effective $\sigma_x \otimes \sigma_z$ geometric term with a strength that allows the realisation of controlled qubit gates for quantum computing (**Montes *et al.*,** 2009). Aside of their potential use as the building blocks of quantum computers, superconducting qubits are fundamental in the understanding of basic macroscopic quantum coherence related phenomena (**Makhlin *et al.*,** 2001; **Clarke & Wilhelm,** 2008).

Other solid-state based proposals involve quantum information processing with large nuclear spins in GaAs semiconductors (**Leuenberger *et al.*,** 2002), nanotubes and fullerenes (**Ardavan *et al.*,** 2003), molecular magnets (**Leuenberger *et al.*,** 2001), single molecule arrays (**Reina *et al.*,** 2004), graphene quantum dots (**Trauzettel *et al.*,** 2007), and organic polymers (**Mujica *et al.*,** 2009).

On a different front, there are fundamental coherence control experiments being performed in soft-condensed matter nanostructures, where there have been some recent breakthroughs. In particular, regarding the quantum coherence of biomolecular excitons, over the past few years has been argued that quantum coherent dynamics at the initial stages of photosynthesis in complex biomolecular structures promote the efficiency of energy transfer from the light-harvesting antenna complexes to the chemical reaction centres (**Brixner *et al.*,** 2005; **Herek *et al.*,** 2002). This hypothesis has been recently boosted by experimental results which reveal long-lived quantum coherent excitonic dynamics in the energy transfer among bacteriochlorophylls in photosynthetic complexes (**Engel *et al.*,** 2007; **Lee *et al.*,** 2007). This said, it is often claimed that coherent dynamical processes in nanostructures for quantum information processing are severely hindered by non-Markovian decoherence (**Weiss,** 2008; **Zurek,** 2002; **Alicki *et al.*,** 2002; **Makri & Makarov,** 1995). By using a numerically exact real-time path-integral approach (**Makri & Makarov,** 1995), Thorwart *et al.* (**Thorwart *et al.*,** 2008; **Eckel *et al.*,** 2009) have shown that quantum coherence of excitons created in photosynthetic biomolecular complexes can be sustained over exceedingly long times due to a constructive role played by the non-Markovian surrounding environment. They provided evidence that a sluggish quantum bath helps to sustain coherence in a single pair of Förster coupled excitons compared to a Markovian environment. Furthermore, it has also been shown that the quantum entanglement of excitations in two pairs of coupled chromophores is more stable against decoherence generated by a slow bath, and that the entanglement robustness persists up to surprisingly high temperatures (**Thorwart *et al.*,** 2008). These results can explain why naturally existing, correlated protein environments help to maintain electronic coherence in light-harvesting complexes and could prove crucial in the artificial design of robust multipartite biomolecular entanglement or quantum memories (**Kroutvar *et al.*,** 2004; **Rabi *et al.*,** 2006) for the control and conditional dynamics of qubits.

Gating and decoherence time scales

The figure of merit $\mathcal{M} \equiv \tau_{dec}/\tau_{gate}$ for comparing some of the different technologies currently used in quantum information processing is given in Table I. The ratio $\mathcal{M}$ gives an estimation of the largest number of elementary operations that can, in principle, be performed on the register states before decoherence takes over.

The gating time τ_{gate} is the minimum time required to execute an elementary gate. This has been estimated in Table I as $\hbar/\Delta E$, where ΔE is the energy splitting between the qubit states $|0\rangle$, and $|1\rangle$. τ_{dec} is the corresponding qubit phase coherence time.

VI. CONCLUSIONS

A concise review of some of the basic concepts in the field of quantum information and quantum computation

Quantum hardware	τ_{gate} (s)	τ_{dec} (s)	$\mathcal{M}$
Trapped ions [a]	10^{-5}	10^{-1}	10^4
Optical cavities[b]	10^{-14}	10^{-5}	10^9
Nuclear spin[c]	10^{-3}	10^4	10^7
Cavity QED[d]	10^{-9}	10^{-3}	10^6
Electron spin[e]	10^{-7}	10^{-3}	10^4
QDs excitons[f]	10^{-14}	10^{-10}	10^4

[a] **Blatt & Wineland,** 2008; **Monroe *et al.*,** 1995; **Sackett *et al.*,** 2000

[b] **Bloch,** 2008; **Mandel *et al.*,** 2003

[c] **Jones *et al.*,** 1998; **Luenbeerger *et al.*,** 2002

[d] **Turchete *et al.*,** 1995; **Rauschenbeutel *et al.*,** 1999

[e] **Vrijen *et al.*,** 2000; **Kroutvar *et al.*,** 2004

[f] **Borri,** 2001; **Birkedal *et al.*,** 2001; **Robledo *et al.*,** 2008

TABLE I Characteristic 'gating,' and dephasing time scales for comparing different physical systems currently used as qubits. The figure of merit $\mathcal{M}$ gives an estimation of the number of qubit operations that could be realised on a qubit register before it decoheres.

has been presented. Quantum registers, through to the universal gate for building quantum circuits that are universal for quantum computation, were introduced. It has been shown how two-qubit gates suffice for quantum computation, and the power of the quantum circuit representation for entangling and disentangling quantum states was emphasised, in terms of both *local* and *global* control quantum computing. This led to a discussion of the no-cloning theorem and its interesting implications. The basic formulations of one-way quantum computation, and holonomic or geometric computation—alternative approaches for quantum computation—were also introduced. Following this, the power of quantum entanglement as a communication resource was highlighted in order to describe some practical applications, such as quantum teleportation, quantum cryptography, dense coding, and quantum data compression. The problem of entanglement quantification was discussed and some examples of entanglement measures were given. Deutsch's concept of quantum parallelism was introduced in order to gain insight into the potential for efficiently solving certain classically intractable algorithms. After this, two processes fundamental to QIP, decoherence and 'recoherence' (e.g., quantum error correction), were discussed. The main qubit systems currently employed for the processing of quantum information were also described.

As was shown, there have been some successful demonstrations of few-qubit manipulations, and there exists a vast and still growing range of proposals for realizing quantum information processing. This intense experimental and theoretical research activity has been ongoing for more than a decade. The way forward is still very open—the key routes to few-qubit and large-scale QIP, which could well differ, have yet to be identified. In this respect, proposals and implementations of hybrid systems that combine the so-called stationary (matter) and flying (photon) qubits seem a perspective worth pushing forward.

Whether the task of building a true (large scale) quantum computer is ever going to be achieved remains an open question. The final goal of building a quantum computer will be extremely challenging, with basic physical mechanisms needing to be addressed and fully understood. As has been shown, due to their contact with their reservoirs, the interacting qubit networks for QIP are subjected to irreversible dissipation mechanisms which spoil the required coherent qubit dynamics. Such hardware-dependent noise sources are a major hurdle that have to be understood and overcome if the dream of efficient large scale quantum computing is to become a reality.

Acknowledgements. The author would like to thank G. Paz-Silva for discussions on entanglement measures (Sec. III.B), and J. D. Jaramillo for help with the illustrations of Sec. II.C. JHR is grateful to the Departamento de Física of the Universidad del Valle, Colciencias (Grant No. 1106-452-21296), and the DAAD-PROCOL Program for financial support.

APPENDIX A: The no-cloning theorem

The no-cloning theorem (**Wootters & Zurek,** 1982) is a consequence of the fundamental principles of quantum physics. It leads to interesting applications such as quantum cryptography (see Subs. III.F). To prove the "no-cloning theorem" it suffices to note that, in order to generate a copy of an arbitrary quantum state $|\Psi\rangle$, we should be able to realise a unitary transformation U that produces the evolution $U(|\Psi\rangle\,|0\rangle) = |\Psi\rangle\,|\Psi\rangle$. Consider the state $|\Psi'\rangle$ such that $|\Psi'\rangle \neq |\Psi\rangle$. Hence, $U(|\Psi'\rangle\,|0\rangle) = |\Psi'\rangle\,|\Psi'\rangle$. Next, we make $|\Phi\rangle = (|\Psi\rangle + |\Psi'\rangle)/\sqrt{2}$, obtaining $U(|\Phi\rangle\,|0\rangle) = (|\Psi\rangle\,|\Psi\rangle + |\Psi'\rangle\,|\Psi'\rangle)/\sqrt{2} \neq |\Phi\rangle\,|\Phi\rangle$, which fails the cloning operation since U must not depend on any chosen $|\Phi\rangle$. From this we can state that unless we know beforehand the state of a qubit (which is to be represented by classical information), it is impossible to generate copies of a quantum state faithfully.

APPENDIX B: Cluster and graph states

A *cluster state* is a type of highly entangled state of multiple qubits. Cluster states are generated in lattices of qubits with Ising type interactions. A cluster C is a connected subset of a d-dimensional lattice, and a cluster state is a pure state of the qubits located on C. They are different from other types of entangled states such as GHZ states or W states because it is more difficult to eliminate quantum entanglement (via projective measurements) in the case of cluster states. Another way of thinking of cluster states is as a particular instance of graph states, where the underlying graph is a connected subset of a d-dimensional lattice. To define a cluster state, the eigenstates $|U\rangle_G = \sigma_z^U\,|G\rangle$ of K_a^G, according to the eigenvalues U_a, are introduced:

$$K_a^G\,|U\rangle_G = (-1)^{U_a}\,|U\rangle_G\,, \tag{B1}$$

or, in terms of the symmetric Γ $(N \times N)$ matrix of elements

$$\Gamma_{ab} = \begin{cases} 1, & \text{if } \{a,b\} \in E, \\ 0, & \text{otherwise.} \end{cases} \tag{B2}$$

For this we define a *neighbourhood* as the set of adjacent vertices to a given vertex, and denote it as

$$N_a := \{b \in V | \{a,b\} \in E\}, \tag{B3}$$

for a given vertex $a \in V$. The number of neighbours $|N_a|$ is the vertex *grade* of vertex a (**Raussendorf & Briegel,** 2001). Thus, we write for the cluster state

$$K_a^G \equiv \sigma_x^{(a)} \prod_{b\in V} (\sigma_z^{(b)})^{\Gamma_{ab}} = \sigma_x^a \otimes \sigma_z^{N_a} = \sigma_x^a \otimes \sigma_z^{\Gamma a}. \tag{B4}$$

A *graph* $G = (V, E)$ is a collection of vertices V, and a set of edges (one-dimensional line segments joining two vertices) E. A graph state is usually represented by a two-dimensional diagram, where each vertex is represented by a point and the edges by lines that join two vertices. Formally, a graph state is defined as a pair

$$|G\rangle = (V, E) = \prod_{\{a,b\}\in E} U_{ab} \, |+\rangle^{\otimes V}, \tag{B5}$$

where the operator $U_{a,b}$ is the interaction between the two vertices (qubits) a, b

$$U_{ab} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \tag{B6}$$

and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. An alternative and equivalent definition is as follows. Define an operator K_a^G for each vertex a of G:

$$K_a^G \equiv \sigma_x^{(a)} \prod_{b\in N_a} \sigma_z^{(b)}, \tag{B7}$$

Where N_a is the neighborhood of a (the set of all b such that $(a, b) \in E$), and σ_i are the pauli matrices. Then, the graph state $|G\rangle$ is defined as the simultaneous eigenstate of the $N = |V|$ operators $\{K_a^G\}_{a\in V}$ with eigenvalue 1: $K_a^G \, |G\rangle = |G\rangle$.

APPENDIX C: Examples of QEC codes

1. Example 1: Bit-flip σ_x-error-correction

Suppose Q has three qubits, and a has two qubits. Let M_s be the bit-flip error generator σ_x. In this case, there are two orthonormal recoverable states: $|000\rangle$, and $|111\rangle$, thus $dim(\mathcal{RH}) = 2$. The state $|\Phi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$ is a general recoverable state of Q. The noisy environment entangles the qubit register as follows:

$$|e_0\rangle\,(\alpha\,|000\rangle + \beta\,|111\rangle) + |e_1\rangle\,(\alpha\,|001\rangle + \beta\,|110\rangle) + |e_2\rangle\,(\alpha\,|010\rangle + \beta\,|101\rangle) + |e_3\rangle\,(\alpha\,|100\rangle + \beta\,|011\rangle). \tag{C1}$$

In this case, the syndrome extraction A consists of the following four CNOT gates, with "Q" ("a") as the control (target) system: $\text{CNOT}_{14}\text{CNOT}_{24}\text{CNOT}_{15}\text{CNOT}_{35}$. After this A-operation, the whole register "$Q + E + a$" is left in the state

$$|e_0\rangle|00\rangle_a(\alpha|000\rangle + \beta|111\rangle) + |e_1\rangle|01\rangle_a(\alpha|001\rangle + \beta|110\rangle) + |e_2\rangle|10\rangle_a(\alpha|010\rangle + \beta|101\rangle) + |e_3\rangle|11\rangle_a(\alpha|100\rangle + \beta|011\rangle). \tag{C2}$$

Next, a measurement of the ancilla a is performed. Hence, conditional to the measurement result, the following simple operations over the Q-qubits project back the system onto the noise-free state $|\Phi\rangle$: "do nothing," $\sigma_x^{(1)}$, $\sigma_x^{(2)}$, $\sigma_x^{(3)}$, if the ancilla measurement gives 00, 01, 10, or 11, respectively. As said, in the above procedure, the measurement step can be avoided by using Toffoli gates (see below), but in this case, with "a" ("Q") as the control (target) (**Steane,** 1996(A, B, C)).

2. Example 2: Phase-flip σ_z-error-correction

A single-phase-error-correcting-code that uses three qubits has the following two quantum codewords (encoding)

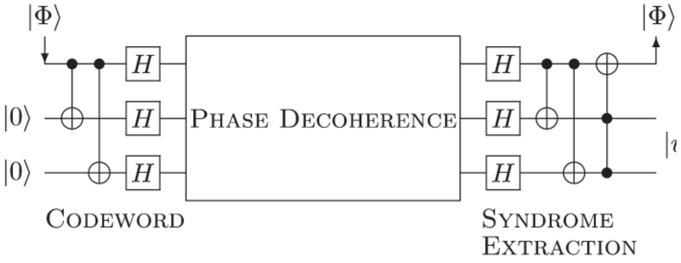
$$\begin{aligned} H(|000\rangle) &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &\equiv |\bar{0}\bar{0}\bar{0}\rangle \qquad \text{(C3)} \\ H(|111\rangle) &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\equiv |\bar{1}\bar{1}\bar{1}\rangle \qquad \text{(C4)} \end{aligned}$$

Next, let's illustrate how to perform QEC without realising the final ancilla measurement operation, i.e., by means of quantum gates only. Suppose one is given the state $|\Phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ (system "Q") that needs to be protected against phase decoherence (in this example it is assumed that only single-qubit dephasing errors occur). In so doing, an ancilla "a" of two qubits is introduced. Next, the register "$Q + a$" is encoded following the codeword given before. For illustrative purposes, let's assume that the environment interaction 'dephases' the second qubit only. Then, the decohered state becomes (the normalisation factor $2^{-3/2}$ has been ommitted)

$$\alpha(|0\rangle + |1\rangle)(|0\rangle\,|e_0\rangle + |1\rangle\,|e_1\rangle)(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)(|0\rangle\,|e_0\rangle - |1\rangle\,|e_1\rangle)(|0\rangle - |1\rangle)\ . \tag{C5}$$

The syndrome extraction A (decoding) is then built from two CNOT gates and a Toffoli gate, as shown in the schematic below, thus correcting the phase error and recovering the original state $|\Phi\rangle$. Note that while $|\Phi\rangle$ is a noise-free state, the final ancilla state

$|u\rangle_a = |00\rangle\left(|e_0\rangle + |e_1\rangle\right) + |10\rangle\left(|e_0\rangle - |e_1\rangle\right)$ becomes entangled with the environment.



3. Example 3: σ_x, σ_z, & $\sigma_x\sigma_z$-error correction

The construction of codes following the above recipe are referred to in the literature as CSS codes (for Calderbank, Shor, and Steane). This method leads to a single-error-correcting quantum code that has the following parameters: $[[\ n, 2k-n, d\ ]] = [[7,1,3]]$. The notation indicates that the length of the codewords is n, there are 2^{2k-n} orthonormal quantum codewords, and d is the 'minimum distance' of the code (the minimum number of places in which each word differs from all others). Hence, the prescribed code requires 7 qubits in order to store and protect a single qubit. The simplest CSS code is obtained from the classical Hamming code, and has the following two orthogonal codewords (**Steane,** 1996(A, B, C))

$$\begin{aligned} |c_0\rangle &\equiv |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + \\ &\quad |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \ , \\ |c_1\rangle &\equiv \sigma_x^{(1111111)} |c_0\rangle \ . \end{aligned} \tag{C6}$$

The superscripts indicate that the bit-flip operation must be performed on each qubit of each single codeword. It is worth pointing out that the above description is not the most general possible theory of QEC. The most general treatment of QEC codes has been developed in (**Gottesman,** 1996; **Knill & Laflamme,** 1997; **Calderbank *et al.*,** 1997). It turns out that there are more efficient quantum code constructions. In fact, Laflamme *et al.* (**Laflamme *et al.*,** 1996) and Bennett *et al.* (**Bennett *et al.*,** 1996) have provided a 5-qubit single-error-correcting code that produces the same control as CSS's code, but with the advantage that it requires only 5 qubits to do the job. This $[[5,1,3]]$ code has been referred to as a "perfect quantum code" (**Laflamme *et al.*,** 1996; **Bennett *et al.*,** 1996; **Calderbank *et al.*,** 1997). Hence, an arbitrary quantum state $|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle$ that is encoded by using 4 additional ancillary qubits (prepared in the state $|0\rangle$), using a $[[5,1,3]]$ encoding, can evolve in the presence of a general quantum noise (σ_x, σ_y, and $-i\sigma_z$-errors) in such a way that by the end of the computation it can be extracted completely free of noise from the 5-qubit system: that is, if at any stage of the computation, something 'wrong' happened to its coherence, the encoding guarantees that by the end of the computation, $|\Phi\rangle$ is error-free, and completely disentangled from the environment!

References

Alicki R., M. Horodecki, P. Horodecki & R. Horodecki. 2002. Dynamical Description of Quantum Computing: Generic Nonlocality of Quantum Noise. Phys. Rev. A **65**: 062101-62111.

Amico L., R. Fazio, A. Osterloh & V. Vedral. 2008. Many-Body Entanglement. Rev. Mod. Phys. **80**: 517-576.

Ardavan A., M. Austwick, S. Benjamin, A. Briggs, T. Dennis, A. Ferguson, D. Hasko, M. Kanai, A. Khlobystov, B. Lovett, G. Morley, R. Oliver, D. Pettifor, K. Porfyrakis, J. H. Reina, J. Rice, J. Smith, R. Taylor, D. Williams, C. Adelmann, H. Mariette & R. J. Hamers. 2003. Nanoscale Solid-State Quantum Computing. Phil. Trans. R. Soc. London A **361:** 1473-1485.

Aspect A., J. Dalibard & G. Roger. 1982. Experimental Test of Bell's Inequalities Using Time-Varying Analyzers. Phys. Rev. Lett. **49:** 1804-1807.

Averin D. 1998. Adiabatic Quantum Computation with Cooper Pairs. Solid State Commun **105:** 659-664.

Barenco A. 1995. A Universal Two-Bit Gate for Quantum Computation. Proc. R. Soc. Lond. A **449:** 679-683.

Barenco A., C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin & H. Weinfurter. 1995(A). Elementary Gates for Quantum Computation. Phys. Rev. A **52:** 3457-3467.

Barenco A., D. Deutsch, A. Ekert & R. Jozsa. 1995(B). Conditional Quantum Dynamics and Logic Gates. Phys. Rev. Lett. **74:** 4083-4086.

Barenco A. & A. Ekert. 1995. Dense Coding Based on Quantum Entanglement. J. Mod. Opt. **42:** 1253-1259.

Barrett, M. D. et al. J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri & D. J. Wineland. 2004. Deterministic Quantum Teleportation of Atomic Qubits. Nature **429:** 737-739.

Bastidas V., J. H. Reina & T. Brandes. 2009. Non-Equilibrium Entanglement in a Driven Dicke Model. Journal of Physics: Conf. Series **167:** 012063/1-5.

Bell J. 1964. On the Einstein Podolsky Rosen Paradox. Physics **1:** 195-200.

Bell J. 1987. Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press.

Bennett C. & G. Brassard. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proc. IEEE Int. Conference on Computers, Systems and Signal Processing. Bangalore, India (IEEE, New York): 175-179.

Bennett C. & G. Brassard. 1989. The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype is Working! SIGACT news **20:** 78-82.

Bennett C., G. Brassard & A. Ekert 1992(A). Quantum Cryptography. Scientific American **267:** 50-57.

Bennett C., G. Brassard & N. Mermin. 1992(B). Quantum Cryptography Without BellÆs Theorem. Phys. Rev. Lett. **68:** 557-559.

Bennett C. & S. Wiesner. 1992(C). Communication via One-and Two-Particle Operators on Einstein-Podolsky-Rosen States. Phys. Rev. Lett. **69:** 2881-2884.

Bennett C., G. Brassard, C. Cr¦epeau, R. Jozsa, A. Peres & W. Wooters. 1993. Teleporting an Unknown Quantum State Via Dual Classical and Einstein-Podolsky-Rosen Channels. Phys. Rev. Lett. **70:** 1895-1899.

Bennett C. 1995. Quantum Information and Computation. Physics Today **48:** 24-30.

Bennett C. H., D. P. DiVincenzo, J. Smolin & W. K. Wootters. 1996. Mixed-State Entanglement and Quantum Error Correction. Phys. Rev. A **54:** 3825-3851.

Bennett C. H., C. A. Fuchs & J. A. Smolin. 1997. Proc. QCM96, ed. by O. Hirota, A. S. Holevo and C. M. Caves, New York: Plenum, pp. 79. E-print quant-ph/9611006.

Bennett C. & D. DiVincenzo. 2000. Quantum Information and Computation. Nature **404:** 247-255.

Bennett C. H., S. Popescu, D. Rohrlich, J. A. Smolin & A. V. Thapliyal. 2001. Exact and Asymptotic Measures of Multipartite Pure-State Entanglement. Phys. Rev. A **63:** 012307/1-12.

Benioff P. 1982(A). Quantum Mechanical Hamiltonian Models of Turing Machines. J. Stat. Phys. **29:** 515-546.

Benioff P. 1982(B). Quantum Mechanical Models of Turing Machines That Dissipate No Energy. Phys. Rev. Lett. **48:** 1581-1585.

Benjamin S. C. & P. Hayden. 2001(A). Comment on æQuantum Games and Quantum Strategie's. Phys. Rev. Lett. **87:** 069801. E-print quant-ph/0003036.

Benjamin S. C. & P. Hayden. 2001(B). Multiplayer Quantum Games. Phys. Rev. A **64:** 030301-30304(R). E-print quant-ph/0007038.

Benjamin S. C. 2000. Schemes for Parallel Quantum Computation Without Local Control of Qubits. Phys. Rev. A **61:** 020301-20304(R).

Benjamin S. C. 2002. Quantum Computing Without Local Control of Qubit-Qubit Interactions. Phys. Rev. Lett. **88:** 017904/1-4.

Benjamin S. C., B. Lovett & J. H. Reina. 2004. Optical Quantum Computation with Perpetually Coupled Spins. Phys. Rev. A **70:** 060305(R)/1-4.

Berry M. 1984. Quantal Phase Factors Accompanying Adiabatic Changes. Proc. Roy. Soc. A **392:** 45-57.

Biolatti E., R. Iotti, P. Zanardi & F. Rossi. 2000. Quantum Information Processing with Semiconductor Macroatoms. Phys. Rev. Lett. **85:** 5647-5650.

Birkedal D., K. Leosson & J. Hvam. 2001. Long Lived Coherence in Self-Assembled Quantum Dots. Phys. Rev. Lett. **87:** 227401/404.

Blatt R. & D. Wineland. 2008. Entangled States of Trapped Atomic Ions. Nature **453:** 1008-1015.

Bloch I, 2008. Quantum Coherence and Entanglement with Ultracold Atoms in Optical Lattices. Nature, **453:** 1016-1022.

Borri P., W. Langbein, S. Schneider, U. Woggon, R. Sellin, D. Ouyang & D. Bimberg. 2001. Ultralong Dephasing Time in InGaAs Quantum Dots. Phys. Rev. Lett. **87:** 157401/404.

Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter & A. Zeilinger. Experimental Quantum Teleportation. Nature **390:** 575-579.

Brassard G., S. L. Braunstein & R. Cleve. 1998. Teleportation as a Quantum Computation. Physica D **120:** 43-47.

Braunstein S., A. Mann & M. Revzen. 1992. Maximal Violation of Bell Inequalities for Mixed States. Phys. Rev. Lett. **68:** 3259-3261.

Brennen G., C. Caves, P. Jessen & I. Deutsch. 1999. Quantum Logic Gates in Optical Lattices. Phys. Rev. Lett. **82:** 1060-1063.

Briegel H. J. & R. Raussendorf. 2001. Persistent Entanglement in Arrays of Interacting Particles. Phys. Rev. Lett. **86:** 910-913.

Brixner T., J. Stenger, H. M. Vaswani, M. Cho, R. E. Blankenship & G. R. Fleming. 2005. Two-Dimensional Spectroscopy of Electronic Couplings in Photosynthesis. Nature **434:** 625-628.

Browne D. E. & T. Rudolph. 2005. Resource-Efficient Linear Optical Quantum Computation. Physical Review Letters **95:** 010501/1-4.

Burkard G., D. Loss & D. DiVincenzo. 1999. Coupled Quantum Dots as Quantum Gates. Phys. Rev. B **59:** 2070-2078.

Calderbank A., E. Rains, P. Shor & N. Sloane. 1997. Quantum Error Correction and Orthogonal Geometry. Phys. Rev. Lett. **78:** 405-408.

Calderbank R. & P. Shor. 1996. Good Quantum Error-Correcting Codes Exist. Phys. Rev. A **54:** 1098-1115.

Carollo A., I. Fuentes-Guridi, M. Franca Santos & V. Vedral. 2003. Geometric Phase in Open Systems. Phys. Rev. Lett. **90:** 160402/1-4.

Carollo A., I. Fuentes-Guridi, M. Franca Santos & V. Vedral. 2004. Spin-1/2 Geometric Phase Driven by Decohering Quantum Fields. Phys. Rev. Lett. **92:** 020402/1-4.

Carollo A., M. Franca Santos & V. Vedral. 2006. Coherent Quantum Evolution via Reservoir Driven Holonomies. Phys. Rev. Lett. **96:** 020403/1-4.

Cerf N. & C. Adami. 1997. Negative Entropy and Information in Quantum Mechanics. Phys. Rev. Lett. **79:** 5194-5197.

Chen Y.-A., S. Chen, Z.-S Yuan, B. Zhao, C.-S. Chuu, J. Schmiedmayer & J.-W. Pan. 2008. Memory-built-in Quantum Teleportation with Photonic and Atomic Qubits. Nature Physics **4:** 103-107.

Chiaverini J., D. Leibfried, T. Schaetz, M. D. Barrett, R. B. Blakestad, J. Britton,W. M. Itano, J. D. Jost, E. Knill, C.

Langer, R. Ozeri & D. J. Wineland. 2004. Realization of Quantum Error Correction. Nature **432:** 602-605.

Christandl M. & A. Winter. 2004. Squashed Entanglement: An Additive Entanglement Measure. Math. Phys. **45:** 829-840.

Chuang I., L.Vandersypen, X. Zhou, D. Leung & S. Lloyd. 1998(A). Experimental Realization of a Quantum Algorithm. Nature **393:** 143-146.

Chuang I., N. Gershenfeld & M. Kubinec. 1998(B). Experimental Implementation of Fast Quantum Searching. Phys. Rev. Lett. **80:** 3408-3411.

Cirac J., P. Zoller, H. Kimble & H. Mabuchi. 1997. Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network. Phys. Rev. Lett. **78:** 3221-3224.

Cirac J., T. Pellizzari & P. Zoller. 1996. Enforcing Coherent Evolution in Dissipative Quantum Dynamics. Science **273:** 1207-1210.

Cirac J. & P. Zoller. 1995. Quantum Computations With Cold Trapped Ions. Phys. Rev. Lett. **74:** 4091-4094.

Cirac J. & P. Zoller. 2000. A Scalable Quantum Computer With Ions in an Array of Microtraps. Nature **404:** 579-581.

Clarke J. & F. K. Wilhelm. 2008. Superconducting Quantum Bits. Nature **453:** 1031-1042.

Cleve R., A. Ekert, C. Macchiavello & M. Mosca. 1998. Quantum Algorithms Revisited. Proc. R. Soc. Lond. A **454:** 339-354.

Cocks C. 1973. A Note on Non-Secret Encryption. Tech. report. Communications-Electronics Security Group. United Kingdom.

Cory D., A. Fahmy & T. Havel. 1997. Ensemble Quantum Computing by NMR Spectroscopy. Proc. Natn. Acad. Sci. USA **94:** 1634-1639.

d'Espagnat B. 1976. Conceptual Foundations of Quantum Mechanics. Benjamin, Reading. Massachusetts.

Deutsch D. 1985. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proc. R. Soc. London A **400:** 97-117.

Deutsch D. 1989. Quantum Computational Networks. Proc. R. Soc. Lond. A **425:** 73-90.

Deutsch D., A. Barenco & A. Ekert. 1995. Universality in Quantum Computation. Proc. R. Soc. Lond. A **449:** 669-677.

Deutsch D. & R. Jozsa. 1992. Rapid Solution of Problems by Quantum Computation. Proc. R. Soc. London A **439:** 553-558.

DiVincenzo D. 1995. Two-Bit Gates are Universal for Quantum Computation. Phys. Rev. A **51:** 1015-1022.

Duan L., J. Cirac & P. Zoller. 2001. Geometric Manipulation of Trapped Ions for Quantum Computation. Science **292:** 1695-1697.

Dür W., G. Vidal & J. I. Cirac. 2000. Three Qubits Can be Entangled in Two Inequivalent Ways. Phys. Rev. A **62:** 062314/1-12.

Eckel J., J. H. Reina & M. Thorwart. 2009. Coherent Control of an Effective Two-Level System in a Non-Markovian Biomolecular Environment. To appear in New J. Phys., Special Issue: Focus on "Quantum Dissipation in Unconventional Environments". Eprint cond-mat arXiv:0903.2936.

Einstein A., B. Podolsky & N. Rosen. 1935. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. **47:** 777-780.

Eisert J., M. Wilkens & M. Lewenstein. 1999. Quantum Games and Quantum Strategies. Phys. Rev. Lett. **83:** 3077-3080.

Eisert J. & M. Wilkens. 2000. Quantum Games. Eprint quant-ph/0004076.

Ekert A. 1991. Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. **67:** 661-663.

Ekert A., M. Ericsson, P. Hayden, H. Inamori, J. Jones, D. Oi & V. Vedral. 2000(A). Geometric Quantum Computation. J. Mod. Opt. **47:** 2501-2513.

Ekert A., P. Hayden & H. Inamori. 2000(B). Basic Concepts in Quantum Computation. E-print arXiv:quant-ph/0011013v1.

Ekert A. & C. Macchiavello. 1996. Quantum Error Correction for Communication. Phys. Rev. Lett. **77:** 2585-2588.

Ekert A. & R. Jozsa. 1996. Quantum Computation and Shor's Factoring Algorithm. Rev. Mod. Phys. 68: 733-753.

Engel G.S., T. R. Calhoun, E. L. Read, T.-K. Ahn, T. Mancal, Y.-C. Cheng, R. E. Blankenship & G. R. Fleming. 2007. Evidence for Wavelike Energy Transfer through Quantum Coherence in Photosynthetic Systems. Nature **446:** 782-786.

Falci G., R. Fazio, G. Palma, J. Siewert & V. Vedral. 2000. Detection of Geometric Phases in Superconducting Nanocircuits. Nature **407:** 355-358.

Feynman R. 1982. Simulating Physics with Computers. Int. J. Theor. Phys. **21:** 467-488.

Feynman R. 1985. Quantum Mechanical Computers. Opt. News **11:** 11-46.

Fushman I., D. Englund, A. Faraon, N. Stoltz, P. Petroff & J. Vukovi. 2008. Controlled Phase Shifts with a Single Quantum Dot. Science **320:** 769-772.

Galindo A. & P. Pascual. 1990. Quantum Mechanics II. Springer-Verlag. Berlin.

Gershenfeld N. & Chuang I. 1997. Bulk Spin-Resonance Quantum Computation. Science **275:** 350-356.

Giamarchi T., C. Ruegg & O. Tchernyshyov. 2008. Bose-Einstein Condensation in Magnetic Insulators. Nature Physics **4:** 198-204.

Gisin N., G. Ribordy, W. Tittel & H. Zbinden. 2002. Quantum Cryptography. Reviews of Modern Physics **74:** 145-195.

Gottesman D. 1996. Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound. Phys. Rev. A **54:** 1862-1868.

Greenberger D., M. Horne, A. Shimony & A. Zeilinger. 1990. Bell's Theorem Without Inequalities. Am. J. Phys. **58:** 1131-1143.

Greenberger D., M. Horne & A. Zeilinger. 1989. Going Beyond Bell's Theorem. In "Bell's theorem, Quantum Theory, and

Conceptions of the Universe". E. Kafatos (ed.). Kluwer, Dordrecht. The Netherlands. 69-72.

Greiner M., O. Mandel, T. Esslinger, T. Hänsch & I. Bloch. 2002. Quantum Phase Transition from a Superfluid to a Mott Insulator in a Gas of Ultracold Atoms. Nature **415:** 39-44.

Grover L. 1997. Quantum Mechanics Helps in Searching for a Needle in a Haystack. Phys. Rev. Lett. **79:** 325-328.

Hayden P., M. Horodecki & B. Terhal. 2001. The Asymptotic Entanglement Cost of Preparing a Quantum State. J. Phys. A: Math. Gen. **34:** 6891-6898.

Herek J. L., W.Wohlleben, R. J. Cogdell, D. Zeidler & M. Motzkus. 2002. Quantum Control of Energy Flow in Light Harvesting. Nature **417:** 533-535.

Horodecki M., P. Horodecki & R. Horodecki. 1996. Separability of Mixed States: Necessary and Sufficient Conditions. Phys. Lett. A **223:** 1-8.

Horodecki M., P. Horodecki & R. Horodecki. 2001. Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments. Springer Tracts in Modern Physics.

Horodecki M. 2001. Entanglement Measures. Quant. Inform. Comput. **1:** 3-26.

Horodecki M. 2005. Simplifying Monotonicity Conditions for Entanglement Measures. Open Syst. Inf. Dyn. **12:** 231-237.

Horodecki R., P. Horodecki, M. Horodecki & K. Horodecki. 2007. Quantum Entanglement. E-print quant-ph/0702225: 1-110.

Hughes R., D. Alde, P. Dyer, G. Luther, G. Morgan & M. Schauer. 1995. Quantum Cryptography. Contemp. Phys. **36:** 149-163.

Imamoglu A., D. Awschalom, G. Burkard, D. Di-Vincenzo, D. Loss, M. Sherwin & A. Small. 1999. Quantum Information Processing Using Quantum Dot Spins and Cavity QED. Phys. Rev. Lett. **83:** 4204-4207.

Jacksch D., H. Briegel, J. Cirac, C. Gardiner & P. Zoller. 1999. Entanglement of Atoms via Cold Controlled Collisions. Phys. Rev. Lett. **82:** 1975-1978.

Jaramillo J. D. & J. H. Reina. 2008. Temporal Resources for Global Quantum Computing Architectures. Brazilian Journal of Physics **38:** 551-557.

Jones J., M. Mosca & R. Hansen. 1998(A). Implementation of a Quantum Search Algorithm on a Quantum Computer. Nature **393:** 344-346.

Jones J., V. Vedral, A. Ekert & G. Castagnoli. 2000. Geometric Quantum Computation Using Nuclear Magnetic Resonance. Nature **403:** 869-871.

Jones J. & M. Mosca. 1998(B). Implementation of a Quantum Algorithm on a Nuclear Magnetic Resonance Quantum Computer. J. Chem. Phys. **109:** 1648-1653.

Jozsa R. & B. Schumacher. 1994. A New Proof of the Quantum Noiseless Coding Theorem. J. Mod. Optics **41:** 2343-2349.

Kamada H., H. Gotoh, J. Temmyo, T. Takagahara & H. Ando. 2001. Exciton Rabi Oscillation in a Single Quantum Dot. Phys. Rev. Lett. **87:** 246401/04.

Kane B. 1998. A Silicon-Based Nuclear Spin Quantum Computer. Nature **393:** 133-137.

Kitaev A. 1997. Fault-Tolerant Quantum Computation by Anyons. E-print quant-ph/9707021.

Knill E., I. Chuang & R. Laflamme. 1998. Effective Pure States for Bulk Quantum Computation. Phys. Rev. A **57:** 3348-3363.

Knill E. & R. Laflamme. 1997. Theory of Quantum Error-Correcting Codes. Phys. Rev. A **55:** 900-911.

Kroutvar M., Y. Ducommun, D. Heiss, M. Bichler, D. Schuh, G. Abstreiter & J. Finley. 2004. Optically Programmable Electron Spin Memory Using Semiconductor Quantum Dots. Nature **432:** 81-84.

Lo H. & H. Chau. 1999. Unconditional Security of Quantum Key Distribution Over Arbitrarily Long Distances. Science **283:** 2050-2056.

Laflamme R., C. Miquel, J. Paz & W. Zurek. 1996. Perfect Quantum Error Correcting Code. Phys. Rev. Lett. 77: 198-201.

Lee H., Y.-C. Cheng & G. R. Fleming. 2007. Coherence Dynamics in Photosynthesis: Protein Protection of Excitonic Coherence. Science **316:** 1462-1465.

Leggett A. J., Chakravarty S, Dorsey A T, Fisher M P A, Garg A and Zwerger W. 1987. Dynamics of the Dissipative Two-State System. Reviews of Modern Physics **59:** 1-85.

Leuenberger M. N. D. Loss, M. Poggio & D. D. Awschalom. 2002. Quantum Information Processing with Large Nuclear Spins in GaAs Semiconductors. Phys. Rev. Lett. **89:** 207601/1-4.

Leuenberger M. N., M. E. Flatte & D. D. Awschalom. 2005. Teleportation of Electronic Many-Qubit States Encoded in the Electron Spin of Quantum Dots via Single Photons. Phys. Rev. Lett. **94:** 107401/1-4.

Leuenberger M. N. & D. Loss. 2001. Quantum Computing in Molecular Magnets. Nature **410:** 789-793.

Loss D. & D. DiVincenzo. 1999. Quantum Computation with Quantum Dots. Phys. Rev. A **57:** 120-126.

Lovett B., J. H. Reina, A. Nazir, B. Kothari & A. Briggs. 2003(A). Resonant Energy Transfer and Quantum Computation. Phys. Lett. A **315:** 136-142.

Lovett B., J. H. Reina, A. Nazir & A. Briggs. 2003(B). Optical Schemes for Quantum Computation in Quantum Dot Molecules. Phys. Rev. B **68:** 205319/1-18.

Lloyd S. 1995. Almost Any Quantum Logic Gate is Universal. Phys. Rev. Lett. **75:** 346-349.

Lloyd S. 1993. A Potentially Realizable Quantum Computer. Science **261:** 1569-1571.

Makhlin Y., G. Schön & A. Shnirman. 1999. Josephson-Junction Qubits with Controlled Couplings. Nature **398:** 305-307.

Makhlin Y., G. Schön & A. Shnirman. 2001. Quantum-State Engineering with Josephson-Junction Devices. Rev. Mod. Phy. **73:** 357-400.

Makri N. & D. E. Makarov. 1995. Numerical Path-Integral Techniques for Long-Time Dynamics of Quantum Dissipative Systems. J. Math. Phys. **36:** 2430-2457.

Mandel O., M. Greiner, A. Widera, T. Rom, T. W. Hänsch & I. Bloch. 2003. Controlled Collisions for Multi-Particle Entanglement of Optically Trapped Atoms. Nature **425:** 937.

Mayers D. 1998. Unconditional Security in Quantum Cryptography. E-print quant-ph/9802025.

Mermin N. 1985. Is the Moon There When Nobody Looks? Reality and the Quantum Theory. Physics Today **38:** 38-47.

Meyer D. 1999. Quantum Strategies. Phys. Rev. Lett. **82:** 1052-1055.

Meyer D. 2000. Quantum Games and Quantum Algorithms. E-print quant-ph/0004092.

Molmer K. & A. Sorensen. 1999. Multiparticle Entanglement of Hot Trapped Ions. Phys. Rev. Lett. **82:** 1835-1838.

Monroe C., D. Meekhof, B. King, W. Itano & D. Wineland. 1995. Demonstration of a Fundamental Quantum Logic Gate. Phys. Rev. Lett. **75:** 4714-4717.

Montes E., J. Calero & J. H. Reina. 2009. Dissipative Dynamics of Superconducting Hybrid Qubit Systems. J. Phys.: Conf. Series **167:** 012014/1-5.

Mujica C., J. C. Arce, J. H. Reina & M. Thorwart. 2009. Molecular Architectures Based on π-Conjugated Block Copolymers for Global Quantum Computation. J. Phys.: Conf. Series **167:** 012061/1-5.

Nakamura Y., Y. Pashkin & J. Tsai. 1999. Coherent Control of Macroscopic Quantum States in a Single-Cooper-Pair Box. Nature **398:** 786-788.

Nazir A., B. Lovett, S. Barrett, J. H. Reina & A. Briggs. 2005. Anticrossings in Förster Coupled Quantum Dots. Phys. Rev. B **71:** 045334/1-12.

Nielsen M. A. & J. Kempe. 2001. Separable States Are More Disordered Globally than Locally. Phys. Rev. Lett **86:** 5184-5187.

Pachos J., P. Zanardi & M. Rasetti. 1999. Non-Abelian Berry Connections for Quantum Computation. Phys. Rev. **A 61:** 010305-10308(R).

Pachos J. & S. Chountasis. 2000. Optical Holonomic Quantum Computer. Phys. Rev. **A 62:** 052318-52326.

Palma G. M., K.-A. Suominen & A. Ekert. 1996. Quantum Computers and Dissipation. Proc. Roy. Soc. Lond. A **452:** 567-584.

Paz-Silva G. A. & J. H. Reina. 2009. Total Correlations as Multi-Additive Entanglement Monotones. Journal of Physics A: Math. Theor. **42:** 055306/1-12.

Paz-Silva G. A. & J. H. Reina. 2008. Characterizing Total Correlations in Multipartite Systems. Microelectron. J. **39:** 699-701.

Paz-Silva G. A. & J. H. Reina. 2007. Geometric Multipartite Entanglement Measures. Phys. Lett. A **365:** 64-69.

Pellizzari T., S. Gardiner, J. Cirac & P. Zoller. 1995. Decoherence, Continuous Observation, and Quantum Computing: A Cavity QED Model. Phys. Rev. Lett. **75:** 3788-3791.

Peres A. 1993. Quantum Mechanics: Concepts and Methods. Kluwer. Dordrecht.

Peres A. 1996. Separability Criterion for Density Matrices. Phys. Rev. Lett. 77: 1413-1415.

Peres A. 1999. All the Bell Inequalities. Found. Phys. **29:** 589-614.

Phoenix S. & P. Townsend. 1995. Quantum Cryptography: How to Beat the Code Breakers Using Quantum Mechanics. Contemp. Phys. **36:** 165-195.

Plenio M. B. & S. Virmani. 2007. An Introduction to Entanglement Measures. Quant. Inf. Comp. **7:** 1-51. E-print quant-ph/0504163.

Popescu S. 1994. Bell's Inequalities Versus Teleportation: What is Nonlocality? Phys. Rev. Lett. **72:** 797-799.

Popescu S. 1995. Bell's Inequalities and DensityMatrices: Revealing Hidden Nonlocality. Phys. Rev. Lett. **74:** 2619-2622.

Popescu S. & D. Rohrlich. 1997. Thermodynamics and the Measure of Entanglement. Phys. Rev. A **56:** 3319-3321(R).

Preskill J. 1998. Reliable Quantum Computers. Proc. R. Soc. Lond. A **454:** 385-410.

Pretel A., J. H. Reina & R. W. Aguirre. 2008. Excitonic Dynamics of a Quantum Dot Coupled to a Laser-Driven Semiconductor Microcavity. Microelectron. J. **39:** 682-684.

Prevedel R., P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein & A. Zeilinger. 2007. High-Speed Linear Optics Quantum Computing Using Active Feed-Forward. Nature **445:** 65-69.

Privman V., L. Vagner & G. Kventsel. 1998. Quantum Computation in Quantum-Hall Systems. Phys. Lett. A **239:** 141-146.

Quiroga L. & N. Johnson. 1999. Entangled Bell and Greenberger-Horne-Zeilinger States of Excitons in Coupled Quantum Dots. Phys. Rev. Lett. **83:** 2270-2273.

Rabi P., D. DeMille, J. Doyle, M. Lukin, R. Schoelkopf & P. Zoller. 2006. Hybrid Quantum Processors: Molecular Ensembles as Quantum Memory for Solid State Circuits. Phys. Rev. Lett. **97:** 033003/1-4.

Rains E. M. 1999. Rigorous Treatment of Distillable Entanglement. Phys. Rev. A **60:** 173-178.

Rauschenbeutel A., G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J. Raimond & S. Haroche. 1999. Coherent Operation of a Tunable Quantum Phase Gate in Cavity QED. Phys. Rev. Lett. **83:** 5166-5169.

Rauschenbeutel A., P. Bertet, S. Osnaghi, G. Nogues, M. Brune, J. Raimond & S. Haroche. 2001. Controlled Entanglement of Two Field Modes in a Cavity Quantum Electrodynamics Experiment. Phys. Rev. A **64:** 050301-50304(R).

Raussendorf, R., & H. J. Briegel. 2001. A One-Way Quantum Computer. Phys. Rev. Lett. **86:** 5188-5191.

Raussendorf, R., D. E. Browne & H. J. Briegel. 2003. Measurement based Quantum Computation on Cluster States. Phys. Rev. A **68:** 022312/1-32.

Reina J. H., L. Quiroga & N. Johnson. 2000(A). NMR-based Nanostructure Switch for Quantum Logic. Phys. Rev. B **62:** 2267-2270(R).

Reina J. H., L. Quiroga & N. Johnson. 2000(B). Quantum Entanglement and Information Processing via Excitons in Optically Driven Quantum Dots. Phys. Rev. A **62:** 012305/1-8.

Reina J. H., L. Quiroga & N. Johnson. 2000(C). Quantum Information Processing in Semiconductor Nanostructures. Invited chapter, Proceedings of the ISI-Accademia dei Lincei Conference on "Conventional and Non Conventional Computing (Quantum and DNA)". Springer Verlag. E-print quant-ph/0009035.

Reina J. H. & N. Johnson. 2000(D). Quantum Teleportation in a Solid-State System. Phys. Rev. A **63:** 012303 /1-5.

Reina J. H., L. Quiroga & N. Johnson. 2002. Decoherence of Quantum Registers. Phys. Rev. A **65:** 032326/1-15.

Reina J. H., R. Beausoleil, T. Spiller & W. Munro. 2004. Radiative Corrections and Quantum Gates in Molecular Systems. Phys. Rev. Lett. **93:** 250501/1-4.

Reina J. H. & A. Bririd. 2008. Path Integral Approach to Dissipation in Solid-State Qubits. Microelectron. J. **39:** 696-698.

Robledo L., J. Elzerman, G. Jundt, M. Atatüre, A. Högele, S. Fält & A. Imamoglu. 2008. Conditional Dynamics of Interacting Quantum Dots. Science **320:** 772-775.

Riebe, M., H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James & R. Blatt. 2004. Deterministic Quantum Teleportation with Atoms. Nature 429, 734-737.

Rivest R., A. Shamir & L. Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of the ACM **21**(2): 120-126.

Sackett C. A., D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland & C. Monroe. 2000. Experimental Entanglement of Four Particles. Nature **404:** 256-259.

Sherson J. F., H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac & E. S. Polzik. 2006. Quantum Teleportation Between Light and Matter. Nature **443:** 557-560.

Schrödinger E. 1935. Die Gegenwrtige Situation in der Quantenmechanik. Natürwissenschaften **23:** 807-812; 823-828; 844-849.

Schumacher B. 1995. Quantum Coding. Phys. Rev. A **51:** 2738-2747.

Selleri F. 1989. Quantum Paradoxes and Physical Reality. Kluwer. Dordretch.

Shapere A. & F. Wilczek. 1989. Geometric Phases in Physics. World Scientific. Singapore.

Shnirman A., G. Schön & Z. Hermon. 1997. Quantum Manipulations of Small Josephson Junctions. Phys. Rev. Lett. **79:** 2371-2374.

Shor P. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science. IEEE Computer Society. Santa Fe. Los Alamitos (CA): 124-134. A revised version can be found in (**Shor,** 1997(A)).

Shor P. 1995. Scheme for Reducing Decoherence in Quantum Computer Memory. Phys. Rev. A **52:** 2493-2496(R).

Shor P. 1997(A). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAMJournal on Computing **26:** 1484-1509. E-print quant-ph/9508027.

Shor P. 1997(B). Fault-tolerant Quantum Computation. 37th Annual Symposium on Foundations of Computer Science (FOCS '96), pp. 56. E-print quantph/ 9605011v2.

Shor P. 2002. Additivity of the Classical Capacity of Entanglement-Breaking Quantum Channels. J. Math. Phys. **43:** 4334-4340. See also the other papers (Vol. 43, Issue 9) of the Special Issue: Quantum Information Theory.

Shor P. 2004. Equivalence of Additivity Questions in Quantum Information Theory. Comm. Math. Phys. **246:** 453-472.

Simon D. 1994. On the Power of Quantum Computation. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science. IEEE Computer Society. Santa Fe. Los Alamitos (CA). 116-123.

Steane A. 1996(A). Error Correcting Codes in Quantum Theory. Phys. Rev. Lett. **77:** 793-797.

Steane A. 1996(B). Multiple-Particle Interference and Quantum Error Correction. Proc. R. Soc. Lond. A **452:** 2551-2577.

Steane A. 1996(C). Simple Quantum Error-Correcting Codes. Phys. Rev. A **54:** 4741-4751.

Steane A. 1997. Active Stabilization, Quantum Computation, and Quantum State Synthesis. Phys. Rev. Lett. **78:** 2252-2255.

Steane A. 1998. Quantum Computing. Rep. Prog. Phys **61:** 117-173.

Terhal B. M. 2000. Bell Inequalities and the Separability Criterion. Phys. Lett. A **271:** 319-326.

Thorwart M., J. Eckel, J. H. Reina & S. Weiss. 2009. Enhanced Quantum Entanglement in the Non-Markovian Dynamics of Biomolecular Excitons. To appear in Chem. Phys. Lett. E-print arXiv:0808.2906.

Tittel W., J. Brendel, H. Zbinden & N. Gisin. 1998. Violation of Bell Inequalities by Photons More Than 10 km Apart. Phys. Rev. Lett. **81:** 3563-3566.

Toffoli T. 1980. Reversible Computing. Lecture Notes in Computer Science 85. Automata, Languages and Programming. Springer. Berlin. 632-644.

Trauzettel B., D. V. Bulaev, D. Loss & G. Burkard. 2007. Spin Qubits in Graphene Quantum Dots. Nature Physics **3:** 192-196.

Troiani F., U. Hohenester & E. Molinari. 2000. Exploiting Exciton-Exciton Interactions in Semiconductor Quantum Dots for Quantum-Information Processing. Phys. Rev. B **62:** 2263-2266(R).

Turchete Q., C. Hood, W. Lange, H. Mabuchi & H. Kimble. 1995. Measurement of Conditional Phase Shifts for Quantum Logic. Phys. Rev. Lett. **75:** 4710-4713.

Uhlmann A. 1998. Optimizing Entropy Relative to a Channel or a Subalgebra. Open Syst. & Inf. Dyn. **5:** 209-227.

Vandersypen L., M. Steffen, G. Breyta, C. Yannoni, M. Sherwood & I. Chuang. 2001. Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance. Nature **414:** 883-887.

van der Wal C., A. Haar, F. Wilhelm, R. Schouten, C. Harmans, T. Orlando, S. Lloyd & J. Mooij. 2000. Quantum Superposition of Macroscopic Persistent-Current States. Science **290:** 773-777.

Vedral V., A. Barenco & A. Ekert. 1995. Quantum Networks for Elementary Arithmetic Operations. Phys. Rev. A **54:** 147-153.

Vedral V. & M. B. Plenio. 1998. Entanglement Measures and Purification Procedures. Phys. Rev. A **57:** 1619-1633.

Vedral V. 2008. Quantifying Entanglement in Macroscopic Systems. Nature **453:** 1004-1007.

Vidal G. & R. F. Werner. 2002. Computable Measure of Entanglement. Phys. Rev. A **65:** 032314/1-11.

Vidal G. 2000. Entanglement Monotones. J. Mod. Opt. **47:** 355-376.

von Neumann J. & O. Morgenstern. 1953. Theory of Games and Economic Behavior. Third edition. Princeton University Press.

Vrijen R., E. Yablonovitch, K. Wang, H. Jiang, A. Balandin, V. Roychowdhury, T. Mor & D. DiVincenzo. 2000. Electron-Spin-Resonance Transistors for Quantum Computing in Silicon-Germanium Heterostructures. Phys. Rev. A **62:** 012306-12315.

Walther P., K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer & A. Zeilinger. 2006. Experimental One-Way Quantum Computing. Nature, **434:** 169-176.

Weihs G., T. Jennewein, C. Simon, H. Weinfurter & A. Zeilinger. 1998. Violation of Bell's Inequality under Strict Einstein Locality Conditions. Phys. Rev. Lett. **81:** 5039- 5043.

Weiss U. 2008. Quantum Dissipative Systems. 3rd ed. (Singapore: World Scientific).

Werner R. 1989. Quantum States with Einstein-Podolsky-Rosen Correlations Admitting a Hidden-Variable Model. Phys. Rev. A **40:** 4277-4281.

Wilczek F. & A. Zee. 1984. Appearance of Gauge Structure in Simple Dynamical Systems. Phys. Rev. Lett. **52:** 2111-2114.

Wootters W. K. & W. Zurek. 1982. A Single Quantum Cannot be Cloned. Nature **299:** 802-803.

Wootters W. K. 1998. Phys. Rev. Lett. **80:** 2245-2248.

Xiang-Bin W. & M. Keiji. 2001. Nonadiabatic Conditional Geometric Phase Shift with NMR. Phys. Rev. Lett. **87:** 097901/1-4.

Xiang-Bin W. K. Matsumoto, H. Fan, A. Tomita & J. Pan. 2001. A Simple Way to Detect the State Transition Caused by the Nondiagonal Abelian Berry Phase. E-print quant-ph/0112071.

Zanardi P. & M. Rasetti. 1999. Holonomic Quantum Computation. Phys. Lett. A **264:** 94-99.

Zbinden H., J. Gautier, N. Gisin, B. Huttner, A. Muller & W. Tittel. 1997. Interferometry with Faraday Mirrors for Quantum Cryptography. Electron. Lett. **33**(7): 586-588.

Zhang Q., A. Goebel, C. Wagenknecht, Y.-A. Chen, B. Zhao, T. Yang, A. Mair, J. Schmiedmayer & J.-W. Pan. 2006. Experimental Quantum Teleportation of a Two-Qubit Composite System. Nature Physics **2:** 678-682.

Zukowski M., R. Horodecki, M. Horodecki & P. Horodecki. 1998. Generalized Quantum Measurements and Local Realism. Phys. Rev. A **58:** 1694-1698.

Zurek W. 1991. Decoherence and the Transition from Quantum to Classical. Physics Today **44:** 36-44.

Zurek W. 2002. Decoherence and the Transition from Quantum to Classical-Revisited. Los Alamos Science **27:** 1-24.

Zurek W. 2003. Decoherence, Einselection, and the Quantum Origins of the Classical. Reviews of Modern Physics **75:** 715-765. E-print quant-ph/0105127.

Recibido: abril 11 de 2009.

Aceptado para su publicación: mayo 30 de 2009.