

## Chapter 2

# Quantum Information

Quantum information deals with the information processing tasks that can be accomplished by using the laws of quantum mechanics. Its aim is to develop suitable strategies in particular for quantum computation and quantum communication, but also for quantum metrology and quantum simulation. In this chapter, I briefly provide an introduction to the wide range of topics concerning quantum information and recall some basic theoretical elements, to which I will refer in this thesis.

### 2.1 Why Quantum Information

Information theory was introduced by Shannon in 1948 and extended to the quantum world by Feynmann in the early 1980s with the hypothesis that quantum mechanics could be used to process and transmit information [1]. It has been demonstrated that by encoding information on quantum systems many interesting advantages arise, like the enhancement of security in communication protocols, or the speed up of computational algorithms [2].

Moreover, Feynman suggested that a quantum computer would be ideal for simulating quantum-mechanical systems, an unachievable task for classical computers [1].

These promising applications made quantum information a very attractive field: the first experiments took place about 20 years ago and since the 1990s many QI protocols have been developed and realized.

In the following I give a brief description of this wide range of application fields within the large context of quantum information.

### 2.1.1 Quantum Computation

A quantum computer is a system of many qubits (two-level quantum systems), whose evolution can be controlled, and a quantum computation is a unitary transformation that acts on this many-qubit state [3]. The power of quantum computers resides on fundamental quantum laws, such as the quantum superposition principle and entanglement. Entanglement is at the heart of many quantum-information protocols. It is the most intriguing and counter-intuitive manifestation of quantum mechanics, observed in composite quantum systems: it signifies the existence of non-local correlations between measurements performed on separated particles [4].

A quantum computer would allow to solve certain computational problems much more efficiently than a classical computer [3]. These include basic problems of computer science: from the search of a marked item in an unstructured database to integer factoring. In 1994, Peter Shor proposed a quantum algorithm that efficiently solves the prime-factorization problem: given a composite integer, find its prime factors [5, 6]. This is a central problem in computer science and it is conjectured, though not proven, that for a classical computer it is computationally difficult to find the prime factors. Shor's algorithm efficiently solves the integer factorization problem and therefore it provides an exponential improvement in speed with respect to any known classical algorithm. For example, there are cryptographic procedures, such as RSA [7], extensively used today and that are based on the conjecture that no efficient algorithms exist for solving the prime factorization problem. Shor's algorithm, if implemented on a large-scale quantum computer, would break the RSA cryptosystem. Lov Grover has shown that quantum mechanics can also be useful for solving the problem of searching for a marked item in an unstructured database [8]. In this case, the gain with respect to classical computation is quadratic.

The technological challenge of realizing a quantum computer is very demanding: we need to be able to control the evolution of a large number of qubits for the time necessary to perform many quantum gates. Decoherence may be considered the ultimate obstacle to the practical realization of a quantum computer. Here the term decoherence denotes the decay of the quantum information stored in a quantum system, due to its unavoidable interaction with the environment. Such interaction affects the performance of a quantum computer, introducing errors into the computation. Another source of errors that must be taken into account is the presence of imperfections in the quantum-computer hardware. Even though quantum error-correcting codes exist, a necessary requirement for a successful correction procedure is that one can implement many quantum gates inside the decoherence time scale. Notwithstanding the many limitations connected with the experimental realizations, a quantum computer still seems to be an achievable task.

### 2.1.2 Quantum Communication

Another important research direction concerns the (secure) transmission of information. In this case, quantum mechanics allows us to perform not only faster operations but also operations inaccessible to classical means. Among the various features of quantum systems, entanglement is central to many quantum-communication protocols. Of particular importance are *quantum dense coding* [9], which permits transmission of two bits of classical information through the manipulation of only one of two entangled qubits, and *quantum teleportation* [10, 11], which allows the transfer of the state of one quantum system to another over an arbitrary distance. Quantum mechanics also provides a unique contribution to cryptography, i.e. secret communication. Quantum cryptography enables two communicating parties, namely Alice (the sender) and Bob (the receiver), to detect whether the transmitted message has been intercepted by Eve (an eavesdropper). This is a consequence of a basic property of quantum mechanics, the “no-cloning theorem”: an unknown quantum state cannot be cloned [12]. In the context of quantum cryptography the most popular protocol is the one introduced by Bennet and Brassard in 1984 [13], the so called *BB84 protocol*, which enables Alice and Bob to discover whether any eavesdropper is trying to catch information from their communication channel. This task is achieved by exploiting states prepared from Alice and measured by Bob in different basis, whose states correspond to eigenstates of non-commuting observables. In the ideal formulation of the protocol any channel attack is recognized with certainty, while in presence of noise and errors, as it happens in practical realizations, the probability of detecting an eavesdropper decreases. Nevertheless, in analogy to their classical counterparts, a theory of quantum error-correction has been developed which allows quantum computers to compute effectively in the presence of noise, and also allows communication over noisy quantum channels to take place reliably [5].

### 2.1.3 Quantum Simulation

Quantum simulation can be seen as a relevant class of quantum algorithms: algorithms for simulation of physical systems. Simulating one quantum system using another more controllable one has turned out to be not so easy, indeed. However, a lot of progress has been made since 1982, when Feynman delivered his seminal lecture ‘Simulating Physics with Computers’ [1]. The wide advances in isolating, manipulating and detecting single quantum systems—particularly in the past decade or so—allow us to say that physical implementations of ‘quantum simulators’ are now becoming a reality. Quantum simulations are being implemented in, or have been proposed for, a number of other systems—among them nuclear spins addressed using NMR methodology, and electron spins in quantum dots or in point defects. Each platform has its own advantages and limitations, and different approaches often tackle complementary aspects of quantum simulation. Each of them aims to solve problems

that are computationally too demanding to be solved on classical computers. Furthermore, the simultaneous development of different platforms for practical quantum simulation offers the intriguing prospect of verifying, once uncharted territory is reached, one simulator using another. In fact, implementing quantum simulations that are too complex for the most powerful classical computers should be already a short-term goal. This is reported in detail in Part III.

### 2.1.4 Quantum Metrology

As a last scenario quantum metrology is the study of performing high-resolution and highly sensitive measurements of physical parameters using quantum theory to describe the physical systems, particularly exploiting quantum entanglement. This field promises to develop measurement techniques that give better precision than the same measurement performed in a classical framework. One example worth noting is given by the use of the so-called N00N state in a Mach-Zender interferometer to perform accurate phase measurements [14, 15]. A similar effect can be obtained by using other quantum states, such as squeezed states [16].

## 2.2 Basic Elements of Quantum Information

The above brief landscape of quantum information tasks highlights how exploitation of quantum systems in the context of quantum information is a promising scenario, not only for fundamental research in quantum mechanics, but also for technological realizations.

Let us now move to recall some basic concepts of quantum information theory.

### 2.2.1 The Quantum Bit

Quantum information is built upon the concept of “quantum bit” or *qubit*. Qubits are represented by two-level quantum systems so  $\{|0\rangle, |1\rangle\}$  represent the ground and excited state of such a system. These two states constitute the computational basis and are defined in a bi-dimensional Hilbert space. At variance with the classical case, the general state of a qubit is given by a superposition:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

where  $\alpha, \beta$  are complex coefficients satisfying  $|\alpha|^2 + |\beta|^2 = 1$ . Because of this last relation it is possible to rewrite the state (2.1) in the following way:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle. \quad (2.2)$$

The numbers  $\theta$  and  $\phi$  define a point on a unit three-dimensional sphere, known as Bloch sphere. Each point on this sphere represents a possible state of a qubit.

### 2.2.2 The Density Matrix

A possible representation of a state of the system is given by the *density matrix*. If the system is in the pure state  $|\psi\rangle$ , the associated density matrix is

$$\rho = |\psi\rangle\langle\psi|, \quad (2.3)$$

which satisfies the property  $\rho^2 = \rho$ . In the case of mixed states, i.e. for an incoherent mixture of pure states  $\{|\psi_a\rangle\}$ , the density matrix reads:

$$\rho = \sum_a p_a |\psi_a\rangle\langle\psi_a|, \quad (2.4)$$

where  $0 < p_a \leq 1$  are the probabilities associated with each  $|\psi_a\rangle$  and the relation  $\sum_a p_a = 1$  holds. In general for a mixed state  $\rho^2 \neq \rho$ .

### 2.2.3 Bi-Partite Systems and Entanglement

Let us now consider two systems, namely  $A$  and  $B$ , belonging to the Hilbert spaces  $\mathcal{H}_A$  and  $\mathcal{H}_B$  respectively. For a pure state of the joint system the state vector is

$$|\psi\rangle_{AB} = \sum_{ij} a_{ij} |i\rangle_A |j\rangle_B, \quad (2.5)$$

where  $\{|i\rangle_A\}$  and  $\{|j\rangle_B\}$  are two complete bases for systems  $A$  and  $B$  respectively, and  $a_{ij}$  are complex numbers satisfying the condition  $\sum_{ij} |a_{ij}|^2 = 1$ . This state belongs to the Hilbert space  $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$  of dimension  $d = d_A \times d_B$ ,  $d_A$  ( $d_B$ ) being the dimension of the subspace  $\mathcal{H}_A$  ( $\mathcal{H}_B$ ).

When dealing with bi-partite systems, two classes of states can be recognized: the separable states and the entangled ones. A state is separable if it can be decomposed as the inner product of a wavefunction of the first system ( $A$ ) and a wavefunction of the second system ( $B$ ) and it is written as:

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B \quad (2.6)$$

otherwise it is called entangled. This can be generalized for mixed states as well [17]. The space  $\mathcal{H}_{AB}$  is described by a basis of  $d$  states which can be either separable or entangled. For  $d = 4$  the so called Bell states

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}} (|0, 0\rangle + |1, 1\rangle) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}} (|0, 0\rangle - |1, 1\rangle) \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}} (|0, 1\rangle + |1, 0\rangle) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}} (|0, 1\rangle - |1, 0\rangle) \end{aligned} \quad (2.7)$$

represent a basis of entangled states for two-qubit systems.

Entanglement is not only a pure mathematical representation, it represents one of the building blocks of quantum mechanics. Indeed entanglement explains non classical correlation between systems, which has been experimentally observed through Bell inequalities violation [18, 19] and, as previously mentioned, it is the fundamental feature of many quantum information protocols.

## 2.3 Quantum Gates

Changes occurring to a quantum state can be described using the language of quantum computation. Classical computer circuits consist of wires and logic gates. The wires are used to carry information around the circuit, while the logic gates perform manipulations of the information, converting it from one form to another. The two classical single-bit gates are the identity—each bit remain unchanged under this operation—and the NOT gate—in which  $0 \rightarrow 1$  and  $1 \rightarrow 0$ , that is, the 0 and 1 states are interchanged, while there are many gates operating on two-bit inputs.

At the quantum level, operations on a single qubit must preserve its norm, and thus are described by  $2 \times 2$  unitary matrices. Among all these, it is useful to mention the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (2.8)$$

which are widely adopted as basis for description of single-qubit operations.

Other important single-qubit maps are the Hadamard gate and the Phase Shift:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \quad (2.9)$$

respectively. The Hadamard rotates by an angle  $\pi/2$  the computational basis, thus transforming the states  $|0\rangle$  and  $|1\rangle$  into  $|\pm\rangle = \frac{1}{\sqrt{2}}[|0\rangle \pm |1\rangle]$ , while  $S$  introduces a phase shift  $\phi$  between the two basis states. It is also useful to remember operators

associated with rotations of qubits whose expression reads

$$\mathcal{R}_j(\theta) = e^{-i\theta\sigma_j}, \quad j = x, y, z. \quad (2.10)$$

As well as single-qubit gates, there are many two-qubit logic gates. In particular the Controlled-NOT (CNOT) gate is important for quantum information processing and, when combined with single-qubit gates, represents a universal set of operations that can be combined to perform any arbitrary computation. Qubits undergoing the CNOT are labeled *target* and *control*: the gate flips the target qubit depending on the state of the control qubit (in this sense it is a *controlled* gate) [3]. The operator representing this gate is the following  $4 \times 4$  matrix

$$\mathcal{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (2.11)$$

In 2001 Knill et al. demonstrated that scalable universal quantum computing can be achieved with single photons using only linear optics and photon counting measurements [20]. This is based upon the measurement-induced nonlinearity that arises in two-photon, Hong-Ou-Mandel interference [21]. Furthermore, it has been demonstrated that, a general quantum transformation can be achieved by using single qubit gates and one two-qubit gate, thus the CNOT, the most adopted two-qubit gate, is considered one of the building blocks of a quantum computer. More details about this gate are given in Sect. 6.2.

## 2.4 Quantum Processes and Time Evolution

In the present section we describe the formalism for the time evolution of a physical system. For closed systems, the time evolution is described by the Schrödinger equation, which permits to obtain the state vector of a physical system at time  $t$  according to the action of a unitary operator on the initial state. Such a description in terms of unitary operators cannot be adopted in the case of an open system, i.e. interacting with an additional system not accessible by the observer. In this case, the time evolution of the system is described by a completely positive map acting on the density operator [3].

### 2.4.1 Unitary Evolution of Closed Systems

The time evolution properties of a closed physical system are defined by the quantum mechanical extension  $\hat{\mathcal{H}}$  of the classical Hamiltonian  $\mathcal{H}$ . The operator  $\hat{\mathcal{H}}$  acts as

the generator of the time evolution of such a system according to the Schrödinger equation

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{\mathcal{H}}|\psi\rangle; \quad \frac{\partial \hat{\rho}}{\partial t} = -\frac{i}{\hbar}[\hat{\mathcal{H}}, \hat{\rho}], \quad (2.12)$$

where  $[\hat{\mathcal{H}}, \hat{\rho}]$  is the commutator between the two operators [17]. The time evolution at a fixed time  $t$  of a state vector in the initial state  $|\psi(0)\rangle$  and on a density matrix  $\hat{\rho}(0)$  at  $t = 0$  can be obtained as:

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle; \quad \hat{\rho}(t) = \hat{U}(t)\hat{\rho}(0)\hat{U}^\dagger(t), \quad (2.13)$$

where  $\hat{U}(t)$  is a unitary operator describing the evolution of the system.

The expectation value at time  $t$  of a physical observable  $\hat{O}$ , can be then evaluated as the average value over the density matrix  $\hat{\rho}(t)$ , or equivalently, we can consider that the time evolution modifies the action of the observable  $\hat{O}$  without affecting the state  $\hat{\rho}(0)$ . We obtain the two equivalent formulations:

$$\langle \hat{O} \rangle(t) = \text{Tr}[\hat{\rho}(t)\hat{O}] = \text{Tr}[\hat{\rho}\hat{O}(t)]. \quad (2.14)$$

Here,  $\hat{O}(t) = \hat{U}^\dagger(t)\hat{O}\hat{U}(t)$  is the time evolution induced by the Heisenberg equation

$$\frac{\partial \hat{O}}{\partial t} = \frac{i}{\hbar}[\hat{\mathcal{H}}, \hat{O}]. \quad (2.15)$$

The two representations are called the Schrödinger and Heisenberg pictures respectively.

### 2.4.2 Nonunitary Evolution: Quantum Maps

Unitary operators with Hamiltonian generators describe the time evolution of closed physical systems. In general, for any open quantum system it is not possible to describe time evolution in terms of unitary operators acting on the system. However, such evolution can be described in terms of quantum maps  $\mathcal{E}$ , which must obey the following constraints [3]:

- (1) *Hermiticity*—If  $\hat{\rho}^\dagger = \hat{\rho}$ , then  $\hat{\rho}' = \mathcal{E}[\hat{\rho}]$  must satisfy  $(\hat{\rho}')^\dagger = \hat{\rho}'$ .
- (2) *Trace preserving*—If  $\text{Tr}(\hat{\rho}) = 1$ , then  $\hat{\rho}' = \mathcal{E}[\hat{\rho}]$  must satisfy  $\text{Tr}(\hat{\rho}') = 1$ .
- (3) *Complete positivity*—Consider a density matrix acting on a Hilbert space  $\mathcal{H}_A$ . A map  $\mathcal{E}$  is completely positive (CP) if for any extension of the Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  the map  $\mathcal{E}_A \otimes \mathbb{1}_B$  is positive. Recall that a map is positive if  $\hat{\rho}' = \mathcal{E}[\hat{\rho}]$  is nonnegative when  $\hat{\rho}$  is nonnegative.
- (4) *Linearity*—If  $\hat{\rho} = \lambda\hat{\rho}_1 + (1 - \lambda)\hat{\rho}_2$ , then  $\mathcal{E}[\hat{\rho}] = \lambda\mathcal{E}[\hat{\rho}_1] + (1 - \lambda)\mathcal{E}[\hat{\rho}_2]$ .



It can be demonstrated that for a map  $\mathcal{E}$  which obeys the constraints (1)–(4), it is always possible to represent the map in the following form:

$$\mathcal{E}[\hat{\rho}] = \sum_{\mu} \hat{M}_{\mu} \hat{\rho} \hat{M}_{\mu}^{\dagger}, \quad (2.16)$$

where  $\{\hat{M}_{\mu}\}$  is a set of operators satisfying  $\sum_{\mu} \hat{M}_{\mu}^{\dagger} \hat{M}_{\mu} = \hat{1}$  [22]. Note that the number of operators in the set  $\{\hat{M}_{\mu}\}$  in general is not bounded by the dimension of the Hilbert space  $\mathcal{H}_A$ . This decomposition of quantum maps  $\mathcal{E}$  is known as the *Kraus representation theorem* [22], and provides a powerful tool to represent the time evolution of a general open system. The action of the map  $\mathcal{E}$  in the Kraus representation can be also expressed in terms of the action of a rank-4 tensor on the density matrix  $\hat{\rho}$ . By choosing an orthonormal basis  $\{|i\rangle\}$ , the elements of the density matrix  $\mathcal{E}[\hat{\rho}]$  can be evaluated as:

$$(\mathcal{E}[\hat{\rho}])_{l,k} = \sum_{n,m} \mathcal{E}_{l,k}^{n,m} \rho_{n,m}, \quad (2.17)$$

where  $\hat{\rho} = \sum_{n,m} \rho_{n,m} |n\rangle\langle m|$ , and:

$$\mathcal{E}_{l,k}^{n,m} = \sum_{\mu} \langle l | \hat{M}_{\mu} | n \rangle \langle m | \hat{M}_{\mu}^{\dagger} | k \rangle. \quad (2.18)$$

## 2.5 Quantum State Tomography

Quantum state tomography is an experimental procedure which allows determination of the density matrix associated with a system. It is achieved by measuring some system observables. Clearly, with only one measurement we are not able to know exactly the state of the system or to distinguish between non-orthogonal states, so we repeat the same measurements over a sample of many copies of the system under consideration thus achieving the complete knowledge about its state [23, 24].

Let us consider, for simplicity, many copies of a two level system. Its state is described by a  $2 \times 2$  density matrix. It is well known that any  $2 \times 2$  matrix can be decomposed as a sum of 4 linearly independent matrices which form a basis for the space of  $2 \times 2$  matrices. We can choose as a basis the identity matrix and the three Pauli matrices (2.8). Thus the state of the system can be written as:

$$\rho = c_0 \mathbb{1} + c_1 \sigma_x + c_2 \sigma_y + c_3 \sigma_z, \quad (2.19)$$

where  $c_j = \text{Tr}[\sigma_j \rho]$  and  $\sum_j |c_j|^2 = 1$ , thus (2.19) can be rewritten as:

$$\rho = \text{Tr}[\rho] \mathbb{1} + \text{Tr}[\sigma_x \rho] \sigma_x + \text{Tr}[\sigma_y \rho] \sigma_y + \text{Tr}[\sigma_z \rho] \sigma_z. \quad (2.20)$$

Let us recall that expressions like  $Tr[A\rho]$  have the interpretation of the average value of observables. Now our task is to determine the values  $Tr[\sigma_j\rho]$ : for example, to estimate  $Tr[\sigma_z\rho]$  we measure the observable  $\sigma_z$  a large number of times,  $m$ , obtaining outcomes  $z_1, z_2, \dots, z_n$  all equal to  $+1$  or  $-1$ . The empirical average of these quantities,  $\sum_i z_i/m$ , is an estimate for the true value of  $Tr[\sigma_z\rho]$ . We can use the central limit theorem to determine how well this estimate behaves for large  $m$ , where it becomes approximately Gaussian with average equal to  $Tr[\sigma_z\rho]$  and standard deviation  $\Delta(\sigma_z)/\sqrt{m}$ , where  $\Delta(\sigma_z)$  is the standard deviation for a single measurement of  $\sigma_z$ , which is upper bounded by 1. Hence the standard deviation in our estimate  $\sum_i z_i/m$  is at most  $1/\sqrt{m}$ . In a similar way we can estimate the quantities  $Tr[\sigma_x\rho]$  and  $Tr[\sigma_y\rho]$  with a high degree of confidence in the limit of a large sample size, and thus obtain a good estimate for  $\rho$ .

Such measurements are easily achieved in an experimental setup by adopting the proper basis to be measured. This procedure can be extended to systems with a higher dimensionality, but clearly the number of measurements will grow: if  $d$  is the dimension of the system under consideration, the number of measurements is given by  $d^2 - 1$ .

A similar method may be adopted for the experimental reconstruction of quantum processes: this argument is detailed in Chap. 7.

## 2.6 Comparison Between Theory and Experiment

Let us now ask how to compare the experimentally reconstructed quantum state with the theoretical prediction, or how much two items of information are similar. A quantitative answer to these questions is provided by *distance measures* [3]. Distance measures are defined in a number of different ways, both classically and quantum mechanically. Two of those measures, the *trace distance* and the *fidelity*, have particularly wide currency today, and are the distance measures we adopted in our experiments. The properties of both are quite similar, however for certain applications it may be easier to deal with one over the other.

Since in the field of quantum information we deal with both quantum states and probability distributions, I will start by defining distance measures for quantum states and then I will generalize it to the case of probability distribution.

### 2.6.1 Quantum State Fidelity

How *close* are two quantum states? Let us consider two density matrices  $\rho_1$  and  $\rho_2$  associated to two quantum states to be compared. The quantum state fidelity, defined as

$$\mathcal{F}(\rho_1, \rho_2) = Tr \left[ \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}} \right]^2, \quad (2.21)$$

can be an estimator of how close those states are [25]. The fidelity is bounded by  $0 \leq \mathcal{F} \leq 1$  and  $\mathcal{F} = 1$  if  $\rho_1 = \rho_2$ , while  $\mathcal{F} = 0$  if they are orthogonal. These bounds can be easily obtained in the case of two pure states, indeed (2.21) reduces to

$$\mathcal{F}(|\psi_1\rangle, |\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|^2 \quad (2.22)$$

which is clearly vanishing if  $|\psi_1\rangle$  and  $|\psi_2\rangle$  are orthogonal, while  $\mathcal{F} = 1$  for  $|\psi_1\rangle = |\psi_2\rangle$ .

### 2.6.2 Trace-Distance

Let us now move to a second definition of a distance measure between quantum states. Let us consider again two quantum states  $\rho_1$  and  $\rho_2$ , the *trace distance* between them is defined as

$$D(\rho_1, \rho_2) = \frac{1}{2} \text{Tr}|\rho_1 - \rho_2|, \quad (2.23)$$

where for definition  $|\beta| \equiv \sqrt{\beta^\dagger \beta}$ .  $0 \leq D \leq 1$ : if  $\rho_1 = \rho_2$  the trace distance is vanishing, while  $D(\rho_1, \rho_2) = 1$  if  $\rho_1$  and  $\rho_2$  are orthogonal.

A property of the trace distance is its invariance under unitary transformations, i.e. for a generic unitary operator  $U$  acting on the states under consideration the equality

$$D(U\rho_1 U^\dagger, U\rho_2 U^\dagger) = D(\rho_1, \rho_2) \quad (2.24)$$

holds.

### 2.6.3 Comparison Between Processes

I now describe how to compare two quantum processes. It is well known that a quantum state can be completely determined by a tomographic reconstruction [24, 26, 27] and compared with the expected theoretical state by a variety of measures, such as quantum state fidelity [25]. Similarly, we know that a convenient way to describe a generic quantum operation  $\mathcal{E}$  is given by the process matrix  $\chi_{\mathcal{E}}$ , indeed its action on a generic state  $\rho$  can be written as  $\mathcal{E}(\rho) = \sum_{mn} \chi_{mn} A_m \rho A_n^\dagger$ , where  $\{A_j\}$  is a complete set of Kraus operators and the elements  $\chi_{mn}$  constitute the process matrix  $\chi_{\mathcal{E}}$  [28]. A closely related but more abstract representation is provided by the Jamiolkowski isomorphism [29], which relates a quantum operation  $\mathcal{E}$  to a quantum state,  $\rho_{\mathcal{E}}$ :

$$\rho_{\mathcal{E}} \equiv (\mathbb{I} \otimes \mathcal{E}) |\Phi\rangle\langle\Phi|, \quad (2.25)$$

where  $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_j |j\rangle|j\rangle$  is a maximally entangled state associated with the  $d$ -dimensional system with another copy of itself, and  $\{|j\rangle\}$  is an orthonormal basis set. If  $\mathcal{E}$  is a trace-preserving process, then the quantum state  $\rho_{\mathcal{E}}$  is normalized,  $\text{Tr}[\rho_{\mathcal{E}}] = 1$ . In this way, by associating a quantum process to a quantum state, for two trace-preserving processes  $\mathcal{E}$  and  $\mathcal{G}$ , a *Process Fidelity*  $\Delta$  has been defined as follows [30–33]

$$\Delta(\mathcal{E}, \mathcal{G}) = \mathcal{F}(\rho_{\mathcal{E}}, \rho_{\mathcal{G}}) \quad (2.26)$$

where  $\mathcal{F}$  is the quantum state fidelity (2.21). It is easy to demonstrate that, by choosing the set  $A_m = \{\sqrt{d}|i\rangle\langle j|\}$  as Kraus operators, we have  $\rho_{\mathcal{E}} \equiv \chi_{\mathcal{E}}$ , and, in general,  $\mathcal{F}(\rho_{\mathcal{E}}, \rho_{\mathcal{G}}) = \mathcal{F}(\chi_{\mathcal{E}}, \chi_{\mathcal{G}})$  if any complete set of operators  $A'_m$  satisfying  $\text{Tr}[A'_m A_n^{\dagger}] = d\delta_{mn}$  is used ( $\delta_{mn}$  is the Kronecker delta). Thus, if we want to compare an experimental map  $\chi$  with the expected one  $\chi_{id}$ , the process fidelity is

$$\Delta = \text{Tr} \left[ \sqrt{\sqrt{\chi} \chi_{id} \sqrt{\chi}} \right]^2. \quad (2.27)$$

The last expression gives the fidelity of density matrices with unit trace.

The same generalization can be adopted for the trace distance in the case of two quantum processes: given  $\chi_1$  and  $\chi_2$  two process matrices describing two quantum maps, the trace distance reads:

$$D(\chi_1, \chi_2) = \frac{1}{2} \text{Tr} |\chi_1 - \chi_2|. \quad (2.28)$$

### 2.6.4 Comparison Between Probability Distributions: Similarity

As a last step, it is useful to define a quantity able to give a measure of the *distance* between two probability distributions. It is provided by the Similarity

$$S = \frac{(\sum_{i,j} \sqrt{D_{ij} D'_{ij}})^2}{\sum_{i,j} D_{ij} \sum_{i,j} D'_{ij}}, \quad (2.29)$$

which is a generalization of the classical fidelity between two distributions  $D$  and  $D'$ .

## References

1. R. Feynman, Simulating physics with computers. *Int. J Theor. Phys.* **21**, 476 (1982)
2. V. Potocek, A. Gabris, T. Kiss, I. Jex, Optimized quantum random-walk search algorithms on the hypercube. *Phys. Rev. A* **79**, 012325 (2009)
3. I.L. Chuang, M.A. Nielsen, *Quantum Information and Quantum Computation* (Cambridge University Press, Cambridge, 2000)
4. A. Einstein, B. Podolski, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 77 (1935)
5. G. Benenti, G. Casati, G. Strini, *Principles of Quantum Computation and Information*, vol. I, Basic Concepts (World Scientific, Singapore, 2004)
6. G. Benenti, G. Casati, G. Strini, *Principles of Quantum Computation and Information*, vol. II, Basic Tools and Special Topics (World Scientific, Singapore, 2007)
7. R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120 (1978)
8. L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325 (1997)
9. K. Mattle, H. Weinfurter, P.G. Kwiat, A. Zeilinger, Dense coding in experimental quantum communication. *Phys. Rev. Lett.* **76**, 4656 (1996)
10. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Experimental quantum teleportation. *Nature* **390**, 575 (1997)
11. D. Boschi, S. Branca, F.D. Martini, L. Hardy, S. Popescu, Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **80**, 1121 (1998)
12. W.K. Wootters, W.H. Zurek, A single quantum cannot be cloned. *Nature* **299**, 802 (1982)
13. C.H. Bennet, G. Brassard, Public key distribution and coin tossing, in *Proceedings of IEEE International Conference Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, p. 175, Bangalore, India (1984)
14. L.M.V. Giovannetti, S. Lloyd, Quantum metrology. *Phys. Rev. Lett.* **96**, 010401 (2006)
15. P. Kok, S.L. Braunstein, J.P. Dowling, Quantum lithography, entanglement and Heisenberg-limited parameter estimation. *J. Opt. B: Quantum Semiclassical Opt.* **6**, S811 (2003)
16. R. Loudon, *Quantum Theory of Light* (Oxford University Press, Oxford, 2000)
17. J.J. Sakurai, *Meccanica Quantistica Moderna* (Zanichelli, 2003)
18. J. Bell, On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195 (1964)
19. A. Aspect, P. Grangier, G. Roger, Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: a new violation of Bell's inequalities. *Phys. Rev. Lett.* **49**, 91 (1982)
20. E. Knill, R. Laflamme, G.J. Milburn, A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46 (2001)
21. C.K. Hong, Z.Y. Ou, L. Mandel, Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987)
22. K. Kraus, *States, Effects and Operations Fundamental Notions of Quantum Theory* (Academic Press, 1983)
23. D.T. Smithey, M. Beck, M.G. Raymer, A. Faridani, Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: application to squeezed states and the vacuum. *Phys. Rev. Lett.* **70**, 1244 (1993)
24. D.F.V. James, P.G. Kwiat, W.J. Munro, A.G. White, Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001)
25. R. Jozsa, Fidelity for mixed quantum states. *J. Mod. Opt.* **41**, 2315 (1994)
26. G. Stokes, On the composition and resolution of polarized light from different sources. *Trans. Cambridge Philos. Soc.* **9**, 399–416 (1852)
27. U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997)
28. I.L. Chuang, M.A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455 (1997)

- 29. A. Jamiolkowski, Linear transformations which preserve trace and positive semidefiniteness of operators. Rep. Math. Phys. **3**, 275 (1972)
- 30. M. Raginsky, A fidelity measure for quantum channels. Phys. Lett. A **290**, 11 (2001)
- 31. M.A. Nielsen, A simple formula for the average gate fidelity of a quantum dynamical operation. Phys. Lett. A **303**, 249 (2002)
- 32. A. Gilchrist, N.K. Langford, M.A. Nielsen, Distance measures to compare real and ideal quantum processes. Phys. Rev. A **71**, 062310 (2005)
- 33. G. Wang, M. Ying, Unambiguous discrimination among quantum operations. Phys. Rev. A **73**, 042301 (2006)

Integrated Devices for Quantum Information with  
Polarization Encoded Qubits

Sansoni, L.

2014, XII, 140 p. 48 illus., 19 illus. in color., Hardcover

ISBN: 978-3-319-07102-2