Chapter 2
Fundamentals of Quantum Information Processing

Quantum mechanics is a part of quantum theory that aims at describing the nature when we consider the subatomic physics, or *quantum physics*. It can also be understood as the mathematical framework to describe isolated quantum systems, whose behavior cannot be captured by *classical physics* [10]. We have two ways to consider when we have the necessity to incorporate quantum mechanical effects into computing and communications: (1) use it to strive to suppress the quantum effects and still preserve a semblance of classicality even though the computational or communication elements are very small; or (2) use it to enhance quantum effects and try to find clever ways to enhance and sustain them to achieve old computational and communication goals in new ways. *Quantum computing* and *communications* use the latest strategy by harnessing quintessentially quantum effects [13].

Taking into account the approach required for quantum computation and communications, when we desire to build algorithms and hardware for quantum computing and communications we must consider the *postulates of quantum mechanics*. These postulates specify how we can represent, process, and measure information in this new domain.

In this chapter we are going to introduce some basic concepts of quantum information processing. Firstly, we make the reader familiar with the Dirac notation [1], a concise representation of the quantum mechanics concepts, which implies in a simplification of the calculi to be performed. After that, we are going to introduce the *density operators*, very useful in the domain of quantum communications.

This chapter provides a quick review of basic concepts for the understanding of subsequent chapters. However, it does not contain a complete explanation of the mathematics behind quantum mechanics. It is extensive and there are entire books dedicated to it. The chapter concludes with suggestions for further reading.

This chapter is organized as follows. Section 2.1 introduces the qubit, which is the fundamental unit of information in a quantum system. Section 2.2 describes how the evolution is carried out in a quantum system, whereas Sect. 2.3 shows how we can bring information from a quantum system to a classical level by means of

E.B. Guedes et al., *Quantum Zero-Error Information Theory*,
DOI 10.1007/978-3-319-42794-2_2

projective measurements and of positive operator-value measurements. The density operator formalism, very useful for quantum communications, is shown in Sect. 2.4. Entanglement, which does not have a classical counterpart, is discussed in Sect. 2.5. The postulates of quantum mechanics are presented in Sect. 2.6 using the density operator notation.

2.1 Representing Information

The basic unity of information in classical computing and communications is the *bit*, or *binary digit*, which can be 0 or 1 (false or true, respectively). The information is represented, or encoded, by a sequence of bits.

On the other hand, the basic unity of information in quantum computing and communications is a two-state quantum mechanical system: the *qubit*, or *quantum bit*. Consequently, the state of a qubit is represented by a unit vector in a 2-dimensional complex Hilbert space. We call such a vector a *ket* and we denote the state by $|\psi\rangle$, where $|\cdot\rangle$ is the vector and ψ is the label of the qubit. The following definition formalizes the state of a qubit.

Definition 2.1 (State of a Qubit). The state of a qubit ψ, denoted by $|\psi\rangle$, can be represented by a vector in a 2-dimensional Hilbert space $\mathcal{H}$, i.e.,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

where α and β are complex numbers ($\alpha, \beta \in \mathbb{C}$), which must satisfy the unitary restriction

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

The states $|0\rangle$ and $|1\rangle$ form a basis for the 2-dimensional Hilbert space.

The use of $|\psi\rangle$ to represent the state of a qubit does not depend on the manner that it is physically encoded. A certain state $|\phi\rangle$, for example, could refer to the state of a polarized photon, or an excited state of an atom, or the direction of circulation of a superconducting current, etc. [13]. Such representation enables us to treat qubits as abstract mathematical objects [10, Chap. 1].

In (2.1), the states $|0\rangle$ and $|1\rangle$ are known as *computational basis states*, and form an orthonormal basis for the 2-dimensional Hilbert space. The notation of $|0\rangle$ and $|1\rangle$ in terms of vectors is

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.3}$$

Using the computational basis, the general state of a qubit $|\psi\rangle$ is denoted by

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ &= \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. \end{aligned} \tag{2.4}$$

We say that α and β are the *amplitudes* associated with the states $|0\rangle$ and $|1\rangle$, respectively.

When α and β in (2.1) are non-zero, we say that the qubit is in a *superposition* state. Differently from bits, qubits are not constrained to be wholly 0 or wholly 1 at a given moment [13]. According to quantum mechanics, the modulus squared of α, β in the former equation gives the probability of measuring the qubit in state $|0\rangle$ or in state $|1\rangle$, respectively [7]. It means that

- $|\alpha|^2$ gives the probability of finding $|\psi\rangle$ in state $|0\rangle$;
- $|\beta|^2$ gives the probability of finding $|\psi\rangle$ in state $|1\rangle$.

The unitary restriction of Definition 2.1 is related to the probability of obtaining a given measurement result. In particular, if $|\alpha| = |\beta|$, we say that the qubit is in an equally distributed superposition.

Example 2.1 (Qubits in Superposition). Let $|\varphi\rangle$ and $|\phi\rangle$ denote the states of two qubits in superposition:

$$|\varphi\rangle = \frac{1}{\sqrt{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle\,, \tag{2.5}$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\,. \tag{2.6}$$

Although both qubits are in superposition, only the state $|\phi\rangle$ is in an equally distributed superposition.

The Hermitian conjugate of a ket $|\psi\rangle$ is called a *bra* or *dual vector*. A bra is denoted by $\langle\psi| = |\psi\rangle^\dagger$, where $\dagger$ indicates complex conjugation and matrix transposition.

$$\begin{aligned} \langle\psi| &= |\psi\rangle^\dagger \\ &= \left(|\psi\rangle^*\right)^T \\ &= \begin{bmatrix} \alpha^* \\ \beta^* \end{bmatrix}^T \\ &= \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix}. \end{aligned} \tag{2.7}$$

Example 2.2 (Bra). The Hermitian conjugate of (2.5) is given by

$$\begin{aligned}\langle\varphi| &= |\varphi\rangle^\dagger \\ &= \begin{bmatrix} \frac{1}{\sqrt{3}} \\ \sqrt{\frac{2}{3}} \end{bmatrix}^\dagger \\ &= \begin{bmatrix} \frac{1}{\sqrt{3}}^* & \sqrt{\frac{2}{3}}^* \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \end{bmatrix}.\end{aligned}$$

A remarkable difference from quantum to classical computing and communication is that while a bit can represent only two distinct values, a qubit can assume infinitely many different states. The only constraint is the unitary restriction (2.1). Therefore, while the basic unity of quantum information is unlimited, the classical unity of information is restricted to the values "true" and "false."

We can also introduce a geometrical representation for a single qubit. To do so, we rewrite (2.1) as

$$|\psi\rangle = e^{\iota\gamma}\left[\cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{\iota\beta}\sin\left(\frac{\alpha}{2}\right)|1\rangle\right], \tag{2.8}$$

where $\alpha, \beta, \gamma \in \mathbb{R}$. Factor $e^{\iota\gamma}$ is called the global phase. The factor does not influence measurement statistics, since its absolute value is equal to one. Consequently, global phase is often omitted [5]. While (2.1) is related to a vector in a two-dimensional Hilbert space, the qubit (2.8) without $e^{\iota\gamma}$ has a nice geometrical interpretation on a three-dimensional polar coordinate system. Figure 2.1 illustrates the representation of (2.8) in a *Bloch sphere*.

Example 2.3 (Geometrical Representation). The qubit (2.6) can be denoted according to the geometrical representation as

$$|\phi\rangle = \cos\left(\frac{\pi}{4}\right)|0\rangle - \sin\left(\frac{\pi}{4}\right)|1\rangle.$$

2.1.1 Composite Quantum Systems

In classical computing and communications, a bit can represent two values, 0 or 1. Therefore, a register of n bits can store 2^n different values, one each time. Thanks to the superposition of quantum states, a quantum register of n qubits can store 2^n different values at the same time. The concept of composite quantum systems is shown in Definition 2.2.

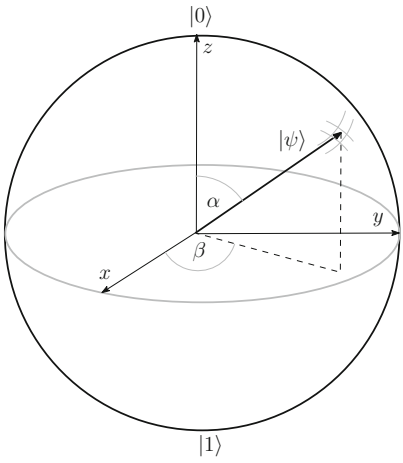

Fig. 2.1 Geometrical visualization of a qubit in Bloch sphere

Definition 2.2 (Composite Quantum Systems). A *composite quantum system*, also called quantum register or multi-qubit quantum systems, is made up of two or more distinct physical systems. The state space of a composite quantum system is the tensor product of the state space of its components. If $|\psi_1\rangle, \ldots, |\psi_n\rangle$ describe the states of n isolated quantum systems, the state of the composite system is $|\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$.

The tensor product of the states $|a\rangle$ and $|b\rangle$, also known as direct or Kronecker product, is denoted by $|a\rangle \otimes |b\rangle = |ab\rangle$, and calculated as follows:

$$\begin{aligned} |a\rangle \otimes |b\rangle &= \begin{bmatrix} a_1 \\ a_2 \\ \cdots \\ a_n \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix} \\ &= \begin{bmatrix} a_1 \cdot |b\rangle \\ a_2 \cdot |b\rangle \\ \cdots \\ a_n \cdot |b\rangle \end{bmatrix}. \end{aligned} \tag{2.9}$$

Let $|\psi\rangle$ be the state of a certain 2-qubit system. The representation of $|\psi\rangle$ is given by

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\ &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \\ &= \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_2\beta_2 |11\rangle \\ &= \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \end{aligned} \tag{2.10}$$

$$= \alpha'_0 |0\rangle + \alpha'_1 |1\rangle + \alpha'_2 |2\rangle + \alpha'_3 |3\rangle$$
$$= \sum_{i=0}^{2^2-1} \alpha'_i |i\rangle . \tag{2.11}$$

It is interesting to notice that (2.11) uses decimal notation for indexes and labels instead of binary notation employed in (2.10)—this is a simplification commonly adopted in quantum computation and communication. The state $|\psi\rangle$ of two qubits contains all the states 0, 1, 2, and 3 at the same time, each of them with its own amplitude α'_i. In this case, if at least two distinct $\alpha'_i \neq 0$, we say that $|\psi\rangle$ is in a superposition. Storing these amplitudes on a classical computer simultaneously requires up to four registers. Instead, quantum computers perform the same task just using a composite quantum system of two qubits in superposition.

In a general way, the state of an n-qubit system can be written as

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle , \tag{2.12}$$

with $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. The states $|0\rangle , |1\rangle , \ldots , |2^n - 1\rangle$ form the computational basis of the 2^n-dimensional Hilbert space.

Another way to represent a composite quantum state is to consider it as belonging to a larger Hilbert space $\mathcal{H}$ composed by tensor product of state vectors belonging to Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. We can construct a certain vector $|\psi\rangle \in \mathcal{H}$ as the tensor product of two vectors $|\phi\rangle \in \mathcal{H}_1$ and $|\varphi\rangle \in \mathcal{H}_2$:

$$|\psi\rangle = |\phi\rangle \otimes |\varphi\rangle . \tag{2.13}$$

The tensor product has the following properties:

1. For $\alpha \in \mathbb{C}$, $|\phi\rangle \in \mathcal{H}_1$ and $|\psi\rangle \in \mathcal{H}_2$,

$$\alpha (|\phi\rangle \otimes |\psi\rangle) = (\alpha |\phi\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes (\alpha |\varphi\rangle) . \tag{2.14}$$

2. For $|\phi_1\rangle , |\phi_2\rangle \in \mathcal{H}_1$ and $|\psi\rangle \in \mathcal{H}_2$,

$$(|\phi_1\rangle + |\phi_2\rangle) \otimes |\psi\rangle = |\phi_1\rangle \otimes |\psi\rangle + |\phi_2\rangle \otimes |\psi\rangle . \tag{2.15}$$

3. For $|\phi\rangle \in \mathcal{H}_1$ and $|\psi_1\rangle , |\psi_2\rangle \in \mathcal{H}_2$,

$$|\phi\rangle \otimes (|\psi_1\rangle + |\psi_2\rangle) = |\phi\rangle \otimes |\psi_1\rangle + |\phi\rangle \otimes |\psi_2\rangle . \tag{2.16}$$

2.2 Processing Information

Classical information processing is performed by applying operations on bits that represent information. In the quantum scenario, the information processing is also performed by *operators*, which are applied on the state of qubits. Typically, these operators are denoted by capital letters of the alphabet and have special properties stated in the following definition:

Definition 2.3 (Quantum Operator). An isolated quantum system originally in the state $|\psi_1\rangle$ *evolves* to state $|\psi_2\rangle$ by means of the application of a *quantum operator* U:

$$|\psi_2\rangle = U\,|\psi_1\rangle\,. \tag{2.17}$$

Quantum operators are required to be *unitary* because they should preserve vector norms. A unitary operator U has the following property: $U^\dagger = U^{-1}$, where $U^\dagger$ denotes the Hermitian conjugate (conjugate transpose) of U and U^{-1} is the inverse of U. Therefore, any unitary operator satisfies

$$U^\dagger \cdot U = U \cdot U^\dagger = \mathbb{1}, \tag{2.18}$$

where $\mathbb{1}$ is the identity matrix [6].

Because quantum operators are unitary, the evolution of an isolated quantum system is *reversible*. For example, we can easily return to the state $|\psi_1\rangle$ from $|\psi_2\rangle$ just applying the unitary operator $U^\dagger$:

$$U^\dagger\,|\psi_2\rangle = U^\dagger(U\,|\psi_1\rangle) = (U^\dagger U)\,|\psi_1\rangle = |\psi_1\rangle\,. \tag{2.19}$$

Some operators play an important role in quantum information processing and quantum computing. Particularly, the set known as *Pauli matrices* is specially interesting:

$$\sigma_0 = \mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The Pauli matrices are Hermitian, i.e., $\sigma_k = \sigma_k^\dagger$, $k = 0, \ldots, 3$. The operator X, in particular, is the quantum analog of the classical *NOT* gate. For instance, when this operator is applied to $|0\rangle$ we get $X\,|0\rangle = |1\rangle$. Pauli matrices are widely used in several quantum computation and communication algorithms.

The *Hadamard matrix*, denoted by H, is another very important operator because it can build equally distributed superpositions. Moreover, when applied to any state

of a 2-dimensional Hilbert space, it performs a 45° rotation on such state. The matricial representation of this operator is

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.20}$$

If we apply Hadamard to the state $|1\rangle$, this operator will create the superposition $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$. The states $|-\rangle$ and $|+\rangle = H|0\rangle$ are known as the *Hadamard basis*.

2.2.1 Tensor Product of Operators

Suppose we have a composite quantum system and we wish to apply a quantum operator to each of the respective states. To enable quantum operators to be applied in multi-qubit systems, we must define tensor products of quantum operators.

Definition 2.4 (Tensor Product of Operators). Let A and B be the matricial representation of two quantum operators with dimensions $m \times n$ and $p \times q$, respectively. The tensor product $A \otimes B$ is defined by

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}. \tag{2.21}$$

The resulting matrix $A \otimes B$ has dimension $(nq) \times (mp)$ and can be applied to a composite quantum system as previously explained. We denote the n-tensor product of the operator U with itself by $U^{\otimes n}$. For example, $U^{\otimes 3} = U \otimes U \otimes U$.

The Hadamard operator, in particular, is very useful in many quantum computing and communication algorithms. For example, n-tensor product of Hadamard operators can be used to create n equally distributed superposition of qubits. Then, an arbitrary quantum operator acting on the state space of the n-qubits can be applied to the composite system in a simultaneous way. This feature, called *quantum parallelism*, is restricted to quantum computation. Parallelism is not performed efficiently by classical computers because, for instance, simulating a superposition of n qubits requires 2^n classical registers and individual application of the operation in each of them.

Example 2.4 (Tensor Product of Operators). Let $|\psi\rangle = |00\rangle = |0\rangle^{\otimes 2}$ be a 2-qubit quantum system. The application of the Hadamard operator to both qubits is performed by the operator $H^{\otimes 2} = H \otimes H$ in the following way:

$$
\begin{aligned}
H^{\otimes 2}\left|0\right\rangle^{\otimes 2} &= H\left|0\right\rangle \otimes H\left|0\right\rangle \\
&= \left[\frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)\right] \otimes \left[\frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)\right] \\
&= \left|+\right\rangle\left|+\right\rangle \\
&= \left|+\right\rangle^{\otimes 2}.
\end{aligned}
$$

2.2.2 Projection Operators

The result of the outer product operation on a vector $\left|\psi\right\rangle$ with itself, denoted by $\left|\psi\right\rangle\left\langle\psi\right|$, is a linear projection operator. Such operator $\left|\psi\right\rangle\left\langle\psi\right|$, performs the following mapping:

$$
\left|\psi\right\rangle\left\langle\psi\right|\left|\varphi\right\rangle \mapsto \left|\psi\right\rangle\left\langle\psi\right|\varphi\rangle = \left\langle\psi\right|\varphi\rangle\left|\psi\right\rangle, \tag{2.22}
$$

where $\left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}$. That is, the operator $\left|\psi\right\rangle\left\langle\psi\right|$ projects a vector $\left|\varphi\right\rangle$ onto the 1-dimensional subspace of $\mathcal{H}$ spanned by $\left|\psi\right\rangle$. Such an operator is called an *orthogonal projector* [6].

More generally, suppose $\mathcal{H}$ is an n-dimensional Hilbert space. Let $\{\left|1\right\rangle, \ldots, \left|k\right\rangle\}$ be any orthonormal basis of a subspace $\mathcal{H}'$ of $\mathcal{H}$, $k \leq n$. Then,

$$
P = \sum_{i=1}^{k} \left|i\right\rangle\left\langle i\right| \tag{2.23}
$$

is an orthogonal projector onto the subspace $\mathcal{H}'$. It is easy to see that projectors are Hermitian operators. Moreover, for any orthogonal projector P, $P^2 = P$ [7].

Projection operators also satisfy the *completeness relation*, i.e., if $\{\left|1\right\rangle, \ldots, \left|n\right\rangle\}$ is an orthonormal basis of an n-dimensional Hilbert space $\mathcal{H}$, then

$$
P = \sum_{i=1}^{n} \left|i\right\rangle\left\langle i\right| = \mathbb{1}. \tag{2.24}
$$

Example 2.5 (Completeness Relation). Let $B_H = \{\left|+\right\rangle, \left|-\right\rangle\}$ be the Hadamard basis of the 2-dimensional Hilbert space. The corresponding projection operators are

$$
P_+ = \left|+\right\rangle\left\langle+\right| = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix},
$$

$$
P_- = \left|-\right\rangle\left\langle-\right| = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}.
$$

It is straightforward to see that $P_+ + P_- = \mathbb{1}$.

2.3 Measuring Information

An isolated quantum system evolves by means of unitary transformations. While it remains closed, no information can be inferred from the system. In order to access the state of a quantum system, we need to perform a task called *measurement*. Measurements can be viewed as an "interface" from the quantum world to the classical level; it is the unique way to extract useful information from qubits after some processing.

In the classical scenario, measurement is a trivial task and the results depend only on the apparatus accuracy. Moreover, measurements do not disturb the state of the classical system, no matter how many times we measure the corresponding quantity. However, in quantum scenario, measurement is not a trivial task because it affects the isolated quantum system causing a collapse in the state space of corresponding quantum system being measured. As a consequence, measurements are irreversible operations in quantum systems—once a qubit is measured, it is not possible to return to the state it had right before the measurement [8].

A classical computer follows essentially a load-run-read cycle wherein one loads data into the machine, runs a program using this data as input, and then reads out the result. This becomes an analogous prepare-evolve-measure cycle on a quantum computer. That is, one prepares a quantum state, evolves it on the quantum computer by means of unitary transformations and, finally, measures the result [13].

There are two special cases of general measurements that play an important role in quantum information and computation: projective measurements and positive operator-valued measurements.

Definition 2.5 (Projective Measurement). A projective measurement is described by an observable M, which is a Hermitian operator on the state space of the system being measured. The observable M has a spectral decomposition

$$M = \sum_m \lambda_m P_m, \tag{2.25}$$

where P_m is a projector onto the eigenspace of M with eigenvalue λ_m. Measurement outcomes correspond to the eigenvalue indexes m. When a system in a state $|\psi\rangle$ is observed, the probability of getting output m is

$$p(m) = \langle\psi| P_m |\psi\rangle . \tag{2.26}$$

Given that the outcome m occurred, the state of the system immediately after the measurement will be

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{2.27}$$

Instead of giving an observable to describe a projective measurement, we can simply construct a list of projectors P_m satisfying $\sum_m P_m = \mathbb{1}$ and $P_i P_j = \delta_{ij} P_i$, i.e., projectors must be pairwise orthogonal. The corresponding observable is then $M = \sum_m m P_m$. We say that a quantum system is measured in a basis $|m\rangle$ when a projective measurement with projectors $P = |m\rangle \langle m|$ is performed, where $|m\rangle$ is an orthonormal basis.

Example 2.6 (Projective Measurements). Suppose a quantum system in the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Performing a projective measurement in the computational basis with projectors $\{P_0 = |0\rangle \langle 0|, P_1 = |1\rangle \langle 1|\}$ gives the output "0" with probability

$$\begin{aligned} p(0) &= \langle \psi | P_0 | \psi \rangle \\ &= \left(\frac{\langle 0| - \langle 1|}{\sqrt{2}} \right) |0\rangle \langle 0| \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{2}. \end{aligned}$$

Similarly, we found that $p(1) = \frac{1}{2}$. In this case, getting the two possible outputs is an equally likely event. Given that outcome "0" occurs, the post measurement state will be

$$\begin{aligned} |\psi'\rangle &= \frac{P_0 |\psi\rangle}{\sqrt{p(0)}} \\ &= \frac{|0\rangle \langle 0| \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)}{\sqrt{\frac{1}{2}}} \\ &= |0\rangle . \end{aligned}$$

As we can expect, the post-measurement state given that output "1" occurred is $|\psi'\rangle = |1\rangle$.

In some applications, however, the system state after the measurement is not important. For example, in quantum error-correction codes, the measurement output on the received quantum codeword gives the error syndrome, which is used to choose a unitary operator in order to (possibly) correct the error introduced by the noisy quantum channel. In such situations, we are only interested in the outcomes and their associated probabilities. The *Positive Operator-Value Measurement formalism* (POVM formalism) is the most appropriate theoretical tool to deal with this scenario.

Definition 2.6 (POVM Measurements). A Positive Operator-Value Measurement (POVM) is defined by a set of Hermitian, positive operators $\{E_m\}$ acting on the state space of the quantum system being measured [10, Sect. 2.2.6]. The probability of

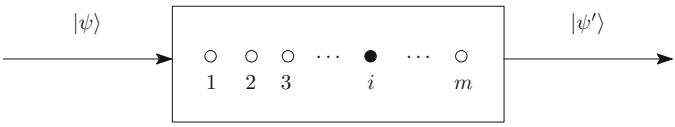

Fig. 2.2 A POVM measurement apparatus. When a quantum state is measured using a set of POVM elements $\{E_1, \ldots, E_m\}$, an led is turned on indicating the outcome

getting outcome m given that the state $|\psi\rangle$ is measured is

$$p(m) = \langle\psi| E_m |\psi\rangle . \tag{2.28}$$

POVM operators must satisfy the completeness relation, i.e.,

$$\sum_m E_m = \mathbb{1}. \tag{2.29}$$

Differently from general and projective measurements, we are not able to predict the post-measurement state of quantum system after a POVM measurement. Fortunately, most of the applications in quantum computation and information do not care about post-measurement states. Instead, we are often interested in measurement outcomes and the corresponding associated probabilities. Figure 2.2 illustrates a POVM measurement apparatus. When an unknown quantum state $|\psi\rangle$ is measured, a led turns on to indicate the outcome.

2.4 Density Operator

Pure quantum states are represented by unitary vectors belonging to an appropriate Hilbert space. This kind of system suggests a lowest degree of ignorance, since we have nothing further to discover than the quantum state itself.

However, a qubit can be in an *ensemble* of pure states, i.e., the system can be in a certain state $|\psi_i\rangle$ with probability p_i, $i > 1$. We describe the state of such qubit as an ensemble of possible pure states and their associated probabilities $\{|\psi_i\rangle, p_i\}$, where $\sum_i p_i = 1$. The whole system is said to be in a *mixed quantum state*. In summary, the formalism we have used so far is not adequate to represent quantum systems in two situations:

1. When the quantum system state is one of $|\psi_1\rangle, |\psi_2\rangle, \ldots$ with probabilities $p_1, p_2, \ldots$.
2. When a certain system (called A) is part of a larger quantum system AB.

In these situations, the mathematical formalism of *density operators* is more suitable to describe the state of the whole quantum system.

Definition 2.7 (Density Operator). Suppose that a quantum system is in one of the states $|\psi_i\rangle$ with probability p_i, $\sum_i p_i = 1$. We say that the quantum system is an ensemble $\{|\psi_i\rangle, p_i\}$. The density operator that describes the whole system is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| . \tag{2.30}$$

Example 2.7 (Density Operator—Pure State). Suppose that we apply the Hadamard operator to a quantum state $|\psi_0\rangle$ initially on the state $|0\rangle$. Then, the state of the quantum system will be

$$\begin{aligned} |\psi_1\rangle &= H |\psi_0\rangle \\ &= H |0\rangle \\ &= \frac{1}{\sqrt{2}} (|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| - |1\rangle \langle 1|) |0\rangle \\ &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) . \end{aligned}$$

Using the density operator formalism, the system state after the Hadamard operation can be denoted as

$$\begin{aligned} \rho &= |\psi_1\rangle \langle\psi_1| \\ &= \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)\right] \left[\frac{1}{\sqrt{2}} (\langle 0| + \langle 1|)\right] \\ &= \frac{1}{2} (|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) \\ &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} . \end{aligned}$$

Although we had used the density operator formalism to represent the state of the system, the system itself remains in a quantum pure state.

Example 2.8 (Density Operator—Mixed State). Consider that a quantum system can be in one of the states $|+\rangle$ and $|-\rangle$ with probability 1/3 and 2/3, respectively. The density operator of the system is given by

$$\begin{aligned} \rho &= \left[\frac{1}{3} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right)\right] + \left[\frac{2}{3} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right)\right] \\ &= \frac{1}{6} (|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) + \end{aligned}$$

$$
\begin{aligned}
&+\frac{2}{6}\left(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|\right) \\
&= \frac{|0\rangle\langle 0|}{2} - \frac{|0\rangle\langle 1|}{3} - \frac{|1\rangle\langle 0|}{3} + \frac{|1\rangle\langle 1|}{2} \\
&= \begin{bmatrix} 1/2 & -1/3 \\ -1/3 & 1/2 \end{bmatrix}.
\end{aligned}
$$

Density operators have a well-defined characterization. The reader can easily prove the following theorem:

Theorem 2.1 (Density Operator). *An operator ρ is a density operator associated with an ensemble $\{|\psi_i\rangle, p_i\}$ if and only if it satisfies two conditions:*

1. ***Trace Condition**. ρ has trace equal to 1;*
2. ***Positivity Condition**. ρ is a positive operator.*

Example 2.9 (Trace and Positivity). From the density operator ρ of the previous example, we can see that its trace is equal to 1, as stated by the trace condition.

$$
\begin{aligned}
\mathrm{Tr}(\rho) &= \mathrm{Tr}\left(\begin{bmatrix} 1/2 & -1/3 \\ -1/3 & 1/2 \end{bmatrix}\right) \\
&= \frac{1}{2} + \frac{1}{2} \\
&= 1.
\end{aligned}
$$

Positivity condition can be checked by calculating the eigenvalues of ρ, which are $\lambda_1 = \frac{5}{6}$ and $\lambda_2 = \frac{1}{6}$. Since both eigenvalues are positive, ρ is a positive operator as well.

Given a density matrix ρ, how can we infer that the corresponding quantum system is in a pure or mixed state? It turns out that all we need to do is calculate the trace of ρ^2, as shown in the following theorem.

Theorem 2.2 (Condition to ρ Describe a Pure or Mixed State). *Let ρ be a density operator representing a quantum system. Then, $\mathrm{Tr}\left(\rho^2\right) \leq 1$, with equality if and only if the system is in a pure state.*

The two previous examples are useful to illustrate the theorem. Density operator of Example 2.7 represents a quantum system in a pure state. Since

$$
\rho = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},
$$

then

$$\begin{aligned}\mathrm{Tr}\left(\rho^2\right) &= \mathrm{Tr}\left(\frac{1}{4}\begin{bmatrix}2 & 2\\ 2 & 2\end{bmatrix}\right)\\ &= 1.\end{aligned}$$

Similarly, for the density operator of Example 2.8,

$$\begin{aligned}\mathrm{Tr}\left(\rho^2\right) &= \mathrm{Tr}\left(\begin{bmatrix}13/36 & -1/3\\ -1/3 & 13/36\end{bmatrix}\right)\\ &= 13/18\\ &< 1,\end{aligned}$$

which means that the quantum system is in a mixed state.

2.5 Entanglement

Quantum systems display properties that are unknown for classical ones, such as the superposition of quantum states, interference, or tunneling. These are all one-particle effects that can be observed in quantum systems, which are composed of a single particle. But these are not the only distinctions between classical and quantum objects—there are further differences that manifest themselves in composite quantum systems, that is, systems that are comprised of at least two subsystems [9].

Entanglement is a property of two or more quantum systems which exhibit correlations that cannot be explained by classical physics [12], being a key resource in quantum computation and quantum information theory. Entanglement occurs on composite quantum systems and involves unusually strong correlation between parts of them [13]. We begin by defining an entangled pure state.

Definition 2.8 (Entangled Pure State). A multi-qubit pure state is entangled if and only if it cannot be factored into the direct product of a definite state for each qubit individually. Thus, a pair of qubits, A and B, are entangled if and only if their joint state $|\psi_{AB}\rangle$ cannot be written as the product of a pure state for qubit A and a pure state for qubit B, i.e., $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$ for any choice of states $|\psi_A\rangle$ and $|\psi_B\rangle$ [13].

If the systems A and B are entangled, this means that the values of certain properties of system A are correlated with the values that those properties will assume for system B. The properties can become correlated even when the two systems are spatially separated [7].

Example 2.10 (Entangled Pure State [12]). States of two quantum systems can be considered together by taking their tensor product. For example, the two Hadamard states $|+\rangle$ and $|-\rangle$ can be considered together in the form

$$\begin{aligned} |+\rangle \otimes |-\rangle &= \left[\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right] \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right] \\ &= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right). \end{aligned}$$

The state $|+\rangle \otimes |-\rangle$ represents a 2-qubit system which is not entangled. On the other hand, consider the following quantum state:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.31}$$

If we try to write $|\beta_{00}\rangle$ as a tensor product of two pure qubits $|\psi_A\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\psi_B\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$, we get

$$\begin{aligned} |\beta_{00}\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\ &= \alpha\gamma\,|00\rangle + \beta\gamma\,|01\rangle + \alpha\delta\,|01\rangle + \beta\delta\,|11\rangle. \end{aligned}$$

It is easy to see that we cannot find α, β, γ, and δ that simultaneously satisfy $\alpha\gamma = \beta\delta = 1$ and $\beta\gamma = \alpha\delta = 0$. Therefore, the state $|\beta_{00}\rangle$ is entangled, since it cannot be broken down into two separate qubit pure states.

The state $|\beta_{00}\rangle$ belongs to a very important set of entangled states known as *Bell states* or *EPR pairs*. The Bell states form a basis for the 4-dimensional Hilbert space and play an important role in many quantum communication protocols. The Bell states are defined as

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{2.32}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \tag{2.33}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \tag{2.34}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.35}$$

If a state $|\psi_{AB}\rangle$ is entangled, then tracing out one of the two systems leads to a mixed state. If $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ is not entangled, then tracing out part A or part B of the space leads to $|\psi_B\rangle$ or $|\psi_A\rangle$, respectively. Recalling that $\mathrm{Tr}(\rho^2) = 1$ if and only if ρ is a pure state, we have a simple formula for testing whether a state is

entangled or not [12]. Therefore, the state $|\psi_{AB}\rangle$ is entangled if and only if

$$\mathrm{Tr}(\mathrm{Tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)^2) < 1. \tag{2.36}$$

This procedure works well once the composite system $|\psi_{AB}\rangle$ is a quantum pure state.

Example 2.11. We want to use (2.36) to check the entangled state $|\beta_{00}\rangle$. First, we trace out the system B from the state $|\beta_{00}\rangle$:

$$\begin{aligned}\rho_A &= \mathrm{Tr}_B(|\beta_{00}\rangle\langle\beta_{00}|)\\ &= \left[\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right].\end{aligned}$$

Finally,

$$\begin{aligned}\mathrm{Tr}(\rho_A^2) &= \mathrm{Tr}\left(\left[\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right]^2\right)\\ &= \frac{1}{4} + \frac{1}{4}\\ &< 1.\end{aligned}$$

We investigate now the entanglement in the framework of quantum mixed states. Tensor products of mixed states, $\rho = \rho_1 \otimes \rho_2$, do not exhibit correlations, as do not the tensor products of pure states. A convex sum of different product states,

$$\rho = \sum_i p_i \rho_{1,i} \otimes \rho_{2,i}, \tag{2.37}$$

with $p_i > 0$ and $\sum_i p_i = 1$, will in general yield correlated measurement results, i.e., there are local observables a and b such that $\mathrm{Tr}(\rho(a \otimes b)) \neq \mathrm{Tr}(\rho(a \otimes \mathbb{1}))\,\mathrm{Tr}(\rho(\mathbb{1} \otimes b)) = \mathrm{Tr}_1\,\rho_1 a\,\mathrm{Tr}_2\,\rho_2 b$. These correlations can be described in terms of the classical probabilities p_i and, therefore, they are considered classical. States like (2.37) are called *separable mixed states* [9].

In contrast, *mixed entangled states* are characterized by the non-existence of a decomposition into product states, as stated in the next definition.

Definition 2.9 (Mixed Entangled State [9]). A mixed state ρ is entangled if there are no local states $\rho_{1,i}$ and $\rho_{2,i}$, and non-negative weights p_i, such that ρ can be expressed as a convex mixture, i.e.,

$$\nexists \rho_{1,i}, \rho_{2,i}, p_i \geq 0 \text{ such that } \rho = \sum_i p_i \rho_{1,i} \otimes \rho_{2,i}. \tag{2.38}$$

Entanglement plays an important role in quantum information, communication, and computing. Perhaps, the most impressive application of entanglement is *teleportation*. Suppose that two physically separated parties, Alice and Bob, each takes one qubit of an EPR pair. Then, Alice can perform a teleportation of an arbitrary and unknown quantum state toward Bob by sending to him two classical bits of information. The quantum key distribution protocol proposed by Ekert [2], for instance, is based on this idea. A very didactic presentation of this protocol can be found in Fayngold and Fayngold [3].

2.6 Postulates of Quantum Mechanics

The concepts presented previously are organized in a framework of a workable physical theory, the so-called *postulates of quantum mechanics*. These postulates are a set of axioms that define how the theory operates [7]. According to the state-of-the-art knowledge, most of the rules in the universe can be traced back to these postulates and only a few effects seem to be an exception [5].

Frequently, the postulates of quantum mechanics are enunciated using the Dirac notation. Considering our purposes, we are going to enunciate these postulates using the density operators formalism, which is more convenient in quantum information and communication applications [10].

The first postulate tells us how physical states are represented in quantum mechanics. A quantum mechanical two-level system might be a single photon that can be found in one of the two distinct paths or a presence or absence of a photon in a particular location or path [6].

Postulate 2.1 (State Space of an Isolated Quantum System). *We associate with an isolated quantum system a complex vector space with inner product (i.e., a Hilbert space) known as* space state of the system. *This system is completely described by a density operator ρ, which is positive and has trace equal to* 1, *acting on the space state of the system. If the quantum system is in the state ρ_i with probability p_i, then the density operator of this system is $\sum_i p_i \rho_i$.*

The evolution of a closed quantum system is described by a unitary operator U. If the system is initially in the state $|\psi_i\rangle$ with probability p_i, after applying the operator U the state will be $U|\psi_i\rangle$ with probability p_i. Thus, the evolution of a quantum system according to the density operator framework is described by

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \xrightarrow{U} \sum_i p_i U |\psi_i\rangle \langle\psi_i| U^\dagger = U\rho U^\dagger. \tag{2.39}$$

Postulate 2.2 (Evolution of Closed Quantum Systems). *The evolution of a closed quantum system is described by a unitary transformation. Therefore, the state of a quantum system ρ at time t_1 is associated with the state ρ' at time t_2 by means of a unitary operator U that depends only on t_1 and t_2:*

$$\rho' = U\rho U^\dagger. \tag{2.40}$$

Measuring a quantum system that is in the state $|\psi\rangle$ seeks to obtain classical information about this state [11]. We can say that measurements connect the quantum and classical worlds; they are the only tools which allow taking a look at what happens in the quantum world [6]. Measuring the state of an unknown quantum system, in general, disturbs the state irreversibly. In those cases, there is no way to know or recover the state before the measurement. If the state was not disturbed, no new information about it is obtained [11]. Thus, measurements are obviously not reversible and therefore they represent the only exception under the unitary constraint.

The third postulate of quantum mechanics is synthesized as follows.

Postulate 2.3 (Quantum System Measurement). *Quantum measurements are described by a set of measurement operators* $\{M_m\}$*. These operators act on the space state of the quantum system being measured. The index m refers to the output that can occur at the measurement. If the state of the system prior to the measurement is* ρ*, then the probability of getting m at the measurement is*

$$p(m) = \text{Tr}(M_m^\dagger M_m \rho). \tag{2.41}$$

Given that the output m occurred, the post-measurement state of the system will be

$$\rho' = \frac{M_m \rho M_m^\dagger}{\text{Tr}(M_m^\dagger M_m \rho)}. \tag{2.42}$$

The set of measurement operators satisfies the completeness relation $\sum_m M_m^\dagger M_m = \mathbb{1}$.

The most common type of measurement in quantum mechanics is the projective measurement. This kind of measurement projects the system onto one of the eigen-subspaces of an observable and returns the corresponding eigenvalue. However, there exists a whole range of problems, such as pure state discrimination or joint measurement on several qubits, where it is more advantageous to use a general measurement procedure that tries to detect outcomes using a set of non-orthogonal operators. For such situations, a POVM measurement is adequate [3].

So far we have discussed the postulates for the case of a single system. If we want to study potentially useful quantum computing and communication applications, we need to understand how quantum mechanics works for systems composed of several qubits interacting with each other [6]. Entanglement, for instance, arises from composite quantum systems defined in the fourth postulate.

Postulate 2.4 (Composite Quantum Systems). *The state space of a composite quantum system is the tensor product of the space of states that compose it. If these systems are numbered from* 1 *to n, and the system i is in the state* ρ_i*, then the state of the composite system will be* $\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$.

In a very ingenious way, Portugal says that the postulates of quantum mechanics presented previously can be understood as "game rules." If you break then, you

are out of the game, i.e., you must respect them to create and understand quantum algorithms, protocols, etc. Considering the idea of game rules, the first postulate can be described as the arena where the game goes on. The second describes the dynamics of the game. The third describes the process of physical measurement. The fourth postulate describes how we adjoin various systems [11].

2.7 Further Reading

In this chapter we introduced an overview of some important quantum mechanics concepts. We presented the notion of qubits, evolution of quantum systems and projective and POVM measurements using the Dirac notation [1], widely known for simplifying the operations to be performed. We showed how entanglement represents non-trivial correlations between two or more quantum systems. Lastly, we introduced the density operators and enunciated the quantum mechanics postulates according to this framework.

Concepts presented in this chapter are an overview organized from many works in the literature: Williams [13], Nielsen and Chuang [10], Kaye et al. [6], Imre and Balazs [5], Hirvensalo [4], McMahon [7], Fayngold and Fayngold [3], among others. We kindly recommend these references for further reading.

References

1. Dirac P (1982) The principles of quantum mechanics, 4th edn. Oxford University Press, Oxford
2. Ekert A (1991) Quantum cryptography based on Bell's theorem. Phys Rev Lett 67:661–663
3. Fayngold M, Fayngold V (2012) Quantum mechanics and quantum information. Wiley, Singapore
4. Hirvensalo M (2004) Quantum computing. Springer, Berlin
5. Imre S, Balazs F (2005) Quantum computing and communications - an engineering approach. Wiley, Chichester
6. Kaye P, Laflamme R, Mosca M (2007) An introduction to quantum computing. Oxford University, Oxford
7. McMahon D (2008) Quantum computing explained, 1st edn. Wiley, New York
8. Mermin ND (2007) Quantum computer science – an introduction. Cambridge University Press, Cambridge
9. Mintert F, Viviescas C, Buchleitner A (2009) Basic concepts of entangled states. Springer, New York, pp 61–86
10. Nielsen MA, Chuang IL (2010) Quantum computation and quantum information. Cambridge University Press, Cambridge
11. Portugal R (2013) Quantum walks and search algorithms. Springer, New York
12. Vedral V (2006) Introduction to quantum information science. Oxford University Press, Oxford
13. Williams CP (2011) Explorations in quantum computing. 2nd edn. Springer, New York

http://www.springer.com/978-3-319-42793-5

Quantum Zero-Error Information Theory

Guedes, E.B.; de Assis, F.M.; Medeiros, R.A.d.C.

2016, XIX, 189 p. 50 illus., Hardcover
ISBN: 978-3-319-42793-5