Università degli studi di Ferrara

ENGINEERING DEPARTMENT

Laurea degree in
Electronics and Telecommunications Engineering

Quantum communications and entanglement

Candidate:
Stefano Guerrini

Supervisor:
Prof. Andrea Conti

Academic Year 2016-2017

Errata and Author's notes

Version 1 - 24/10/2017
Version 2 - 27/04/2018

Errata

Page	Reference	Error	Correction
15	Section 2.3.2	Mixed state	Mixed states
27	Middle page	$\sigma_x^2 = E[X^2] - E[X]^2$	$\sigma_x^2 = E\{X^2\} - E\{X\}^2$
36[1]	End page	all separable mixed states admits a LHV model	all the states that admit a LHV model are separable
45	The evolution of this system is determined by a unitary operator... (This "error?" is repeated in the thesis)	U in $\mathcal{H}_1 \otimes \mathcal{H}_2$	$U \in L(\mathcal{H}_1 \otimes \mathcal{H}_2)$
46	Using the Schmidt decomposition...	$A_i \in \mathcal{H}, B_i \in \mathcal{H}_E$	$A_i \in L(\mathcal{H}), B_i \in L(\mathcal{H}_E)$
54, 59		ϱ is the density matrix	ϱ is the density operator
63	Theorem 4.3.1	density matrix	density operator
78	Definition A.3	Pure	Product

The red marked errors are notation errors.

[1] This part (one of the last being written in the thesis) is exposed with the wrong words. The concept here is to show that there exist states which admit a LHVM but which are not separable.

Sommario

L'utilizzo della meccanica quantistica come mezzo fisico per la trasmissione delle informazioni, ha aperto nuovi orizzonti nel campo delle telecomunicazioni, specialmente nell'ambito della sicurezza. Sebbene lo studio di questi sistemi sia tuttora oggetto di una intensa attività di ricerca a livello mondiale, è opinione comune che tali sistemi possano raggiungere un livello di maturità sufficiente per poter essere prodotti su larga scala, nell'arco del prossimo decennio. In questo scenario, è di fondamentale importanza conoscere in dettaglio il funzionamento di tali sistemi, i loro punti di forza, le loro debolezze e gli aspetti ancora incompresi o inesplorati. Questa dissertazione tratta le basi teoriche delle comunicazioni quantistiche. In particolare, il lavoro di questa tesi mira a: (i) fornire una accurata descrizione matematica degli strumenti e dei sistemi per le comunicazioni quantiche, con particolare attenzione ai sistemi di distribuzione a chiave quantistica e ai protocolli di purificazione; (ii) individuare ed esporre gli aspetti teorici non ancora completamente investigati, ma di rilevante interesse dal punto di vista applicativo; e (iii) sviluppare un applicativo software per la simulazione di tali sistemi. Nell'esposizione vengono evidenziate le analogie e le differenze con i sistemi classici di comunicazione.

Abstract

The idea to use quantum mechanics as the physical mean to convey informations, has opened new horizons and possibilities in the future of telecommunications, especially in security sectors. Even if the study of quantum communication systems is a newborn field of research, it is now a common belief that they will become mature enough for large-scale implementation by the end of the next decade, and they will probably drive the evolution of information and communication technologies. In this futuristic scenario, it is of fundamental importance to get a deep knowledge of such systems, with an eye on their weakness and on the unexplored aspect of these technologies. Indeed, the main objective of this thesis is to acquire the basic knowledge about quantum communications.

In particular, this thesis work is intended to: (i) provide an accurate mathematical description and a physical interpretation of the tools and the systems that are extensively used in the field of quantum communications, with a particular attention to quantum key distribution protocols and purification algorithms; (ii) identify the theoretical aspects that still need to be investigated, but with a relevant impact on the applications; and (iii) develop a high-level software to simulate quantum systems. During the exposition of the above arguments, the analogies and the differences between quantum and classical communication systems are highlighted, to clarify the role of classical results and ideas in the field of applied quantum information theory. Indeed, the recent foundation of a dedicated technical committee in the IEEE community, has opened the possibility to use engineers know-how to boost up the research on quantum technology.

Contents

Errata and Author's notes **i**

1 Introduction **1**

2 Elements of Quantum Mechanics **5**

2.1 Postulates . . . 5
2.1.1 First postulate . . . 6
2.1.2 Second postulate . . . 6
2.1.3 Third postulate . . . 7
2.1.4 Fourth postulate . . . 7
2.1.5 Fifth postulate . . . 8
2.1.6 Sixth postulate . . . 11
2.2 Combining systems and entanglement . . . 11
2.2.1 Product states . . . 11
2.2.2 Entangled states . . . 12
2.3 The density operator . . . 13
2.3.1 Pure states . . . 13
2.3.2 Mixed state . . . 15
2.3.3 Reduced density operator . . . 16
2.3.4 Physical interpretation . . . 18
2.4 Generalized quantum measurements . . . 19
2.5 Quantum bits . . . 20
2.5.1 Pauli matrices . . . 20
2.5.2 The Bloch sphere . . . 21
2.5.3 Spin operators . . . 23
2.5.4 Entangled qubits . . . 25
2.5.5 Qubit operators . . . 26
2.6 Important results . . . 27
2.6.1 Uncertainty principle . . . 27
2.6.2 No-cloning theorem . . . 27

3 Quantum Entanglement **29**
3.1 Einstein's point of view . . . 29
3.2 Bell's theorem . . . 31
3.2.1 The CHSH inequality . . . 32
3.3 Formal definition . . . 34
3.3.1 Pure states . . . 34
3.3.2 Mixed states . . . 35
3.4 Entanglement manifestations . . . 36
3.4.1 Bell inequalities . . . 36
3.4.2 Entropy . . . 37
3.4.3 Entanglement measures . . . 38

4 Quantum Communications **39**
4.1 Theoretical applications . . . 39
4.1.1 Quantum teleportation . . . 39
4.1.2 Quantum dense coding . . . 41
4.1.3 Quantum key distribution . . . 42
4.1.4 Quantum key distribution using entanglement . . . 43
4.2 Quantum operations and quantum channels . . . 45
4.2.1 Deterministic quantum operations . . . 45
4.2.2 Physical interpretation of deterministic operations . . . 48
4.2.3 General quantum operations . . . 49
4.2.4 Quantum channels . . . 51
4.2.5 Local operations and classical communications . . . 53
4.2.6 Fidelity . . . 55
4.3 Entanglement distillation . . . 56
4.3.1 Bennett recurrence algorithm . . . 57
4.3.2 Efficient algorithm for phase-damping channels . . . 63
4.3.3 Simulation results . . . 66

5 Conclusions **69**

A Mathematical Preliminaries **71**
A.1 Hilbert Spaces . . . 72
A.2 Linear operators . . . 73
A.2.1 Definitions . . . 73
A.2.2 Dual space and the bra-ket notation . . . 73
A.2.3 Linear operators in finite dimensional space . . . 74
A.2.4 Adjoint operators . . . 75

A.2.5 Projection operators 76
A.3 Tensor product 77
A.3.1 Definition 77
A.3.2 Operators 79
A.3.3 Matrices 80

Bibliography **82**

List of Acronyms

BB84 Bennett-Brassard QKD

CHSH Clauser, Horne, Shimony and Holt

QXOR quantum XOR

E91 Ekert QKD

EPR Einstein, Podolsky and Rosen

LHVM local hidden-variable model

LOCC local operations and classical communication

QED quantum entanglement distillation

QKD quantum key distribution

SNR signal-to-noise ratio

Chapter 1

Introduction

The telecommunications field has experienced an incredible outgrowth during the last century and it is one of the driving force of the information and communication technologies (ICT) era. The success of the Internet and the increasing demand of high speed networks is an undeniable evidence.

A milestone in the development of the telecommunications has been the pioneering treatise of Shannon [1], worked out in 1948. Shannon has been the first who defined information and gave a formal mathematical description of communication systems, and the problems which inevitably affect all communications. These theoretical studies have permitted, on one side, to understand the intrinsic limits on the performances of real communication systems and, on the other side, they have stimulated the research in finding a way to approach these limits.

The global diffusion of the Internet and the success of cloud applications and services, faced up the users with the problem of keeping their sensitive data safe. This is a well-known problem in the history of mankind, but now it has reached unprecedented proportions as it has been considered on of the three key policy priorities in the last G7 meeting. Modern cryptography is based on another outbreaking treatise of Shannon [2], who gave to cryptography a formal mathematical framework that can be used to prove the theoretical security of a cryptographic system. The most used cryptographic systems [3] have two fundamental limits: first, their security relies upon the difficulty of reversing a particular cryptographic problem, making them potentially vulnerable with an increment in the computational power; and second, if a malicious user intercepts the messages without leaving traces, no one can be informed about its presence on the communication channel. Even if the first problem could in principle be "solved" by using new complex cryptographic systems or longer keys, the possibility to intercept an unauthorized user in the channel is not in any way possible using classical systems.

The solution to this problems came out from an unexpected field of physics: that

is, quantum mechanics. Indeed, it turns out that the peculiarities of this strange world, described in the earlier '20s, can be used as an advantage in cryptography. One of the key points of the quantum theory is that any measurement performed on a quantum system, inevitably perturbs its state. So, if a quantum channel is used to connect two parties, this physical effect could then be exploited to intercept and report every action of an unauthorized user in the channel to the end users. This is the wonder of the so-called quantum key distribution (QKD), which was invented in the 1984 by Bennett and Brassard. It is worth to note that such a physical property is not contemplated by the laws of classical physics and an analogue security simply can not be achieved using classical communication channels.

The possible applications of quantum effects as a physical resource for communication tasks, does not end here. The most controversial effect of quantum mechanics, namely entanglement, who puzzled different greatest mind for almost half a century, turns out to be the fundamental pillar upon which build quantum communication systems. The discovery of some key effects like quantum teleportation and superdense coding, and the discovery of the quantum bit, during the 1990s, has definitely consecrated quantum mechanics as one of the most promising technologies for the future, boosting up the research on the field now known as quantum information.

However, as it happens in classical communication systems, quantum states are inevitably subject to noise and attenuation phenomenas during their transit in quantum channels. Furthermore, entanglement is inherently a very weak link between quantum particles which is strongly subject to the decoherence phenomenon [4] that inevitably destroys the link that was originally created. All these degradation effects does not allow for faithful communications between parties, which were originally conceived to work in an ideal world. For this reason, entanglement-assisted communication systems are still an active field of research.

Inspired by classical communication theory, different theoretical solution has been proposed in the literature to face up the entanglement degradation phenomenas, as quantum error-correcting codes (QECCs) to provide quantum bits with an a-priori protection to noise phenomenas and entanglement purification protocols (EPPs) which make use of local quantum operation and a classical communication channel to distillate a small set of purified states, starting from a larger set of noisy states. In this sense, the communication theory developed by Shannon has been a profound source of inspiration for the whole field of quantum information. Despite their powerfulness, these solutions have not yet been implemented in practice.

From the birth of quantum communications, lot of research effort were spent on trying to get a physical implementation of quantum communication systems. It was immediately clear that this process was far to be trivial and the field of ap-

plied quantum communication is still a very active topic of research. The Chinese government has recently raised funds to put into orbit a satellite for quantum communications which has already reached important and unprecedented results [5, 6] as entanglement distribution and teleportation over one thousand kilometers, which first allowed to use these phenomenas over interesting distances. These work boosted up the research on satellite quantum communication, as free space attenuation is lower than the one achievable in the best optical fibers [5]. However, these technologies are far to be ready for commercialization or large scale implementation, and lot of work needs still to be done to achieve this difficult task. Despite these difficulties, it is now commonly believed [7] that quantum technologies are a potentially outbreaking technology for the future, and they will probably become fully-productive by the end of the next decade. This means that we live in a privileged period in which doing research on quantum technologies is fundamental for the near-future.

As quantum technologies will probably be a driving force in the future of ICT, an increasing interest in this topic is expected from the industrial world. Indeed, both Google and IBM have recently announced massive investments on quantum computers [8, 9] in order to bring this very expensive technologies out of scientific laboratories. This will also allow a faster and better deployment of future quantum communication systems, as soon as they will be ready for implementation.

Motivations and objectives

The main objective of this thesis is to collect and gather together a set of results from different research areas of quantum information and the development of a framework to analyze quantum communication systems. Furthermore, the opened questions and the possible future developments of the theory are emphasized. The big picture is to define and pave the way for a research activity in the field of quantum communications.

The introduction of quantum mechanics as the physical mean for communication systems broaden new and unknown horizons in the applications. However, the typical engineer's background is different from the preparation of a physicist so that this gap must be first filled in order to work with these cutting-edge topics. On the other side a particular attention must be taken in order to don't lose the focus on the engineers objective: that is the application of quantum information. Indeed, the mathematical tools needed to tackle quantum information are different from the ones given in a typical quantum physics course so that a recap is given in the first part, trying to catch the similarities with classical communication systems. In the second part, an eye is keep on the most promising application and the recent advances in quantum information and the result of different simulations is given.

The remainder of this dissertation is organized as follows.

Chapter 2 recaps the main concepts and the principal mathematical tools from quantum mechanics that are needed to describe and comprehend the theory and the physical effects that are extensively used in quantum communications.

Chapter 3 gives a detailed overview of the entanglement phenomenon and the mathematical tools needed to understand and characterize it.

Chapter 4 gives a comprehensive overview on the main applications and protocols, and illustrates the recent advances in that field. Furthermore, some preliminary results are illustrated.

Chapter 2

Elements of Quantum Mechanics

In this chapter, a brief overview of the tools and results from quantum mechanics is given. This treatment is not intended to be exhaustive, since lot of introductive [10, 11, 12] and advanced [13, 14] treatises are available in the literature. The rationale here is to review the physical concepts of quantum mechanics, and the mathematical tools needed to understand the theory behind quantum communication systems. This chapter makes use of mathematical results from functional analysis and linear algebra, some of which are reported and commented in the appendix.

2.1 Postulates

Every physical theory is described by mean of a mathematical framework. There are different, but mathematically equivalent, formulations of Quantum Mechanics, which grew up in the early twentieth century by the mind of various scientists who started from different ideas and different hypothesis, which lead to different *interpretations* of quantum mechanics. The most common approach is based on Dirac-von Neumann axioms, since they were first hypotized by Dirac [15], in 1930, and then mathematically refined by von Neumann [16], in 1932. Even if they don't have a persuasive a-priori justification, the Dirac-von Neumann axioms provide a clean and elegant mathematical framework to quantum mechanics, dramatically supported by experimental evidences. The postulates presented in this section are essentially a restatement of the ones proposed by Cohen-Tannoudji [13]. It is possible to reformulate the postulates such that they form the minimum number to describe quantum mechanics. However, even if this could be a mathematically interesting question, it is of little relevance from a physical point of view [11].

2.1.1 First postulate

Postulate 1 (States)**.** The state space of an isolated physical system is a separable complex Hilbert space $\mathcal{H}$. The system is completely described by its state vector $|\psi\rangle$, which is a unit vector in the space $\mathcal{H}$.

The first postulate is very easy to understand from a mathematical perspective, but it immediately shows the counterintuitiveness of quantum mechanics. In fact, it has no counterpart in classical mechanics, in which the state space is always a *set* of points (e.g. the position of a particle is a real vector in a three-dimensional space) and not a vector space.

Consequences. The most important consequence of the first postulate is the state superposition principle: if $|\psi_1\rangle$, $|\psi_2\rangle$ are two possible states in $\mathcal{H}$, then $|\psi\rangle = \alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle$ with $\alpha_1, \alpha_2 \in \mathbb{C}$ is also a possible state in $\mathcal{H}$.

2.1.2 Second postulate

Postulate 2 (Observables)**.** Every observable is associated with a linear, self-adjoint operator $\mathcal{L}$ on the space $\mathcal{H}$. The possible outcomes of the measurements are the eigenvalues of $\mathcal{L}$.

Consequences. Since $\mathcal{L}$ is self-adjoint, its eigenvalues are real (Theorem A.2.3). This means that every measurable quantity of a quantum system is a real number. Furthermore, if the state space $\mathcal{H}$ is finite-dimensional, then $\mathcal{L}$ could be uniquely represented by a complex matrix $\mathbf{L}$ (Lemma A.2.2), which depends on the representation basis $\{|i\rangle\}_i$ chosen for $\mathcal{H}$, so that $\mathbf{L}_{ij} = \langle i|\mathcal{L}|j\rangle$.

Remark 1. The interesting state spaces, in almost all cases of practical interest in quantum communications, are finite dimensional (e.g. qubits). This is a remarkable property since it allows to work with the simpler and well understood theory of matrices, and avoid mathematical complications that may arise with infinite-dimensional spaces and, in particular, with the continuous spectrum of operators.

Remark 2. The assumption on $\mathcal{L}$ to be self-adjoint, which has strong consequences on the mathematical properties of the measurement, was first advanced by von Neumann [16], relying on physically reasonable and ideal assumptions. However, it turns out that in different cases of practical interest in quantum information theory [17], they are unreasonable. It will be shown that such a postulate could be generalized by introducing the concept of *generalized measurements*. To distinguish between them, the measurements as defined in this postulate, are someteime referred as *projective* or *von-Neumann* measurements.

2.1.3 Third postulate

Postulate 3 (Born's Rule)**.** If the system is in the state $|\psi\rangle$, the probability to get the measurement λ_n from the observable $\mathcal{L}$ is equal to

$$\mathbb{P}(\lambda_n) = \langle\psi| \mathcal{P}_n |\psi\rangle$$

where $\mathcal{P}_n$ is the projector onto the eigenspace $\mathcal{E}_n$ corresponding to λ_n.

The Born's rule is one of the core features of quantum mechanics, as it tells that quantum systems have an intrinsic stochastic behavior. Furthermore, it can be used to define the concept of distinguishable states. Two states are said to be physically different if there exists a measurement which could *reliably* (e.g. with probability 1) distinguish between them. This simple definition highlights the importance of orthogonal states for a quantum system, as the following properties show:

Lemma 2.1.1. *All orthogonal states can always be distinguished*

Lemma 2.1.2. *Non orthogonal states can't be reliably distinguished*

Remark 3. The Born's Rule is a way to justify that a state vector must be unitary. Indeed, the summation of the probabilities of the single experiment outcomes must sum up to 1, according to the axioms of probability theory [18]. If the state vector is not unitary, this condition is not satisfied at all.

The non-degenerate case

A simpler version of the Born's rule could be used in the case that all eigenvalues of $\mathcal{L}$ are non-degenerate[1]. Indeed, in this case, every eigenvalue λ_n is associated with one eigenvector $|\lambda_n\rangle$, so that $\mathcal{P}_n = |\lambda_n\rangle \langle\lambda_n|$. The Born's rule becomes the following:

Postulate. If the system is in the state $|\psi\rangle$, the probability to get the measurement λ_n from the observable $\mathcal{L}$ is equal to $|\langle\lambda_n|\psi\rangle|^2$, where $|\lambda_n\rangle$ is the eigenvector associated to λ_n.

2.1.4 Fourth postulate

Postulate 4 (Wavefunction Collapse)**.** If the measurement of the observable $\mathcal{L}$, on a system in the state $|\psi\rangle$, gives the result λ_n, then the state $|\psi'\rangle$ of the system immediately after the measurement is the normalized projection of $|\psi\rangle$ onto the eigenspace $\mathcal{E}_n$ associated to λ_n, e.g.:

$$|\psi'\rangle = \frac{\mathcal{P}_n |\psi\rangle}{\sqrt{\langle\psi| \mathcal{P}_n |\psi\rangle}}$$

[1] An eigenvalue of $\mathcal{L}$ is said to be degenerate if there exist at least two linearly independent vectors which are both eigenvectors of $\mathcal{L}$ with the same eigenvalue.

Remark 4 (Reproducibility)**.** This postulates is of fundamental importance to ensure the reproducibility of quantum mechanics: the first measurement on a system will always have a probabilistic nature but, due to the wavefunction collapse property, the same measurement performed afterwards will always confirm the previous result with certainty, and no other results are possible.

Remark 5. Let $\mathcal{L}$, $\mathcal{M}$ be two different observables for a quantum system. In order to measure both $\mathcal{L}$ and $\mathcal{M}$ simultaneously, they must share a complete basis of eigenvectors, since the state of the system collapses after the measurement. This is equivalent [13] to say that $[\mathcal{L}, \mathcal{M}] = 0$.

The non-degenerate case

Postulate. If the measurement of the observable $\mathcal{L}$ on the system in the state $|\psi\rangle$ gives the result λ_n, then the state of the system after the measurement is $|\lambda_n\rangle$.

2.1.5 Fifth postulate

Postulate 5 (Evolution)**.** The evolution of a *closed* quantum system is described by a unitary operator $\mathcal{U}$ in $\mathcal{H}$. Let the system be in the state $|\psi(t_0)\rangle$ at the time istant t_0. Then, the state of the system $|\psi(t)\rangle$ at the time istant t is:

$$|\psi(t)\rangle = \mathcal{U}(t, t_0)\,|\psi(t_0)\rangle \tag{2.1}$$

With:

$$\mathcal{U}^\dagger \mathcal{U} = 1$$

Remark 6. The operator $\mathcal{U}$ does not depend on the initial state $|\psi(t_0)\rangle$.

Remark 7. The requirement for evolution operator to be unitary, could be justified by a fundamental principle of physics: that is, reversibility of laws [10]. In plain english, this means that physically distinguishable states must evolve to physically distinguishable states, otherwise there would be a loss of information. This is true if the operator is unitary, indeed let $|\psi(0)\rangle$ and $|\varphi(0)\rangle$ be distinguishable states, e.g.: $\langle\psi(0)|\varphi(0)\rangle = 0$. Then:

$$\langle\psi(t)|\varphi(t)\rangle = \big\langle\psi(0)\big|\mathcal{U}^\dagger\mathcal{U}|\varphi(0)\big\rangle = \langle\psi(0)|\varphi(0)\rangle = 0$$

Remark 8. The "conservation of information", as described in the previous remark, is a consequence of the unitariness of $\mathcal{U}$. This is a particular case of a more general principle that is called *conservation of overlaps* [10]:

$$\forall\,|\psi(0)\rangle\,, |\varphi(0)\rangle \in \mathcal{H} \implies \langle\psi(t)|\varphi(t)\rangle = \langle\psi(0)|\varphi(0)\rangle$$

In other words, this means that the logical relationships between states is preserved during the system evolution. If this principle is not observed, after the system has evolved, there would be a violation of probability axioms, thus leading to internal inconsistencies of the whole theory. It is possible to show that conservation of overlaps is mathematically equivalent to unitarity.

The Schrödinger equation

It is possible to give an alternative form to the evolution equation (2.1), which gives further physical insights. The evolution operator $\mathcal{U}$ is unitary and it is natural to assume that $\mathcal{U}$ is also continuous, e.g. $\mathcal{U}(t, t_0) \xrightarrow{t \to t_0} I$, as the system has not evolved for $t = t_0$. By Theorem A.2.5, the operator $\mathcal{U}$ could then be written as:

$$\mathcal{U}(t, t_0) = e^{itH(t_0)}$$

Where $H(t)$ is a self-adjoint operator. If $t = t_0 + \varepsilon$, with $\varepsilon \to 0$, then, ignoring higher order infinitesimals, it follows that:

$$\mathcal{U}(t_o + \varepsilon, t_0) \approx I - i\varepsilon H(t_0)$$

So that:

$$|\psi(t_0 + \varepsilon)\rangle = |\psi(t_0)\rangle - i\varepsilon H(t_0) |\psi(t_0)\rangle$$

By rearranging the terms, and taking the limit as $\varepsilon \to 0$

$$\lim_{\varepsilon \to 0} \frac{|\psi(t_0 + \varepsilon)\rangle - |\psi(t_0)\rangle}{\varepsilon} = \frac{\partial |\psi\rangle}{\partial t}\bigg|_{t_0} = -iH(t_0) |\psi(t_0)\rangle$$

The following result is thus obtained:

$$\frac{\partial}{\partial t} |\psi(t)\rangle = -iH(t) |\psi(t)\rangle \tag{2.2}$$

The operator $H(t)$ is called *Hamiltonian*, by analogy to classical mechanics, as it represents the total energy of the system [10, 15]. This results makes the previous equation completely unsatisfactory from a dimensional point of view: indeed, H is expressed in Joule (J), while time in seconds (s). Indeed, the left hand side of (2.2) has the dimension of s^{-1}, while the right hand side, of J. Thus a constant must be introduced to make the equation consistent with the measurement unities[2]. With such a correction, (2.2) becomes the time-dependent *generalized Schrödinger equation*:

[2]Without loss of generality, the value of $\hbar$ could be assumed to be 1, such that it could be ignored when doing calculations [17]. However, to make the prediction according reality, $\hbar$ must be equal to the reduced Planck constant, e.g. $\hbar = h/2\pi = 1.055 \times 10^{-34}$ J $\cdot$ s.

$$i\hbar\frac{\partial}{\partial t}\left|\psi(t)\right\rangle = H(t)\left|\psi(t)\right\rangle \tag{2.3}$$

When the Hamiltonian does not depend on time, e.g. $H(t) = H$, the system is said to be *autonomous* or *closed*, meaning that no forces act on the system [15]. In this case the total energy of the system is conserved, and the Schrödinger equation has the analytical solution [13]:

$$\left|\psi(t)\right\rangle = \sum_j \left\langle E_j|\psi(0)\right\rangle e^{-\frac{i}{H}E_j t}\left|E_j\right\rangle$$

Where E_j and $|E_j\rangle$ are, respectively, the eigenvalues and the eigenvectors of the Hamiltonian operator H.

Remark 9. If the energy varies with time, it means that the system is perturbed by an external action [15]. In this case, the Schrödinger equation should not be used to predict the system evolution, because the system interacts with the environment, and thus it is not closed. However, in different cases of practical interest, it is possible to write down a time-varying Hamiltonian which approximates the real behavior of the system [17].

Ignoring the overall phase factor

When dealing with the states of a quantum system, it is always possible to ignore the overall phase factor, because it has no observable effects on a physical measurement. Indeed, consider two states $|\varphi\rangle, |\psi\rangle$ such that:

$$\left|\varphi\right\rangle = e^{j\vartheta}\left|\psi\right\rangle$$

Where $\vartheta \in \mathbb{R}$. The two vectors have the same amplitude, indeed:

$$\left\langle\varphi|\varphi\right\rangle = \left\langle\psi\right| e^{-j\vartheta}e^{j\vartheta}\left|\psi\right\rangle = \left\langle\psi|\psi\right\rangle$$

Furthermore, the probabilities of an arbitrary measurement are the same:

$$P_\lambda = |\left\langle\lambda|\varphi\right\rangle|^2 = |e^{j\vartheta}\left\langle\lambda|\psi\right\rangle|^2 = |\left\langle\lambda|\psi\right\rangle|^2$$

And so are the expected values:

$$\left\langle\varphi|\mathcal{L}|\varphi\right\rangle = \left\langle\psi e^{-j\vartheta}\middle|\mathcal{L}|e^{j\vartheta}\psi\right\rangle = \left\langle\psi|\mathcal{L}|\psi\right\rangle$$

Therefore, changing the *overall* phase factor of a state does not affects any physical prediction. This means that the two states are physically equivalent.

2.1.6 Sixth postulate

Postulate 6 (Composite systems)**.** The space state $\mathcal{H}$ of a system composed by two subsystems, $\mathcal{H}_1$ and $\mathcal{H}_2$, is given by the tensor product:

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

Remark 10. This postulate could be derived as a consequence of the *superposition principle*, which has strong experimental confirmations and that should not come unexpected from the first postulate. The main consequence of this postulate is the entanglement phenomenon, which has no counterparts in classical physics. This effect is the base brick upon which to build quantum communication systems, and it will be examined in chapter 3.

Remark 11. Different notations will be used throughout this Thesis, to express the product vector $|\psi\rangle = |\varphi\rangle \otimes |\xi\rangle \triangleq |\varphi\rangle\,|\xi\rangle \triangleq |\varphi\xi\rangle$, depending on the context to simplify the notation or avoid misunderstandings.

2.2 Combining systems and entanglement

The last postulate has important consequences for composite system. Entanglement is a fundamental phenomenon of quantum mechanics, both from a theoretical and an applicative point of view, and it will be reviewed in detail in the dedicated chapter.

2.2.1 Product states

Definition 2.2.1. *A state $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is called product state if there exists $|\varphi\rangle \in \mathcal{H}_1$, $|\xi\rangle \in \mathcal{H}_2$ such that:*

$$|\psi\rangle = |\varphi\rangle \otimes |\xi\rangle$$

Physical meaning of product states

A product state physically represents a combination of two system which don't interact, meaning that every operation on one of them does not depends, or perturb, the other. To show this, suppose, without loss of generality, that a measurement $\mathcal{L}_1$ is performed on the first subsystem. Then the probability to observe λ_n is:

$$\mathbb{P}(\lambda_n) = \langle\psi|\,\tilde{\mathcal{P}}_n\,|\psi\rangle = \langle\varphi|\,\langle\xi|\,(\mathcal{P}_n \otimes I)\,|\varphi\rangle\,|\xi\rangle = \langle\varphi|\,\mathcal{P}_n\,|\varphi\rangle$$

Such a probability does not depend on the state $|\xi\rangle$ of the second subsystem. Analogously, the state after the projection is independent from $|\xi\rangle$:

$$|\psi'\rangle = \frac{\tilde{\mathcal{P}}_n |\psi\rangle}{\langle\varphi| \mathcal{P}_n |\varphi\rangle} = \frac{\mathcal{P}_n |\varphi\rangle}{\langle\varphi| \mathcal{P}_n |\varphi\rangle} \otimes |\xi\rangle = |\varphi'\rangle \otimes |\xi\rangle$$

In probabilistic terms, every event on one subsystem is (statistically) independent from any other event on the second system. Indeed, a generalization of the previous result can be obtained by choosing two observables $\mathcal{A}$ and $\mathcal{B}$ on, respectively, $\mathcal{H}_1$ and $\mathcal{H}_2$, so that:

$$\begin{aligned}\mathbb{P}(\mathcal{A} = \lambda_n \cap \mathcal{B} = \mu_m) &= \langle\psi| \langle\xi| \mathcal{P}_n^A \mathcal{P}_m^B |\psi\rangle |\xi\rangle = \langle\psi| \mathcal{P}_n^A |\psi\rangle \langle\xi| \mathcal{P}_m^B |\xi\rangle \\ &= \mathbb{P}(\mathcal{A} = \lambda_n) \mathbb{P}(\mathcal{B} = \mu_m)\end{aligned}$$

2.2.2 Entangled states

Whenever a system is not in a product state, as specified in the definition 2.2.1, the system is said to be into an *entangled* state. Despite its very simple definition[3], entanglement has profound implications, which have no counterparts in classical mechanics. When a system is into an entangled state $|\psi\rangle$, it is not possible to characterize the two subsystems by mean of a state vector, as if they were in a product state, even if the state vector of the composite system is well known. It is immediately clear that this is a peculiar behavior: in a *classical* world, if the state of a combined system is known, then the state of the single constituents is also known. This peculiar characteristic of quantum mechanics was first noted by Einstein [19], and then refined by Schrödinger [20, 21].

Entanglement is the core feature and one of the most counterintuitive aspect of quantum mechanics. It took different decades to mathematize the concept and to draw up experiments who can reveal its real nature. Even if almost a century has passed since its discovery, entanglement is still an active subject of study both from a theoretical and practical point of view. Indeed, it is a very powerful phenomenon on which to build quantum communication systems. The aspects discussed here will be deepened in the following chapter.

These considerations immediately lead to an interesting question: if a system is into an entangled state, how is it possible to predict the behavior of the single subsystem if a state vector for it could not even be defined? The answer is given by the density operator, which will be introduced in the following section.

[3] A more formal definition will be given in the next chapter.

2.3 The density operator

Whenever the state of a system is known, the postulates of quantum mechanics allow to make all possible predictions about the future state or the outcomes of a measurement. In practice, the state of a system is not always perfectly determined. As an example, this situation could occur if the initial state preparation is somewhat affected by noise, or if the generating process is too complex to model. This is nothing special, and it is also used in classical mechanics to model the *uncertainty* about a physical phenomenon. However, as described in the previous section such an uncertainty can also be a consequence of the entanglement phenomenon, which can not be explained in classical terms and which reflects the incapacity of quantum mechanics to assign a definite state to a system. Whenever the state of a system is unknown, it is necessary to define a mathematical tool which can model such an uncertainty and, at the same time, carries on all needed informations to make all possible predictions about the system itself. It must be noted [13] that, in this case, the uncertainty manifests on two levels: (i) on the *initial* state of the system, which is unknown to the experimenter (as in classical mechanics); and (ii) on the possible outcomes of a measurements, which have an intrinsic probabilistic nature in quantum mechanics.

2.3.1 Pure states

Before studying the general case, it is useful to introduce the density operator in the case that the state of the system is perfectly known. In this case, the system is said to be in a pure state. The state could then be expressed using an orthonormal basis:

$$|\psi\rangle = \sum_i \alpha_i |i\rangle$$

If $\mathcal{A}$ is an observable, it could be expressed in matrix form:

$$\mathbf{A}_{ij} = \langle i| \mathcal{A} |j\rangle$$

Then, from postulates 3:

$$\langle \mathcal{A} \rangle = \langle \psi| \mathcal{A} |\psi\rangle = \sum_i \sum_j \alpha_i^* \alpha_j \mathbf{A}_{ij} \tag{2.4}$$

It is thus possible to define the coefficients:

$$\mathbf{R}_{ji} = \alpha_j \alpha_i^* = \langle j|\psi\rangle \langle \psi|i\rangle$$

That are the matrix elements of the following operator, called *density operator*:

$$\varrho = |\psi\rangle \langle \psi| \tag{2.5}$$

Thus, from equation (2.4):

$$\langle \mathcal{A} \rangle = \sum_i \sum_j \mathbf{R}_{ji} \mathbf{A}_{ij}$$

could be rewritten as:

$$\langle \mathcal{A} \rangle = \mathrm{Tr}\left\{ \mathbf{AR} \right\} \tag{2.6}$$

Or, equivalently, using the language of the operators:

$$\langle \mathcal{A} \rangle = \mathrm{Tr}\left\{ \mathcal{A}\varrho \right\} \tag{2.7}$$

Analogously, the probability to observe λ_n could be derived by replacing $\mathcal{A}$ with the projector $\mathcal{P}_n$ in (2.4), so that:

$$\mathbb{P}\left(\lambda_n\right) = \mathrm{Tr}\left\{ \mathcal{P}_n \varrho \right\} \tag{2.8}$$

and if the measurement $\mathcal{A}$ gives λ_n the system collapses to the density operator:

$$\varrho' = \frac{\mathcal{P}_n \varrho \mathcal{P}_n^\dagger}{\mathrm{Tr}\left\{ \mathcal{P}_n \varrho \mathcal{P}_n^\dagger \right\}}$$

Finally, if the system evolves according to the unitary operator $\mathcal{U}$, then:

$$|\psi(t)\rangle = \mathcal{U} \, |\psi(t_0)\rangle$$

$$\varrho(t) = \mathcal{U} \varrho(t_0) \mathcal{U}^\dagger \tag{2.9}$$

where $\varrho(t)$ is the density operator at the time istant t. It is also possible to derive an evolution equation for $\varrho(t)$, using the Hamiltonian operator [13]:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} \varrho(t) = [H(t), \varrho(t)] \tag{2.10}$$

This means that the density operator $\varrho(t)$ is *sufficient* to describe **any** physically observable quantity of a system. Using this results, it is also possible to reformulate the postulates of quantum mechanics using the density operator [17, 22].

Properties

If the system is in a pure state it follows, from the definition (2.5), that:

$$\varrho^\dagger = \varrho$$
$$\varrho^2 = \varrho$$
$$\mathrm{Tr}\left\{ \varrho^2 \right\} = 1$$

Moreover, since ϱ is an idempotent operator, it follows from Lemma A.2.7, that all the eigenvalues of ϱ are either 0 or 1.

2.3.2 Mixed state

As already pointed out in the introductory paragraph, there are cases of practical interest in which the state is not known with certainty, and the system is said to be in a mixed state. Let suppose that a system could be in the states $|\psi_1\rangle, |\psi_2\rangle, ...$ with probability, respectively, $p_1, p_2, ...$, with the normalization condition $\sum_k p_k = 1$. In this case, the probability $\mathbb{P}(\lambda_i)$ to observe the result λ_i could be derived using the law of total probability:

$$\mathbb{P}(\lambda_i) = \sum_k p_k \mathbb{P}(\lambda_i|k)$$

Where:

$$\mathbb{P}(\lambda_i|k) = \langle\psi_k| \mathcal{P}_i |\psi_k\rangle = \mathrm{Tr}\{\varrho_k \mathcal{P}_i\}$$

is the probability to get the measurement λ_i if the system is in the state $|\psi_i\rangle$. Using the linearity of the trace operator:

$$\mathbb{P}(\lambda_i) = \sum_k p_k \,\mathrm{Tr}\{\varrho_k \mathcal{P}_i\} = \mathrm{Tr}\left\{\sum_k p_k \varrho_k \mathcal{P}_i\right\}$$

This suggests to define the density operator as:

$$\varrho = \sum_k p_k \varrho_k \tag{2.11}$$

to express all physical predictions about the system. Note that this is a generalization of the density operator in the pure state case, where $p_k = \delta_j$.

General properties

From the definition (2.11), the following properties follows immediately:

$$\varrho^\dagger = \varrho$$
$$\mathrm{Tr}\{\varrho\} = 1$$

Furthermore, the density operator is also positive-semidefinite, indeed for all $|\varphi\rangle$:

$$\langle\varphi|\varrho|\varphi\rangle = \sum_k p_k \langle\varphi|\varrho_k|\varphi\rangle = \sum_k p_k |\langle\varphi|\psi_k\rangle|^2 \geq 0$$

In the case of a mixed state, it is not generally true that $\varrho^2 = \varrho$. This implies that:

$$\mathrm{Tr}\left\{\varrho^2\right\} \leq 1$$

However this property can be used to get a characterization of pure states, in terms of density operators:

Theorem 2.3.1. *Let ϱ be a density operator. Then ϱ represents a pure state if and only if* $\mathrm{Tr}\{\varrho^2\} = \mathrm{Tr}\{\varrho\} = 1$.

Proof. The necessary condition follows immediately from the properties of the density operator in the pure case. Now assume that $\mathrm{Tr}\{\varrho^2\} = 1$. Since ϱ is a self-adjoint operator, it could be expressed in the diagonal form:

$$\varrho = \sum_i \lambda_i |i\rangle \langle i|$$

This implies that:

$$\varrho^2 = \sum_i \lambda_i^2 |i\rangle \langle i|$$

Since $\mathrm{Tr}\{\varrho^2\} = \mathrm{Tr}\{\varrho\} = 1$, it follows that $\sum_i \lambda_i = \sum_i \lambda_i^2 = 1$. Thus, by rearranging the terms:

$$\sum_i (\lambda_i - \lambda_i^2) = 0$$

Because $\lambda_i \in [0, 1]$, it follows that $\lambda_i - \lambda_i^2 \geq 0$. This two constraints implies that either $\lambda_i = 0$ or $\lambda_i = 1$. This means that there is only one eigenvalue, let's say λ_j, such that $\lambda_j = 1$, while all the others are zero. Thus:

$$\varrho = |j\rangle \langle j|$$

This density operator represents the pure state $|j\rangle$. □

Sometimes [10], the above characterization is given in the following terms:

Corollary 2.3.2. *Let ϱ be a density operator. Then ϱ represents a pure state if and only if it has only one non-zero eigenvalue.*

2.3.3 Reduced density operator

When dealing with composite systems it is possible to define the density operator ϱ for the composite system in the state space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ using the previous definitions, depending on the a-priori knowledge of the initial state. However, it is fundamental to derive an operator, namely ϱ_1, which describes the knowledge about the first subsystem $\mathcal{H}_1$ (and, analogously, an operator ϱ_2 for the second subsystem) which is sufficient to perform any prediction with respect to the first subsystem (or, equivalently, the second). The operators ϱ_1 and ϱ_2 are inevitably related to ϱ.

Let's take the composite state space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ and suppose, without loss of generality, that $|\psi\rangle \in \mathcal{H}$ is a pure state. Then its density operator is:

$$\varrho = |\psi\rangle \langle \psi|$$

Let $\mathcal{A}$ be an operator on $\mathcal{H}_1$, and $\tilde{\mathcal{A}}$ its extension into $\mathcal{H}$. If the basis $|ij\rangle$ is used in $\mathcal{H}$ then:

$$|\psi\rangle = \sum_{ij} \alpha_{ij} |ij\rangle$$

The mean value of $\tilde{\mathcal{A}}$ is given by:

$$\langle\psi| \tilde{\mathcal{A}} |\psi\rangle = \sum_{ij} \sum_{i'j'} \alpha^*_{ij} \alpha_{i'j'} \langle ij| \tilde{\mathcal{A}} |i'j'\rangle$$

Since $\tilde{\mathcal{A}} = \mathcal{A} \otimes I$ then $\langle ij| \tilde{\mathcal{A}} |i'j'\rangle = \langle i| \mathcal{A} |i'\rangle \langle j|j'\rangle = \mathbf{A}_{ii'} \delta_{jj'}$, thus:

$$\langle\tilde{\mathcal{A}}\rangle = \sum_{ii'} \left[\sum_j \alpha^*_{ij} \alpha_{i'j} \right] \mathbf{A}_{ii'}$$

This expression is in the same form as (2.4). This suggests to define the quantities:

$$(\mathbf{R}_1)_{i'i} = \sum_j \alpha^*_{ij} \alpha_{i'j} = \sum_j \langle i'j| \varrho |ij\rangle$$

So that the mean values assumes a form analogue to (2.6) :

$$\langle\tilde{\mathcal{A}}\rangle = \mathrm{Tr}\{\mathbf{R}_1 \mathbf{A}\}$$

where $\mathbf{R}_1$ is called the reduced density matrix associated to the first subsystem. The same passages leads to the definition of $\mathbf{R}_2$, the reduced density matrix of the second subsystem. In the next paragraph, a generalization of this result is given, extending and formalizing the definition to operators.

Alternative representations

In the last section, a *matrix* form representation of the reduced density operator is given. However, there are different equivalent ways to define it. Given the density operator ϱ, defined in $L(\mathcal{H}_1 \otimes \mathcal{H}_2)$, it is possible to describe the reduced density operator ϱ_1, associated to the subsystem 1, as a linear operator acting on $\mathcal{H}_1$. Thus:

$$\varrho_1 = \mathrm{Tr}_2\{\varrho\}$$

Where $\mathrm{Tr}_2 : L(\mathcal{H}_1 \otimes \mathcal{H}_2) \to L(\mathcal{H}_1)$, is called partial trace operator, defined as:

$$\mathrm{Tr}_2\{\mathcal{A} \otimes \mathcal{B}\} = \mathcal{A}\,\mathrm{Tr}\{\mathcal{B}\} \tag{2.12}$$

This particular representation is commonly translated into a somewhat confusing notation:

$$\varrho_1 = \mathrm{Tr}_2\{\varrho\} = \sum_i \langle i| \varrho |i\rangle \tag{2.13}$$

At a first glance, the bra-ket notation used here may be misleading. Indeed $\langle i| \varrho |i\rangle$ is not a scalar product but an operator from $\mathcal{H}_1 \otimes \mathcal{H}_2$ into $\mathcal{H}_1$, so that this notation is just a shorthand for $(I_1 \otimes \langle i|)\varrho(I_1 \otimes |i\rangle)$.

Remark. This representation is useful whenever the density operator is expressed as a linear combination of projection operators. Indeed $\langle i|\,\varrho\,|i\rangle$ is not a complex number as usual, but an operator from $\mathcal{H}_1 \otimes \mathcal{H}_2$ into $\mathcal{H}_1$ defined as in (2.12). To prove the equivalence, note that ϱ is an operator, so it could be decomposed as:

$$\varrho = \sum_{jj'} \sum_{kk'} \mathbf{R}_{jj'kk'} \,|j\rangle\,\langle j'| \otimes |k\rangle\,\langle k'|$$

The reduced density operator for the first subsystem is obtained by *tracing out* the second one. By applying the definition (2.12):

$$\mathrm{Tr}_2\,\{\varrho\} = \sum_{jj'} \sum_{k} \mathbf{R}_{jj'kk} \,|j\rangle\,\langle j'|$$

Equivalently, by applying the notation of definition (2.13):

$$\sum_i \langle i|\,\varrho\,|i\rangle = \sum_i \sum_{jj'kk'} \mathbf{R}_{jj'kk'} \,|j\rangle\,\langle j'|\,\langle i|k\rangle\,\langle k'|i\rangle = \sum_i \sum_{jj'} \mathbf{R}_{jj'ii} \,|j\rangle\,\langle j'| = \mathrm{Tr}_2\,\{\varrho\}$$

It is possible to prove that the reduced density operators are unique [17].

2.3.4 Physical interpretation

It is possible to give a simple physical interpretation [13] to the matrix elements ϱ_{ij} of the density operator ϱ. Indeed let $\{|n\rangle\}_n$ be an orthonormal basis for the state space $\mathcal{H}$, and let ϱ be the density operator for a mixed state in $\mathcal{H}$:

$$\varrho = \sum_k p_k \,|\psi_k\rangle\,\langle\psi_k|$$

Thus:

$$\varrho_{ij} = \sum_k p_k \,\langle i|\psi_k\rangle\,\langle\psi_k|j\rangle$$

The diagonal element ϱ_{ii} is :

$$\varrho_{ii} = \sum_k p_k |\,\langle i|\psi_k\rangle\,|^2$$

The positive real number $|\,\langle i|\psi_k\rangle\,|^2$ is the probability of finding, in a measurement, the system in the state $|i\rangle$ if the system is in the state $|\psi_k\rangle$. Thus, the diagonal element ϱ_{ii} takes into account the indeterminacy of the initial state, so that it represents the average probability to find the system in the state $|i\rangle$, if it is described by ϱ. For this reason ϱ_{ii} is called the *population* of the state $|i\rangle$. The off-diagonal terms ϱ_{ij}, which are referred as *coherence* terms, express the "interference" effect between the states $|i\rangle$ and $|j\rangle$.

2.4 Generalized quantum measurements

Sometimes the measurement process is more complicated as it seems, and may involve the interaction of the quantum system with its surrounding (e.g. if the position of a photon is detected with a silvered screen, which inevitably destroys the photon). Furthermore, every von Neumann measurement is repeatable by definition, while sometimes this is not the case in the real world. Indeed, it could happen that the interaction of the quantum system with the sensing apparatus destroys the states of the particle itself [17]. An accurate modeling of that process may be done by introducing an ancillary system (to model the neighborhood of the quantum system) and a unitary operator which describes the interaction between the two systems. Its immediately clear that such a process describes a new way to intend the measurement, which is more powerful and more general. The general measurement postulate is now given, then its equivalence with the physical argument above is proved afterwards.

Postulate. A quantum measurement is described by a collection $\{\mathcal{M}_m\}$ of operators acting on the state space $\mathcal{H}$ of the system, which satisfy the completeness relation:

$$\sum_m \mathcal{M}_m^\dagger \mathcal{M}_m = I$$

If the state of the quantum system is $|\psi\rangle$, then the probability of the outcome m is:

$$\mathbb{P}(m) = \langle\psi| \mathcal{M}_m^\dagger \mathcal{M}_m |\psi\rangle$$

and the state $|\psi'\rangle$ after the measurement is:

$$|\psi'\rangle = \frac{\mathcal{M}_m |\psi\rangle}{\sqrt{\langle\psi| \mathcal{M}_m^\dagger \mathcal{M}_m |\psi\rangle}}$$

Remark 12. It is easy to see that the von Neumann measurements constitutes a special case of the above postulate. Indeed, the set of operators $\{\mathcal{M}_m\}$ is given by the spectral decomposition of the observable $\mathcal{L}$.

It is important to note that the postulate given here *is not* a new postulate of quantum mechanics. Instead, it gives a more general way to intend quantum measurement, by combining all the Dirac-von Neumann axioms together with the physical interpretation given in the introduction of this section. Indeed, this kind of measurements represent a particular case of quantum operations, that will be presented in Chapter 4.

2.5 Quantum bits

Definition. A *qubit* is a two-state quantum system. The two orthogonal basis states are conventionally written as $|0\rangle$ and $|1\rangle$. The state space is denoted by $\mathcal{Q}$.

The term *qubit* was first introduced by Schumacher, in 1995 [23] and they are now intended to be the base brick upon which build quantum communication systems. However, it is interesting to note that a classical bit can only be either in the 0 state or in the 1 state. Instead, thanks to the superposition principle, a qubit could also be found in a combination of $|0\rangle$ and $|1\rangle$. Indeed, if $|\psi\rangle \in \mathcal{Q}$, then $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, with $\alpha, \beta \in \mathbb{C}$ is a possible state of a qubit. The full description of $|\psi\rangle$, in terms of the coefficients α and β, cannot be given in term of classical bits, because they carry an infinite amount of information. This peculiar property of qubits, although it cannot be used to carry an arbitrary amount of information, turns out to be the key point upon which quantum systems and protocols are built.

2.5.1 Pauli matrices

When dealing with qubits, there is a set of useful operators which are extensively used in the applications. These operators are represented by the Pauli matrices[4]:

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_x = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_y = \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_x = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The importance of the Pauli matrices is given by the following theorem.

Theorem 2.5.1. *Every linear operator $\mathcal{U}$ acting into a two dimensional space $\mathcal{H}$ could be uniquely represented as a linear combination of Pauli matrices:*

$$\mathcal{U} = \sum_{i=0}^{3} \alpha_i \sigma_i \tag{2.14}$$

Proof. The space $\mathcal{H}$ is finite dimensional, thus $\mathcal{U}$ could be uniquely represented by a 2×2 matrix into an arbitrary basis:

$$\mathbf{U} = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$$

[4]It is obviously possible to give the same definition in terms of operators acting on $\mathcal{Q}$.

The equality $\mathbf{U} = \sum_{i=0}^{3} \alpha_i \sigma_i$, gives the following linear system:

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & -i & 0 & 0 \\ 1 & i & 0 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} u_{11} \\ u_{12} \\ u_{21} \\ u_{22} \end{bmatrix}$$

The matrix of coefficients has determinant $4i$, so that by the Rouchè-Capelli Theorem, the system has a unique solution. □

The Pauli matrices are used to define a very interesting class of operator in $\mathcal{Q}$:

Definition (Spin operator [10])**.** A spin operator is an operator in $\mathcal{Q}$ defined as:

$$\sigma_n = \vec{\sigma} \cdot \vec{n} = \sigma_x n_x + \sigma_y n_y + \sigma_z n_z$$

Where $\vec{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is such that $|\vec{n}| = 1$.

It is easy to prove that the spin operator $\vec{\sigma} \cdot \vec{n}$ is a unitary self-adjoint operator in $\mathcal{Q}$ so that it can both represent an evolution operator and a projective measurement for a qubit system $\mathcal{Q}$. The unit vector $\vec{n}$ could be intended as the *direction* of the operator (this physical interpretation turns out to be particularly useful when using the spin operator as a measurement operator).

2.5.2 The Bloch sphere

The state of a qubit has a nice and useful geometrical representation. Let take a generic qubit:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

with $\alpha, \beta \in \mathbb{C}$. The overall phase factor could be ignored, so that:

$$|\psi\rangle = |\alpha| |0\rangle + |\beta| e^{i\varphi} |1\rangle$$

where φ is the phase difference between α and β. The normalization condition $|\alpha|^2 + |\beta|^2 = 1$ is satisfied by any couple of points $|\alpha|, |\beta|$ on the unitary circle in the first quadrant of the Cartesian plane. This suggests to define[5]:

$$|\alpha| = \cos\left(\frac{\vartheta}{2}\right) \quad ; \quad |\beta| = \sin\left(\frac{\vartheta}{2}\right) \quad \vartheta \in [0, \pi]$$

[5]The reason behind the choice of $\vartheta/2$ instead of ϑ is due to the fact that this angle enters in the descriptions of the density matrix, which is a better tool to use in the practice.

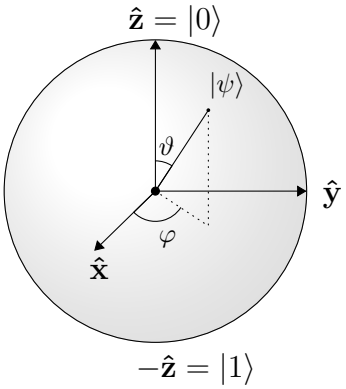

Figure 2.1: Bloch sphere representation of a qubit

so that:

$$|\psi\rangle = \cos\left(\frac{\vartheta}{2}\right)|0\rangle + \sin\left(\frac{\vartheta}{2}\right)e^{i\varphi}|1\rangle = \cos\left(\frac{\vartheta}{2}\right)|0\rangle + (\cos\varphi + i\sin\varphi)\sin\left(\frac{\vartheta}{2}\right)|1\rangle \tag{2.15}$$

With simple algebra, it is possible to find the density matrix of the qubit:

$$\varrho = \frac{1}{2}\begin{bmatrix} 1+\cos(\vartheta) & \sin(\vartheta)e^{i\varphi} \\ \sin(\vartheta)e^{-i\varphi} & 1-\cos(\vartheta) \end{bmatrix} \tag{2.16}$$

Using the Pauli matrices, this could be stated in the more compact form:

$$\varrho = \frac{1}{2}(I + \vec{\sigma}\cdot\vec{n}) \tag{2.17}$$

Where $\vec{n} = (\sin\vartheta\cos\varphi, \sin\vartheta\sin\varphi, \cos\vartheta)$, with $|\vec{n}| = 1$. This means that any pure qubit can be geometrically represented as a unit vector $\vec{n}$ on the unit sphere (Figure 2.1), called *Bloch sphere*.

Remark 13. As already pointed out in the previous section, the unit vector $\vec{n} = (n_x, n_y, n_z)$ which characterizes a spin operator, can be interpreted as the direction of the measurement apparatus. This vector could be intended as a point on the unit sphere by mean of a simple change of coordinates from Cartesian to spherical.

Bloch sphere for mixed states

It is possible to get a generalization of the Bloch sphere that is valid also for mixed states. Indeed, suppose that a generic mixed qubit ϱ is given, then it is represented by the density operator:

$$\varrho = \sum_k p_k \varrho_k$$

Where ϱ_k is a density operator represented by a matrix in the form of (2.16), thus:

$$\varrho_k = \frac{1}{2}\begin{bmatrix} 1+\cos(\vartheta_k) & \sin(\vartheta_k)e^{i\varphi_k} \\ \sin(\vartheta_k)e^{-i\varphi_k} & 1-\cos(\vartheta_k) \end{bmatrix}$$

Using this, the density matrix ϱ becomes:

$$\varrho = \frac{1}{2}\begin{bmatrix} 1+r_z & r_x - ir_y \\ r_x + ir_y & 1-r_z \end{bmatrix} = \frac{1}{2}(I + \vec{\sigma}\cdot\vec{r})$$

Using the implicit declarations:

$$r_x \triangleq \sum_k p_k \sin(\vartheta_k)\cos(\varphi_k) \;\; ; \;\; r_y \triangleq \sum_k p_k \sin(\vartheta_k)\sin(\varphi_k) \;\; ; \;\; r_z \triangleq \sum_k p_k \cos(\vartheta_k)$$

and with simple computations:

$$\mathrm{Tr}\left\{\varrho^2\right\} = \frac{1}{2}(r_x^2 + r_y^2 + r_z^2 + 1)$$

Using the fact that $\mathrm{Tr}\left\{\varrho^2\right\} < 1$ is always verified for mixed states[6], the condition $r_x^2 + r_y^2 + r_z^2 < 1$ is obtained. This proves that a mixed qubit is always represented by a point **inside** the Bloch sphere.

2.5.3 Spin operators

The Bloch sphere gives an interesting representation of a qubit on the unit sphere. However, this characterization turns out to be particularly useful to give a pictorial meaning to quantum operations performed on the qubit space. The following theorems characterize the orientation of a qubit on the bloch sphere as the direction to which turn a measurement apparatus in order to perform a reliable measure on the qubit itself.

Theorem 2.5.2. *For all spin operators σ_n there exists $|\psi_+\rangle, |\psi_-\rangle \in \mathcal{Q}$ such that:*

$$\begin{aligned} \sigma_n |\psi_+\rangle &= \;\; |\psi_+\rangle \\ \sigma_n |\psi_-\rangle &= -|\psi_-\rangle \end{aligned}$$

Proof. It is sufficient to prove that σ_n has two eigenvalues, namely ± 1. The eigenvalues of σ_n could be found by solving the charateristic equation of its matrix representation:

[6] $\mathrm{Tr}\left\{\varrho^2\right\} = 1$ if and only if the state is pure by Theorem 2.3.1

$$|\sigma_n - \lambda I| = \begin{vmatrix} \cos\vartheta - \lambda & \sin\vartheta e^{-i\varphi} \\ \sin\vartheta e^{i\varphi} & -\cos\vartheta - \lambda \end{vmatrix} = -\cos^2\vartheta + \lambda^2 - \sin^2\vartheta = \lambda^2 - 1 = 0$$

This equation has the two solutions: $\lambda = \pm 1$. □

Theorem 2.5.3. *Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a generic qubit.*
Then, there exists a spin operator σ_n such that:

$$\sigma_n|\psi\rangle = |\psi\rangle$$

Proof. To prove this theorem, an explicit form of the eigenvector corresponding to $\lambda = 1$ in Theorem 2.5.2 must be first derived. The eigenvector $|\psi^+\rangle$ has the form:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\left(\frac{\tilde{\vartheta}}{2}\right)|0\rangle + \sin\left(\frac{\tilde{\vartheta}}{2}\right)e^{i\tilde{\varphi}}|0\rangle$$

Note that the angles $\tilde{\vartheta}, \tilde{\varphi}$ are used to avoid confusion with the direction of the spin operator σ_n. The coordinates of $|\psi\rangle$ in the $|0\rangle, |1\rangle$ basis could be found by solving the linear system:

$$[\sigma_n - \lambda I]\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix}\cos\vartheta - 1 & \sin\vartheta e^{-i\varphi} \\ \sin\vartheta e^{i\varphi} & -\cos\vartheta - 1\end{bmatrix}\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix}0 \\ 0\end{bmatrix}$$

Where the first inequality follows from the change of coordinates $\vec{n} = (n_x, n_y, n_z) \to (\sin\vartheta\cos\varphi, \sin\vartheta\sin\varphi, \cos\vartheta)$. This system gives the following:

$$\beta = \alpha e^{i\varphi}\frac{1-\cos\vartheta}{\sin\vartheta} = \alpha e^{i\varphi}\frac{\sin^2\left(\frac{\vartheta}{2}\right)}{\sin\left(\frac{\vartheta}{2}\right)\cos\left(\frac{\vartheta}{2}\right)} = \alpha\tan\left(\frac{\vartheta}{2}\right)e^{i\varphi}$$

Then:

$$\frac{\beta}{\alpha} = \tan\left(\frac{\tilde{\vartheta}}{2}\right)e^{i\tilde{\varphi}} = \tan\left(\frac{\vartheta}{2}\right)e^{i\varphi}$$

It easily follows that it must be $\tilde{\vartheta} = \vartheta$ and $\tilde{\varphi} = \varphi$. In other terms, the eigenvector $|\psi\rangle$ associated with the eigenvalue 1 is a qubit with the same orientation of the apparatus. It should not be surprising that $|\psi^-\rangle$, associated to $\lambda = -1$ is a qubit with opposite orientation: this could be proven with analogue passages. On the other side, given an arbitrary qubit $|\psi\rangle$, it is always possible to define a spin operator σ_n with the same orientation of $|\psi\rangle$ such that $\sigma_n|\psi\rangle = |\psi\rangle$. □

2.5.4 Entangled qubits

Qubits are used to derive a simple example of entangled state. Let suppose to combine two single qubits $\mathcal{Q}_1$, $\mathcal{Q}_2$ into a larger system $\mathcal{Q} = \mathcal{Q}_1 \otimes \mathcal{Q}_2$ (this is commonly called *a pair*). Then, every $|\psi\rangle \in \mathcal{Q}$ could be expressed as:

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

The following states, commonly known as *Bell states*, are fundamental in quantum information and they're crucial in understanding the entanglement phenomenon:

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

The state $|\Psi^-\rangle$ is sometimes referred as the singlet state, and $|\Psi^+\rangle$,$|\Phi^+\rangle$,$|\Phi^-\rangle$ as triplet states [10].

It is easy to prove that these states form a orthonormal basis for $\mathcal{Q}$, they are rotationally invariant, and they are entangled because they cannot be written as product states. Indeed, as an example, suppose that there exists $|a\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle \in \mathcal{Q}_1$, $|b\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle \in \mathcal{Q}_2$, such that

$$|\Psi^-\rangle = |a\rangle \otimes |b\rangle = \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle$$

Because the basis states are orthonormal, it must be $\alpha_1\alpha_2 = 0$, and this implies that $\alpha_1 = 0$ or $\alpha_2 = 0$. However, such a constraint will define a different state than $|\Psi^-\rangle$, leading to a contradiction. This means than $|\Psi^-\rangle$ is not a product state. It should be now clear what is really intriguing with these states: they tell everything there is to know about the composite system, but they tell nothing about the single subsystem. However, there is another interesting aspect which characterize entanglement. If a measurement of σ_z is performed on the first subsystem, this will immediately determine the result of the same measurement σ_z performed on the second subsystem, independently of the distance. This is the so called *spooky action at a distance* and it is one of the most fascinating aspects of entanglement.

These considerations will be deepened in the dedicated chapter.

2.5.5 Qubit operators

There is a set of useful operators when dealing with qubits, that are widely used in applications [17]. Here is a little summary of some of them.

Pauli rotations

As already pointed out in the previous sections, the set of Pauli matrices constitutes a set of valid unitary operation on the space of qubits. Using the Bloch sphere representation, these operators perform a rotation of π radians of the qubit around their respective axes.

Hadamard gate

The Hadamard gate B_z is an operator which performs a rotation of $\pi/2$ radians around the z axis. In plain English, it works as follow in the basis vector $|0\rangle, |1\rangle$:

$$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad ; \quad |1\rangle \to \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

It can be represented by a 2×2 Hadamard matrix:

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Remark 14. It is obviously possible to define other two operators B_x, B_y which perform a rotation of $\pi/2$ radians around the x and the y axis. This set of operators turn out to be particularly useful in the application.

Controlled NOT (CNOT)

The controlled NOT (CNOT) operates on a pair of qubits, the first of which is called *source* and the second one *target*. It can be imagined as a circuit which does a (classical) NOT operation on the target qubit if and only if the control qubit is in the "on" state, e.g. in the state $|1\rangle$. It is thus described as follows:

$$|00\rangle \to |00\rangle \quad ; \quad |01\rangle \to |01\rangle \quad ; \quad |10\rangle \to |11\rangle \quad ; \quad |11\rangle \to |10\rangle$$

Or, equivalently, in the language of operators by:

$$\mathcal{U} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 01|$$

It is sometimes referred as quantum XOR (QXOR), because the input pair $|x\rangle|y\rangle$ is converted into $|x\rangle|x \oplus y\rangle$, where $x \oplus y$ is intended as a classical XOR.

2.6 Important results

There are some interesting results which comes out from the fundamental postulates of quantum mechanics [15, 13, 17]. They have strong consequences both from a theoretical and an applicative point of view.

2.6.1 Uncertainty principle

The Heisenberg uncertainty principle is one of the oldest result in quantum mechanics [15]. It formally states that it is not possible to have, at the same time, a perfect knowledge of two observable quantities which belong to operators that do not commute. Let first remember that if X is a random variable, then its variance, or dispersion, is defined by:

$$\sigma_x^2 = \mathbb{E}[X^2] - \mathbb{E}[X]^2$$

It is possible to determine the variance for operators in quantum mechanics, by applying the same definition and using a different notation:

$$[\Delta\mathcal{M}]^2 = \langle\psi|\,\mathcal{M}^2\,|\psi\rangle - \langle\psi|\,\mathcal{M}\,|\psi\rangle^2$$

Theorem 2.6.1 (Heisenberg)**.** *Let $|\psi\rangle \in \mathcal{H}$. For any two observables $\mathcal{A}$, $\mathcal{B}$:*

$$\Delta\mathcal{A}\Delta\mathcal{B} \geq \frac{1}{2}|\langle\psi|\,[\mathcal{A},\mathcal{B}]\,|\psi\rangle| \tag{2.18}$$

Proof. Given $|\psi\rangle$, let define $\mu_a = \langle\psi|\,\mathcal{A}\,|\psi\rangle$, $\mu_b = \langle\psi|\,\mathcal{B}\,|\psi\rangle$ and the operators:

$$\mathcal{C} = \mathcal{A} - \mu_a \quad ; \quad \mathcal{D} = \mathcal{B} - \mu_b$$

It is trivial to prove that $[\mathcal{C},\mathcal{D}] = [\mathcal{A},\mathcal{B}]$, and $\langle\psi|\,\mathcal{C}^2\,|\psi\rangle = \langle\psi|\,\mathcal{A}^2\,|\psi\rangle - \mu_a^2 = \Delta\mathcal{A}^2$. Analogously, $\langle\psi|\,\mathcal{D}^2\,|\psi\rangle = \Delta\mathcal{B}^2$. By simple calculations it then follows:

$$|\langle\psi|\,[\mathcal{C},\mathcal{D}]\,|\psi\rangle|^2 + |\langle\psi|\,\{\mathcal{C},\mathcal{D}\}\,|\psi\rangle|^2 = 4|\langle\psi|\,\mathcal{C}\mathcal{D}\,|\psi\rangle|^2$$

Then, using the Cauchy-Schwarz inequality it follows that:

$$|\langle\psi|\,[\mathcal{C},\mathcal{D}]\,|\psi\rangle|^2 \leq 4|\langle\psi|\,\mathcal{C}\mathcal{D}\,|\psi\rangle|^2 \leq \left|\langle\psi|\,\mathcal{C}^2\,|\psi\rangle\right|^2\left|\langle\psi|\,\mathcal{D}^2\,|\psi\rangle\right|^2 = \Delta\mathcal{A}^2\Delta\mathcal{B}^2$$

Since $[\mathcal{C},\mathcal{D}] = [\mathcal{A},\mathcal{B}]$ the Heisenberg inequality (2.18) follows immediately. □

2.6.2 No-cloning theorem

One of the most simple result of quantum mechanics is the no-cloning Theorem. Despite its simplicity, it was discovered only in 1982 by Wooters and Zurek [24] and has profound implication in quantum information.

Theorem 2.6.2. *It is not possible to create a copy of an unknown quantum state.*

Proof. Let's suppose that such a system exists. If the state space is the Hilbert space $\mathcal{H}$, it means that there exist a unitary operator $\mathcal{U}$ in $\mathcal{H} \otimes \mathcal{H}$ such that for all source states $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$ it is able to to build a copy of the state, independently from the state $|s\rangle$ of the target system. Thus, $\forall\, |s\rangle \in \mathcal{H}$:

$$\mathcal{U}\big(\, |\psi\rangle \otimes |s\rangle \,\big) = |\psi\rangle \otimes |\psi\rangle$$

$$\mathcal{U}\big(\, |\varphi\rangle \otimes |s\rangle \,\big) = |\varphi\rangle \otimes |\varphi\rangle$$

It follows that:

$$\langle\varphi|\, \langle s|\mathcal{U}^{\dagger}\mathcal{U}\, |\psi\rangle\, |s\rangle = [\langle\varphi|\psi\rangle]^2 = \langle\varphi|\psi\rangle$$

Where the last equality follows from the unitarity of $\mathcal{U}$. However the last relation can hold if and only if $\langle\varphi|\psi\rangle$ is equal to 0 or 1. This means that a *cloning operator* can only work correctly if the input states are orthogonal. Therefore a *general* cloning device can not exist.

□

Chapter 3

Quantum Entanglement

Quantum entanglement is the most controversial and fascinating aspect of quantum mechanics. It's discovery trace back to a famous paper [19] published in 1935 by Einstein, Podolsky and Rosen (EPR), but the term *entanglement* was coined in a second time by Erwin Schrödinger [20, 21]. In the earlier years of quantum mechanics, the nature of the entanglement phenomenon was a source of heated debates between physicists, especially between Niels Bohr and Albert Einstein [25]; however, the arguments were so theoretical and abstract that they were considered to be philosophy and not science. The discovery of the Bell's theorem in 1964 [26], and the subsequent experiments to prove it, have then given an experimental flavor to these discussions, proving that entanglement is a *real* physical phenomenon, that could not be explained in classical terms. The possibility to use quantum entanglement to perform *useful* tasks was discovered only in 1990s. These discoveries boosted up the research on applied quantum physics and very recently has attracted the attention of the IEEE community [27], with the idea to exploit the engineers know-how to design quantum communication systems and get it ready for large-scale implementation. The intrinsic difficulty in understand the physical origin of the entanglement phenomenon can only be circumvented by giving a mathematical description and a formal characterization to it. This chapters gives a formal definition of entanglement and a mathematical description of its properties.

3.1 Einstein's point of view

Before starting a formal discussion, a brief phenomenological description of quantum entanglement is needed. As already pointed out in the historical introduction, entanglement has been a source of famous discussion by physicists with the aim to get a physical explaination of some peculiar aspects of quantum mechanics. The most

famous argument[1] was developed by Einstein together with his colleagues Podolsky and Rosen (EPR) in 1935 [19]. Einstein was aware of the correctness of quantum mechanics, but he was disturbed by some unintuitive, and apparently paradoxical, aspects of quantum mechanics. The main problem was related to the inherent probabilistic nature of quantum mechanics [12]: Einstein was truly convinced that this peculiar behavior is due to the presence of *hidden* parameters, which are not described by quantum mechanics. In other terms, quantum theory is incomplete. The work of 1935 was conceived to mathematically prove this fact, assuming that (i) the property of a physical system are inherent in the system itself, and should thus exist before any measurement is made (realism); and (ii) that no signal can travel faster than light, e.g. the result of a measurement performed at one spatial location cannot istantaneously affect the result of a measurement performed in a remote location (locality). This seems a set of pretty natural *requisites* that a physical theory should satisfy, as they are strongly observed by the *classical* theories of relativity and electromagnetism. The idea behind Einstein's work is the following: let suppose to work with a space composed by a pair of qubits. Thus, $\mathcal{H} = \mathcal{Q}_1 \otimes \mathcal{Q}_2$ where the orthonormal basis of $\mathcal{Q}_i$ is the set $\{|0\rangle, |1\rangle\}$ of eigenvectors of σ_z . As was previously noted, there is an important set of states in $\mathcal{H}$, namely bells states:

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

It is easy to prove that these states form an orthonormal basis in $\mathcal{H}$, say $|\Psi^+\rangle$. Let suppose to prepare a pair of particles in one of these states, the first of which belongs to Alice and the second to Bob. Then, Bob moves away from Alice, let's say 10 light years. If Alice now performs a measurement σ_z on his particle, she will inevitably cause the collapse of the joint state in $|01\rangle$ or $|10\rangle$ with equal probability. Let suppose that she gets the measurement 0, then she instantly knows the result of the Bob's measurement, that is 1. How can it be? How can Alice instantly affect the result of a Bob action that is far away from her? With a little more sophisticated reasoning Einstein came to the conclusion that quantum mechanics is incomplete, in the sense that the result of Alice and Bob measurement is determined *a-priori* by an

[1] The simpler and mostly known version of the paradox presented here, is due to Bohm [28].

hidden parameter, which is not contemplated by quantum mechanics and which was tuned when the particles interacted for the first time. The only tool that could be used to mathematize this uncertainty is statistic. Bohr point of view was completely different: the result of a measurement is *created* during the act of measurement and it is limited only by the statistical distribution of possible results.

3.2 Bell's theorem

The keystone in the Bohr-Einstein debate was a theorem worked out by John Bell in 1964 [26], which is now widely recognized to be one of the most profound result in physics. In its simplest [29] form, it states:

Theorem 3.2.1 (Bell's Theorem)**.** *No physical theory of local hidden variables (LHV) can exactly reproduce all of the predictions of quantum mechanics.*

This theorem confirms that the *quantum* mechanical picture of reality could not be understood using a *classical* reasoning. Stated in this form, the Bell's theorem is a refined version of the Einstein's point of view, and does not tell which view of the reality is the right one: it simply states that any LHV theory will surely have some predictions which are different from the ones of quantum mechanics. It also gives a new insight on the EPR point of view [12]: if Einstein view is right, quantum mechanics is not only incomplete, but also wrong.

However, the main contribution brought by John Bell in his work was the ideation of a physically realizable experiment to *ask the nature* about which view of the reality is effectively correct (Einstenian or Quantum). To do that, Bell derived an experimentally verifiable inequality (now known as Bell's inequality), that if violated would confirm that entanglement is real and not a manifestation of classical correlation. The rest of this section is devoted to explain the Bell's experiment and the inequality to test the LHV hypotesis.

The Bell's experiment

The experiment consists in the preparation of an arbitrary bipartite quantum state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Then, the constituent particles are sent to two spatially separated measurement apparatus, which record, respectively, the results A and B. If the system admits a local hidden-variable model (LHVM), then the result of any measurement on one side is independent from the other[2], and its outcome is uniquely

[2]This is the *locality* assumption, from relativity theory: no signal can travel faster than light.

determined by an *unknown* parameter λ[3]. If $\varrho(\lambda)$ is the probability distribution of λ, then the expectation value of the product of the two components A and B, is:

$$P(A,B) = \mathbb{E}\big\{A(\lambda)B(\lambda)\big\} = \int_\Lambda \varrho(\lambda)A(\lambda)B(\lambda)\,\mathrm{d}\lambda \tag{3.1}$$

With some clever mathematics, Bell derived an inequality that must be satisfied by a set of measurements with different experimental setups. However, the inequality derived by Bell in his preliminary work [26], despite its simplicity, is difficult to be used in practice. The generalization of his inequality that will be given here, was derived by Clauser, Horne, Shimony and Holt (CHSH) [30], and it is now widely recognized as the standard de-facto inequality to test the LHVM hypothesis.

3.2.1 The CHSH inequality

Theorem 3.2.2. *Let $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. If $|\psi\rangle$ admits a LHVM, then:*

$$|S| \leq 2 \tag{3.2}$$

where

$$S = P(A_1,B_1) + P(A_1,B_2) + P(A_2,B_1) - P(A_2,B_2)$$

provided that:

$$|A_i|, |B_i| \leq 1$$

Proof [29]. From the definition (3.1):

$$\begin{aligned} P(A_2,B_1) - P(A_2,B_2) &= \int_\Lambda \big[A_2(\lambda)B_1(\lambda) - A_2(\lambda)B_2(\lambda)\big]\varrho(\lambda)\mathrm{d}\lambda \\ P(A_2,B_1) - P(A_2,B_2) &= \int_\Lambda A_2(\lambda)B_1(\lambda)\big[1 \pm A_1(\lambda)B_2(\lambda)\big]\varrho(\lambda)\mathrm{d}\lambda \\ &\quad - \int_\Lambda A_2(\lambda)B_2(\lambda)\big[1 \pm A_1(\lambda)B_1(\lambda)\big]\varrho(\lambda)\mathrm{d}\lambda \end{aligned}$$

Thanks to the triangle inequality and using the fact that $|A_i|, |B_i| \leq 1$:

$$\begin{aligned} \big|P(A_2,B_1) - P(A_2,B_2)\big| &\leq 2 \pm \int_\Lambda A_1(\lambda)B_1(\lambda)\varrho(\lambda)\mathrm{d}\lambda \pm \int_\Lambda A_1(\lambda)B_2(\lambda)\varrho(\lambda)\mathrm{d}\lambda \\ &\leq 2 \pm \Big[P(A_1,B_1) + P(A_1,B_2)\Big] \\ &\leq 2 - \big|P(A_1,B_1) + P(A_1,B_2)\big| \end{aligned}$$

[3]This is the hidden variable assumption: the result of the experiments depend on some physical parameters which is not determined by the quantum theory, this is why it is referred as hidden.

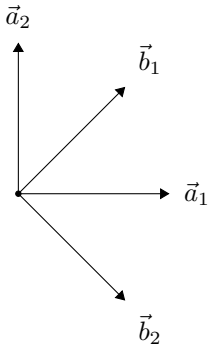

Figure 3.1: Graphical representation of a possible set of vectors which violates the CHSH inequality.

Thus:

$$\big|P(A_2, B_1) - P(A_2, B_2)\big| + \big|P(A_1, B_1) + P(A_1, B_2)\big| \leq 2$$

Using the triangle inequality again leads to the inequality (3.2). □

The postulate of quantum mechanics can be used to give the quantum prediction of the CHSH inequality (3.2). Indeed, the observable quantities A_i, B_i are associated to measurements operator $\mathcal{A}_i, \mathcal{B}_i$ on the Hilbert state spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ of the respective subsystems, so that $P(A_i, B_i) = \langle\psi| \mathcal{A}_i \otimes \mathcal{B}_i |\psi\rangle$. It is thus possible to introduce the CHSH operator:

$$\mathcal{S} = \mathcal{A}_1 \otimes (\mathcal{B}_1 + \mathcal{B}_2) + \mathcal{A}_2 \otimes (\mathcal{B}_1 - \mathcal{B}_2)$$

So that the CHSH inequality becomes:

$$|\langle\psi| \mathcal{S} |\psi\rangle| \leq 2$$

Or equivalently, in the most general form:

$$|\mathrm{Tr}\,\{\mathcal{S}\varrho\}| \leq 2 \tag{3.3}$$

Violating Bell's inequality - An example

A very simple example that violates the CHSH inequality, and thus leads to the formulation of Bell's Theorem is the following. Let suppose to have a pair of qubits in the singlet state:

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

The measurement apparatus is a spin operator $\vec{\sigma} \cdot \vec{n}$, where the direction $\vec{n}$ is a tunable parameter of the experiment. Let suppose to measure the first qubit in the

direction $\vec{a}$ and the second in direction $\vec{b}$; then, according to quantum mechanics, it should be:

$$P(\vec{a},\vec{b}) = \langle\psi| (\sigma_1 \cdot \vec{a})(\sigma_2 \cdot \vec{b}) |\psi\rangle = -\vec{a} \cdot \vec{b}$$

By choosing the apparatuses direction as in Figure 3.1:

$$\vec{a}_1 = \vec{z} \quad ; \quad \vec{a}_2 = \vec{x}$$
$$\vec{b}_1 = \frac{\vec{z}+\vec{x}}{\sqrt{2}} \quad ; \quad \vec{b}_2 = \frac{\vec{z}-\vec{x}}{\sqrt{2}}$$

It follows that quantum mechanics predicts the following value of $|S|$:

$$|S_{QM}| = 2\sqrt{2}$$

While a LHVM, according to (3.2), predicts:

$$|S_L| \leq 2$$

This simple example leads to the formulation of the Bell's theorem. However, it is worth to stress that this is a physically realizable experiment (at least in principle), and as such it can be reproduced inside a laboratory. This allows to turn the Einstein theoretical question into an experimental question and it should be now clear why the Bell's work is considered a milestone in the modern physics.

This simple example is the starting point of different experiments conducted from the '70s to test if entanglement really exists, or if it is only a manifestation of classical correlations, like Einstein predicted. Interestingly, more than fifty years after the publications of Bell's Theorem, the experimental evaluation of Bell's inequalities is still an active research field in scientific community, to try give out all possible loopholes in the experiments, so that an up-to-date list of experiments is hard to find. As the author's knowledge, the most complete and updated list could be found in the work of Brunner et al. [31]. Since all experiments conducted so far confirms the quantum mechanical predictions, entanglement is now widely considered to be a real *spooky* phenomena, despite Einstein's point of view.

3.3 Formal definition

3.3.1 Pure states

Entanglement for pure state is now well understood [32], and the most simple definition can be given in negative terms by first defining product states.

Definition 3.3.1 (Pure state)**.** *Let $|\psi\rangle$ be a pure state in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Then $|\psi\rangle$ is a product state if there exist $|\xi_1\rangle \in \mathcal{H}_1$, $|\xi_2\rangle \in \mathcal{H}_2$ such that:*

$$|\psi\rangle = |\xi_1\rangle \otimes |\xi_2\rangle$$

Sometimes product states are referred as *separable* [32] or *disentangled* [33] states. Pure entangled states could easily be characterized thanks to the following property:

Theorem 3.3.2. *Let $|\psi\rangle$ be a **pure** state in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, with a basis $\{|ij\rangle\}_{ij}$:*

$$|\psi\rangle = \sum_{ij} \mathbf{\Psi}_{ij} |ij\rangle$$

$|\psi\rangle$ is a product state if and only if the matrix of coefficients $\mathbf{\Psi}$ is of rank 1.

Proof. Using the Schmidt decomposition:

$$|\psi\rangle = \sum_{i} \lambda_i |a_i\rangle |b_i\rangle$$

where λ_i are the singular values of $\mathbf{\Psi}$, so that $\text{rank}(\mathbf{\Psi})$ is equal to the number of non-zero singular values. If $\text{rank}(\mathbf{\Psi}) = 1$, there is only one $\lambda_i \neq 0$, then $|\psi\rangle = |a_i\rangle |b_i\rangle$, proving that $|\psi\rangle$ is a product state. Conversely, assuming that $|\psi\rangle$ is a product state, then:

$$|\psi\rangle = \left(\sum_i \alpha_i |i\rangle\right) \otimes \left(\sum_j \beta_j |j\rangle\right) = \sum_{ij} \alpha_i \beta_j |i\rangle |j\rangle$$

In this case $\mathbf{\Psi}_{ij} = \alpha_i \beta_j$. It follows that the columns of $\mathbf{\Psi}$ are all linearly dependent, thus $\text{rank}(\Psi) = 1$. □

3.3.2 Mixed states

The definition of product states in the case of mixed state, is more complicated than in the pure case. The definition has been first proposed by Werner in 1989 [34]:

Definition 3.3.3. *Let ϱ be a density operator into $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Then ϱ represents a separable state if it could be represented as a convex combination:*

$$\varrho = \sum_i p_i \varrho_1^i \otimes \varrho_2^i \tag{3.4}$$

with:

$$\sum_i p_i = 1 \; ; \; p_i \geq 0$$

where ϱ_1^i and ϱ_2^i are density operators on $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively.

The definition of product state in the mixed case is more complicated as it seems. The problem is that there is no known simple characterization of entangled states, as Theorem 3.3.2 does for pure state. Furthermore, a separable decomposition of ϱ may have nothing in common with its eigendecomposition [32]. It turns out that, in general, the decision problem for mixed state is NP-hard [35]. However, there exists different particular cases in which a characterization of mixed entangled states is possible through the so called Positive Partial-Transpose (PPT) condition [32].

Remark 15. The definition of product states (and hence the definition of entangled states), as given in the last sections, involves the composite state space of only two subsystems. For this reason, entanglement in this form is commonly said to be *bipartite*. It is possible to generalize the definitions to an arbitrary number of systems [32], but this generalization leads to further mathematical complications, without involving new physical concepts, so it wont be given here.

The mathematical definition of entangled state, given in negative terms in this section is clean and simple to understand. But there are several question that may arise after the formal definition of entanglement: (i) if a state is given, how is it possible to tell if it is entangled or not?; (ii) is it possible to quantify entanglement? What does it mean that a state is *more* entangled than another?; and (iii) is there a way to get a *positive* definition of entanglement? These questions are at the core of present-day entanglement theory, and are not yet completely solved [32].

3.4 Entanglement manifestations

Even if the definition is given in negative terms, it is possible to observe the effect of entanglement on different quantities with a significant physical meaning.

3.4.1 Bell inequalities

The violation of a Bell inequality is an unambiguous manifestation of a quantum behavior. Indeed, as shown in the previous sections, if a system admits a LHVM (and thus exhibits a *classical* behavior), then it satisfies the CHSH inequality (3.2). A natural question that may arise is if this manifestation could be used as a characterization of the entanglement phenomenon.

To answer this question, it must be first noted that if a state does not violate a particular CHSH inequality, intended as a particular choice of operators A_1, A_2, B_1, B_2 in (3.2), it does not mean that it admits a LHVM. In this sense, it is difficult to say whether a given state violates a particular CHSH inequality or not. Different research efforts were made in 1990s, but a general answer has not been given so far [32]. However, Gisin proved [36] that every pure bipartite non-separable quantum state $|\psi\rangle$ violates some CHSH inequality, e.g. there exist a choice of operators A_1, A_2, B_1, B_2 such that (3.2) is violated by $|\psi\rangle$.

In the case of mixed states the problem is even more complicated. Indeed, in the light of the previous results, one may expect that all separable mixed states, expressed as (3.4), admits a LHV model in analogy to pure states. Surprisingly, Werner showed [34] that there exist separable mixed states which violates the Bell's

inequality. These states are commonly referred as Werner states. As an example let suppose to have the following mixed state of a qubit pair:

$$\varrho = p \left|\psi^-\right\rangle \left\langle\psi^-\right| + (1-p)\frac{I}{2}$$

By definition ϱ is separable. The measurement operators can be chosen to be spin operators with the orientations used in section 3.2. With straightforward calculation it is possible to show that:

$$S_{QM} = p(-2\sqrt{2}) + (1-p)\sqrt{2} = \sqrt{2}[1-3p]$$

If $p \geq \frac{1+\sqrt{2}}{3}$, then $S_{QM} \leq -2$ and the CHSH inequality is violated.

3.4.2 Entropy

In 1935, Schrödinger [20, 21] gave an interesting picture of the entanglement phenomenon, by saying that: "*The best possible knowledge of a whole does not include best possible knowledge of its parts*". Indeed, this peculiar characteristic of quantum mechanics has been highlighted in the previous considerations. However, this pretty abstract definition of entanglement was long unintelligible, as the notion of "knowledge" was not well understood in the quantum context. Inspired by the original work of Shannon [1], Schumacher derived a quantum version of the noiseless coding theorem, in 1995 [23]. Schumacher rediscovered the von Neumann entropy, first defined by von Neumann [16], and proved that it has a significative role in quantum mechanics as Shannon entropy has in classical communication theory.

Definition. The von Neumann entropy S of a quantum state ϱ is defined as:

$$S(\varrho) = -\operatorname{Tr}\{\varrho \ln \varrho\} \tag{3.5}$$

or, equivalently, using the eigendecomposition of ϱ:

$$S(\varrho) = -\sum_i \lambda_i \ln \lambda_i \tag{3.6}$$

It is immediate to see that the von Neumann entropy, as expressed by (3.6) is formally equivalent to the Shannon entropy for a statistical source. It is now well understood that the Shannon entropy is a quantitative measure of information in *classical* information theory. Indeed, roughly speaking, the Shannon noiseless coding theory states that the entropy $H(X)$ of a random source is the minimum number of bits which is necessary to describe the information emitted by the source itself. Schumacher derived [23] an equivalent result for quantum systems, involving the von Neumann entropy, which actually gives a quantum "equivalent" mean of information. Interestingly, this definition of entropy gives an interesting manifestation of entanglement, which formalizes the Schrödinger observation:

Theorem 3.4.1. *Let suppose that ϱ_{AB} is the state of a bipartite quantum system, and let suppose that ϱ_A and ϱ_B are the reduced density operators belonging to the two subsystems. If ϱ_{AB} is entangled then:*

$$S(\varrho_{AB}) \leq S(\varrho_A), S(\varrho_B)$$

To deeply appreciate the difference with the classical notions, note that if X, Y are two random variables, then it is always true that:

$$H(X,Y) \geq H(X), H(Y)$$

In plain english, the Shannon entropy (*information*) of a single random variable is never greater than the entropy of two random variables.

3.4.3 Entanglement measures

When dealing with physical phenomenon of practical utility, it is rather important to assign a numerical value to the quantities which are involved in the physical processes. As it will become clear soon, entanglement is the key process behind the great success of quantum communications. It is thus natural to ask how to quantify entanglement, and maybe mostly important what does it mean that a state is *more entangled* than another. The negative definition of entanglement, as given in section 3.3, does not in any way help to solve this enigma. It turns out that this problem has not a simple solution, as there are different ways to quantify entanglement and the theory is still an active field of research [22, 32].

The first idea to quantify entanglement was connected with its usage as a physical resource in the field of quantum communication systems [37]. It turns out that there exists some *maximally* entangled states (e.g. the singlet state $|\Psi^-\rangle$) which are particularly useful to realize reliable task as quantum teleportation. If a state is not maximally entangled, for example because it has traversed a noisy channel, then no faithful communication can be achieved. As it will be explained in the next section, different processes have been developed to overcome these problems, as the distillation algorithms. Roughly speaking, the idea is to use a set of k impure states to generate a lower number n of purified pairs. Then, an interesting measure of *how strong* entanglement is in a particular quantum state is given by the *purification* ratio n/k that could be achieved using the best possible distillation algorithm. However, it turns out that a formal definition in this terms is very complicated, even from a mathematical point of view [32]. These complications arise when dealing with mixed state, as for pure states a good measure of entanglement, called *entropy of entanglement*, is given by the von Neumann entropy of the single subsystems.

Chapter 4

Quantum Communications

The world of quantum communications is a recent field in applied quantum physics. The main idea is to use the properties and the peculiar effects of quantum mechanics to overcome some intrinsic limit of classical communication systems. Even if some good applications can be achieved using single particles, the most interesting systems relies on the entanglement phenomenon, which involves at least two quantum systems. This chapter gives a comprehensive overview of the most promising applications in the field of quantum communications and of the problems that need to be faced whenever these systems are implemented in practice. Indeed, as in classical systems, all communication channels will be inevitably affected by noise, that degrades the performance of the underlying communication system. This problem is still an active field of research, and some solutions that were proposed in the literature to face the problem will be presented here.

4.1 Theoretical applications

4.1.1 Quantum teleportation

The no-cloning theorem prohibits to copy an unknown quantum state. This is a fundamental result for quantum cryptography, as it limits the possibility for an eavesdropper to act on the communication channel. However, this property seems to be very restrictive and limiting when applied to other communication system. Indeed, let suppose that two parties (Alice and Bob) have no access to a direct quantum communication channels between them, but they can only use a classical communication. In this case, the transmission of an arbitrary *unknown* qubit between the parties is impossible, as the classical communication system will inevitably destroy part of the information. However, it turns out that if Alice and Bob have access to a common source of entangled pairs, they can use local operations and the

classical communication channel to transfer the quantum bit from one place (e.g. Alice) to another (e.g. Bob). The no-cloning theorem prohibits to have a copy of the state, so the transfer process will inevitably destroy the information from the starting place. In analogy of what happens in classical science fiction, this process is called quantum teleportation and it was first proposed by Bennett et al. in 1993 [38]. To see how it works, let suppose that the teleportation is performed from Alice to Bob. Thus, Alice possess a qubit in the unknown state:

$$|\Psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

And the first particle of an entangled qubit pairs (called ancilla), the second of which belongs to Bob, in the singlet state:

$$|\Psi_{23}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Before any interaction, the unknown qubit and the ancilla are uncorrelated, thus they form a product state in $\mathcal{H} = \mathcal{Q}_1 \otimes \mathcal{Q}_2 \otimes \mathcal{Q}_3$:

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_{23}\rangle = \frac{1}{\sqrt{2}}\Big[\alpha\,|001\rangle - \alpha\,|010\rangle + \beta\,|101\rangle - \beta\,|110\rangle\Big]$$

The qubit and the ancilla could be expressed using the Bell operator basis, indeed:

$$|00\rangle = \frac{|\Phi^+\rangle + |\Phi^-\rangle}{\sqrt{2}} \quad ; \quad |01\rangle = \frac{|\Psi^+\rangle + |\Psi^-\rangle}{\sqrt{2}}$$

$$|10\rangle = \frac{|\Psi^+\rangle - |\Psi^-\rangle}{\sqrt{2}} \quad ; \quad |11\rangle = \frac{|\Phi^+\rangle - |\Phi^-\rangle}{\sqrt{2}}$$

Thus:

$$\begin{aligned}|\Psi\rangle =& \frac{1}{2}\Big[\,|\Phi^+\rangle\left(\alpha\,|1\rangle - \beta\,|0\rangle\right) + |\Phi^-\rangle\left(\alpha\,|1\rangle + \beta\,|0\rangle\right) \\ &+ |\Psi^+\rangle\left(\beta\,|1\rangle - \alpha\,|0\rangle\right) - |\Phi^+\rangle\left(\beta\,|1\rangle + \alpha\,|0\rangle\right)\Big]\end{aligned}$$

If a measurement is performed by Alice on the qubit+ancilla system, using the Bell operator basis, the state of the third system can collapse to different states with equal probability:

$$\left|\Phi^+_{12}\right\rangle \to |\Psi_3\rangle = \Big[\alpha\,|1\rangle - \beta\,|0\rangle\Big]$$

$$\left|\Phi^-_{12}\right\rangle \to |\Psi_3\rangle = \Big[\alpha\,|1\rangle + \beta\,|0\rangle\Big]$$

$$\left|\Psi^+_{12}\right\rangle \to |\Psi_3\rangle = \Big[\beta\,|1\rangle - \alpha\,|0\rangle\Big]$$

$$\left|\Psi^-_{12}\right\rangle \to |\Psi_3\rangle = \Big[\beta\,|1\rangle + \alpha\,|0\rangle\Big]$$

Independently from the particular result of the measurement, the information about the original qubit, coded in the coefficients α and β, is completely transferred to Bob. However, to correctly transfer the qubit, a local unitary operator should be performed by Bob in order to get out the correct qubit, in function of the particular results of Alice's measurement. To do so, Bob must be informed of Alice's result through a classical communication, and performs the following operator to his qubit:

$$\left|\Psi_{12}^{-}\right\rangle \rightarrow I$$

$$\left|\Phi_{12}^{-}\right\rangle \rightarrow \sigma_x$$

$$\left|\Psi_{12}^{+}\right\rangle \rightarrow \sigma_z$$

$$\left|\Phi_{12}^{+}\right\rangle \rightarrow \sigma_z\sigma_x$$

Since Bob is not able to reliably recover the original qubit until he gets informed of Alice measurement, the information transfer is not superluminal. It is also worth to note that the original qubit is destroyed, as the measurement inevitably destroys the original state, due to the wavefunction collapse property.

4.1.2 Quantum dense coding

The quantum superdense coding is a simple but surprising technique that can be used to sent two bits of classical information by using only one qubit. It was invented by Bennett and Wiesner in 1992 [39], and it is one of the most elementary application of quantum entanglement. To perform this task, Alice and Bob must first obtain a pair of particles in the singlet state:

$$|\psi_{AB}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Then, Alice applies one of the following operator, depending on the pair of qubits she wants to send Bob:

$$00 : I \quad ; \quad |\psi_{AB}\rangle \rightarrow \left|\Psi^{-}\right\rangle$$

$$01 : \sigma_z \quad ; \quad |\psi_{AB}\rangle \rightarrow \left|\Psi^{+}\right\rangle$$

$$10 : \sigma_x \quad ; \quad |\psi_{AB}\rangle \rightarrow \left|\Phi^{-}\right\rangle$$

$$01 : \sigma_x\sigma_z \quad ; \quad |\psi_{AB}\rangle \rightarrow \left|\Phi^{+}\right\rangle$$

Then, she send her particles to bob, which can now make a complete measurement in the Bell basis to distinguish between the four states. Depending on the result, Bob can reconstruct the pair of qubits coded by Alice.

4.1.3 Quantum key distribution

The security of classical public-key cryptosystems relies on the computational hardness of some algorithms, and are not provably secure from a mathematical point of view. In an ideal situation, with an infinite amount of processing power, and with the capability to intercept the public key exchange between the end users, an evil agent (*eavesdropper*) would be able to intercept and decipher the messages exchanged by the end users, without leaving any trace of his actions. This is a well known problem in modern cryptography and it is considered an Achille's heel for the future of secure communications. The no-cloning theorem, together with the Heisenberg uncertainty principle, turns to be an interesting tool for cryptographic applications, which can overcome the eavesdropper problem. The first quantum key distribution (QKD) protocol was proposed by Bennett and Brassard, in 1984 [40], and it is now commonly referred as BB84, to distinguish it from other protocols.However, it must be noted that QKD protocols provide security only in the case of passive eavesdropping, where the eavesdropper is only able to observe the public channel and cannot act on it. In the case of active eavesdrop, it is not possible to exchange cryptographic keys between two untrusted parties on a public channel, unless they possess some a-priori secret information. Let now proceed to illustrate the BB84 protocol. The exchanged key is in the form of a string of classical bits.

1. Alice generates a random bit $b \in \{0, 1\}$
2. Alice generates a second random bit to decide which *polarization* basis will be used to transmit b. The two basis maps the bit b into different states:

$$\mathrm{H}: \quad 0 \rightarrow |0\rangle \, ; 1 \rightarrow |1\rangle$$

$$\mathrm{D}: \quad 0 \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} ; 1 \rightarrow |1\rangle$$

3. Bob receives the unknown qubit $|\psi\rangle$. He then randomly decides which basis (orientation of the sensing apparatus) use to measure the qubit.
4. Bob reports to Alice which measurement basis he chose, using a classical communication channel. If the two basis coincide, Alice reports a confirmation to Bob which preserves the qubit as a part of the key. Otherwise, the qubit is discarded.

The algorithm is then iterated until Bob has a sufficient amount of bits available. If the qubit sent by Alice remains unperturbed through the quantum channel, the number of qubits discarded by Bob should be one half of the overall qubits sent by Alice. Let suppose now that there is an eavesdropper on the channel (Eve), since

he cannot clone the traveling qubit, by the no-cloning Theorem, he can only try to observe the qubit guessing the polarization basis used by Alice. However, unless he guess Alice's polarization basis, it will inevitably perturb the state of the qubit $|\psi\rangle$. To check for an eavesdropper, Alice and Bob publicly compare a subset of the bits received correctly by Bob. If no eavesdropper is acting on the channel, than all bits should match. There is, however, a non zero probability that Alice and Bob wont detect an eavesdropper. This could happen if Eve guesses the same basis used by Bob, or if Eve misses the right basis and the slim chance makes Bob to measure the same bit sent by Alice. The first event happens with probability 1/2, while the second with probability 1/4. The overall *escape* probability is thus: $p = 3/4$. If k bits are used to check for an eavesdropper, the probability of detection is:

$$P_d = 1 - \left(\frac{3}{4}\right)^k$$

4.1.4 Quantum key distribution using entanglement

The BB84 protocol relies on the no cloning theorem and on the Heisenberg uncertainty principle: entanglement is not used as a resource in this case. The idea to use entanglement in quantum key distribution was worked on by Ekert [41], which proposed a QKD protocol now known as E91. The Ekert protocol for QKD, proposed in 1991, is considered a milestone in quantum information. Indeed, it was the first work to use entanglement as the physical mean to perform a communication task. Since the time of Einstein, the presence of this effect in the quantum theory was considered as a mere curiosity or a source of debates. The surprising applications of quantum entanglement, together with technological advances achieved in the last decades, has definitely consecrated entanglement as a fundamental physical resource for future technologies [32].

The Ekert protocols proceed as follows:

1. Alice, Bob, or a trusted third party prepares a certain amount of pairs of qubit in the singlet state $|\Psi^-\rangle$, and send them to both users.

2. Alice randomly selects one of the following orientations for her measurement apparatus, independently for each qubit:

$$\vec{a_1} = \vec{z} \quad ; \quad \vec{a}_2 = \frac{\vec{z} + \vec{x}}{\sqrt{2}} \quad ; \quad \vec{a_3} = \vec{x}$$

3. Bob randomly selects one of the following orientations for his measurement apparatus, independently for each qubit:

$$\vec{b}_1 = \frac{\vec{z} + \vec{x}}{\sqrt{2}} \quad ; \quad \vec{b_2} = \vec{x} \quad ; \quad \vec{b}_3 = \frac{\vec{z} - \vec{x}}{\sqrt{2}}$$

4. After all measurements, Alice and Bob tell each other the orientations they have chosen for each measurement, using a classical communication channel. Then, they exchange the results obtained for the subset of measurements done with different orientations, to calculate the experimental value of the CHSH inequality (3.2):

$$S = P(\vec{a_1}, \vec{b_1}) + P(\vec{a_1}, \vec{b_3}) + P(\vec{a_3}, \vec{b_1}) - P(\vec{a_3}, \vec{b_3})$$

   Since these orientations are the same used in the example of section 3.2, the predicted value should be $S = -2\sqrt{2}$. If the experimental value is sufficiently near this value, then Alice and Bob can conclude that the qubits were left unobserved. Otherwise, they restart the protocol.

5. After the channel is declared secure, the qubits that were observed in the same direction by both client can be converted into a string of (classical) bits, since they are known to be anticorrelated (e.g. Alice leaves his bit untouched and Bob simply flips it).

Other QKD protocols

The Bennett-Brassard QKD (BB84) and the Ekert QKD (E91) protocols make use of two different aspects of quantum mechanics, in order to provide security at the end users. There exist, of course, other QKD protocols that have been proposed in the literature to overcome some problems of BB84 and E91. However, the two pioneering protocols are considered to be the progenitors of two different categories of QKD algorithms, namely:

- **Prepare-and-measure protocols**: Derived from BB84, these protocols are essentially based on the wavefunction collapse property, which in turn implies that every measurement made on a quantum system inevitably perturbs his state, and on the Heisenberg's uncertainty principle. This property can be exploited to detect an eavesdropper on the channel, which will inevitably perturb the state exchanged by the end parties.

- **Entanglement-based protocols:** In this case, the security of the protocol is possible thanks to the entanglement phenomenon, which is used to link two particles which are sent to the parties. The effect of an eavesdropper on the communication channel is of inevitably destroy the peculiar properties of entangled particles (e.g. the violation of some Bell's inequality).

An interesting and up-to-date review of QKD protocols could be found in [42].

4.2 Quantum operations and quantum channels

It should be now clear the role of quantum mechanics and, in particular, the role of entanglement, in an applicative context. Some effects need still to find a useful field of application, while others are already reality (e.g. QKD). However, these applications require a *noiseless* channel to work flawlessly: all qubits are indeed supposed to travel from one place to another without being perturbed. This is, of course, a distorted view of the reality and no transmission can take place without noise entering the communication, as in classical communication systems. To understand and contrast this phenomenas, a characterization of *quantum* channels is needed.

4.2.1 Deterministic quantum operations

The necessity to characterize quantum channels and the quantum noise is strictly related with a very old question in quantum mechanics, that is how to describe, in the most general way, the evolution of a quantum system when it interacts with its neighboring systems or, in other terms, the theory of open quantum systems. The mathematical formalism developed to explain this phenomenas is now widely known as quantum operation[1]. There are different equivalent approaches to quantum operations [17]. The most intuitive development that will be presented here is due to Hellwig and Kraus [43, 44], but another way to intend quantum operations is to define a set of physically motivated axioms, which turns out to be mathematically equivalent to the first approach [17], so that it won't be reported here.

Let suppose that ϱ is the density operator of a system Q in the Hilbert space $\mathcal{H}$. This system is let free to interact with an ancillary system (e.g. environment) ϱ_E, described in the Hilbert space $\mathcal{H}_E$. Before the interaction, the joint system is described by a product density operator ϱ_{QE} in $\mathcal{H} \otimes \mathcal{H}_E$:

$$\varrho_{QE} = \varrho \otimes \varrho_E$$

The evolution of this system is determined by a unitary operator $\mathcal{U}$ in $\mathcal{H} \otimes \mathcal{H}_E$, that is not necessary a product operator. The state of the system Q after the interaction is given by:

$$\mathcal{E}(\varrho) = \mathrm{Tr}_E \left\{ \mathcal{U}(\varrho \otimes \varrho_E)\mathcal{U}^\dagger \right\} \tag{4.1}$$

The map $\varrho \to \mathcal{E}(\varrho)$ is called *deterministic* quantum operation, and it can be represented using the following property:

[1] A particular case of quantum operation is the framework of generalized measurements, as presented in chapter 2, where a system is free to interact with a surrounding quantum system that reports the measurement to the observer.

Theorem 4.2.1 (Kraus representation [44])**.** *Let ϱ_E be an arbitrary density operator on $\mathcal{H}_E$, with diagonal decomposition $\varrho_E = \sum_j \xi_j |\xi_j\rangle \langle\xi_j|$, and let $|e_j\rangle$ be an arbitrary orthonormal basis of $\mathcal{H}_E$. Then, the deterministic quantum operation:*

$$\mathcal{E}(\varrho) = \mathrm{Tr}_E \left\{ \mathcal{U}(\varrho \otimes \varrho_E)\mathcal{U}^\dagger \right\}$$

has the following representation:

$$\mathcal{E}(\varrho) = \sum_{kj} A_{kj} \varrho A_{kj}^\dagger \tag{4.2}$$

where: $A_{kj} = \sqrt{\xi_j} \langle e_k | \mathcal{U} | \xi_j \rangle$ is an operator on $\mathcal{H}$ and the following property holds:

$$\sum_{kj} A_{kj}^\dagger A_{kj} = I \tag{4.3}$$

Proof. Using the Schmidt decomposition, $\mathcal{U} = \sum_i \lambda_i A_i \otimes B_i$, with $A_i \in \mathcal{H}$ and $B_i \in \mathcal{H}_E$. The partial trace could be computed using the expression (2.13) :

$$\begin{aligned}
\mathcal{E}(\varrho) &= \sum_k \sum_h \xi_h \left\langle e_k \middle| \Big(\sum_i \lambda_i A_i \otimes B_i \Big) \Big(\varrho \otimes |\xi_h\rangle \langle\xi_h| \Big) \Big(\sum_j \lambda_j^* A_j^\dagger \otimes B_j^\dagger \Big) \middle| e_k \right\rangle \\
&= \sum_k \sum_h \xi_h \Big(\sum_i \lambda_i A_i \otimes \langle e_k | B_i \Big) \Big(\varrho \otimes |\xi_h\rangle \langle\xi_h| \Big) \Big(\sum_j \lambda_j^* A_j^\dagger \otimes B_j^\dagger |e_k\rangle \Big) \\
&= \sum_k \sum_h \xi_h \Big(\sum_i \lambda_i A_i \langle e_k | B_i |\xi_h\rangle \Big) \varrho \Big(\sum_j \lambda_j^* A_j^\dagger \langle \xi_h | B_j^\dagger |e_k\rangle \Big) \\
&= \sum_k \sum_h A_{kh} \varrho A_{kh}^\dagger
\end{aligned}$$

Where:

$$A_{kh} = \sqrt{\xi_h} \sum_i \lambda_i A_i \langle e_k | B_i |\xi_h\rangle = \sqrt{\xi_h} \langle e_k | \mathcal{U} |\xi_h\rangle$$

Furthermore, from the unitarity of $\mathcal{U}$, from the fact that $\sum_k \xi_k = 1$, and from the completeness relation $\sum_k |e_k\rangle \langle e_k| = I$, it follows that:

$$\sum_{kh} A_{kh}^\dagger A_{kh} = \sum_{kh} \xi_h \langle \xi_h | \mathcal{U}^\dagger |e_k\rangle \langle e_k | \mathcal{U} |\xi_h\rangle = \sum_h \xi_h = 1$$

Where the last equality follows immediately by noting that $\sum_h \xi_h = \mathrm{Tr}\{\varrho_E\}$, that is equal to one by the properties of the density operator.

□

Remark 16. Some authors [17] prefer a mathematically equivalent but most compact form of equation (4.2), that is obtained by compacting the indexes:

$$\mathcal{E}(\varrho) = \sum_k E_k \varrho E_k^\dagger \tag{4.4}$$

Interestingly, it turns out that the Kraus operator-sum representation offers a complete characterization of deterministic quantum operations. Indeed:

Theorem 4.2.2. *Let ϱ be a density operator in $\mathcal{H}$. Given a set of operators $\{E_k\}_k$ in $\mathcal{H}$, which describe the evolution of the system in the Kraus representation:*

$$\mathcal{E}(\varrho) = \sum_k E_k \varrho E_k^\dagger$$

and obey the trace-preserving relation $\sum_k E_k^\dagger E_k = I$. Then, it is always possible to define an environment system $\mathcal{H}_E$, a pure state ϱ_E in $\mathcal{H}_E$, and a unitary operator $\mathcal{U}$ in $\mathcal{H} \otimes \mathcal{H}_E$ such that:

$$\mathcal{E}(\varrho) = \mathrm{Tr}_E \left\{ \mathcal{U}(\varrho \otimes \varrho_E)\mathcal{U}^\dagger \right\}$$

To prove this Theorem, a simple result is first needed:

Lemma 4.2.3. *Let $\mathcal{U} : W \sqsubset V \to V$ be a linear operator. If:*

$$\langle w_1 | \mathcal{U}^\dagger \mathcal{U} | w_2 \rangle = \langle w_1 | w_2 \rangle \qquad \forall \, |w_1\rangle, |w_2\rangle \in W$$

Then, there exists an extension $\tilde{\mathcal{U}} : V \to V$ of $\mathcal{U}$ which is unitary.

Proof. Let suppose that $\{|w_i\rangle\}_i$ is a basis for W. Then, the assumption on $\mathcal{U}$ implies that $\{|v_i\rangle\}_i$, where $|v_i\rangle = \mathcal{U} |w_i\rangle$, is an orthonormal basis for $\mathrm{Im}(\mathcal{U})$. It is thus possible to extend the two basis such that they span the whole space V. Using that, it is possible to define the extension $\tilde{\mathcal{U}}$ of $\mathcal{U}$ as follows:

$$\tilde{\mathcal{U}} |w_i\rangle = |v_i\rangle$$

Such an extensions preserves the scalar products on V:

$$\langle a | \mathcal{U}^\dagger \mathcal{U} | b \rangle = \left(\sum_i \alpha_i \langle w_i | \right) \left(\sum_j \beta_j |w_j\rangle \right)$$

Thus $\mathcal{U}$ is unitary on V. □

This lemma is due to Nielsen and Chuang [17], who proposed it without proof[2].

[2]The proof proposed here holds only if the space W is finite-dimensional. For a more formal and general proof the interested reader is refered to the work of Peres [45].

Proof of Theorem 4.2.2. Let suppose that $\{E_k\}_k$ is a set of d operators. Then, the environment is defined to be a d-dimensional Hilbert space $\mathcal{H}_d$ with a basis $\{|e_k\rangle\}_k$ on it. If the environment is supposed to be in the state $\varrho_E = |\xi\rangle\langle\xi|$, then, the following operator is defined on a proper linear subset V of $\mathcal{H} \otimes \mathcal{H}_E$:

$$\mathcal{U}|\psi\rangle|\xi\rangle = \sum_k E_k|\psi\rangle|e_k\rangle$$

This operator preserves the inner products on V, indeed:

$$\begin{aligned}\langle\psi|\langle\xi|\mathcal{U}^\dagger\mathcal{U}|\varphi\rangle|\xi\rangle &= \left[\sum_k \langle\psi|\langle e_k|E_k^\dagger\right]\left[\sum_j E_j|\varphi\rangle|e_j\rangle\right] = \sum_{kj}\langle\psi|\langle e_k|E_k^\dagger E_j|\varphi\rangle|e_j\rangle \\ &= \sum_k \langle\psi|E_k^\dagger E_k|\varphi\rangle\langle e_k|e_k\rangle = \langle\psi|\varphi\rangle\end{aligned}$$

Where the last equality follows from the trace-preserving relation. Thus, by Lemma 4.2.3, $\mathcal{U}$ could be extended to a unitary operator on the whole space $\mathcal{H} \otimes \mathcal{H}_E$. Furthermore, let $\varrho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, then:

$$\mathcal{U}(\varrho \otimes |\xi\rangle\langle\xi|)\mathcal{U}^\dagger = \sum_{ikj} p_i E_k|\psi_i\rangle|e_k\rangle\langle\psi_i|\langle e_j|E_j^\dagger = \sum_{ikj} p_i E_k|\psi_i\rangle\langle\psi_i|E_j^\dagger \otimes |e_k\rangle\langle e_j|$$

So that:

$$\mathrm{Tr}_E\left\{\mathcal{U}(\varrho \otimes |\xi\rangle\langle\xi|)\mathcal{U}^\dagger\right\} = \sum_{ikj} p_i E_k|\psi_i\rangle\langle\psi_i|E_j^\dagger\delta_{kj} = \sum_k E_k\varrho E_k^\dagger = \mathcal{E}(\varrho)$$

□

Remark 17. The proof of this theorems gives also an interesting theoretical insight in quantum operations: indeed, with loss of generality, the environment system could also be considered to be in a pure state.

4.2.2 Physical interpretation of deterministic operations

There is another interesting physical interpretation that can be given to the Kraus operator sum-representation [17]. Let suppose to do a measurement $\mathcal{A}$ of the environment after the whole system has evolved through the unitary operator $\mathcal{U}$. If the eigenvectors $|e_i\rangle$ are used as an orthonormal basis for $\mathcal{H}_E$, then the state of the principal system, given the result m, is:

$$\varrho_m = \frac{\mathrm{Tr}_E\left\{\mathcal{P}_m\mathcal{U}(\varrho \otimes \varrho_E)\mathcal{U}^\dagger\mathcal{P}_m^\dagger\right\}}{p_m}$$

with probability:

$$p_m = \mathrm{Tr}\left\{\mathcal{P}_m\mathcal{U}(\varrho \otimes \varrho_E)\mathcal{U}^\dagger\mathcal{P}_m^\dagger\right\}$$

Without loss of generality, it could be assumed that the eigenvalue λ_m is non degenerate, so that $\mathcal{P}_m = |e_m\rangle \langle e_m|$. Thus:

$$\begin{aligned}\varrho_m &= \frac{1}{p_m} \mathrm{Tr}_E \left\{ |e_m\rangle \langle e_m| \mathcal{U}(\varrho \otimes \varrho_E) \mathcal{U}^\dagger |e_m\rangle \langle e_m| \right\} \\ &= \frac{1}{p_m} \sum_k \langle e_k| \left(|e_m\rangle \langle e_m| \mathcal{U}(\varrho \otimes \varrho_E) \mathcal{U}^\dagger |e_m\rangle \langle e_m| \right) |e_k\rangle \\ &= \frac{1}{p_m} \langle e_m| \mathcal{U}(\varrho \otimes \varrho_E) \mathcal{U}^\dagger |e_m\rangle = \frac{1}{p_m} E_m \varrho E_m^\dagger\end{aligned}$$

with:

$$p_m = \mathrm{Tr}_Q \left\{ \mathrm{Tr}_E \left\{ |e_m\rangle \langle e_m| \mathcal{U}(\varrho \otimes \varrho_E) \mathcal{U}^\dagger |e_m\rangle \langle e_m| \right\} \right\} = \mathrm{Tr} \left\{ E_m \varrho E_m^\dagger \right\}$$

If the outcome of the measurement is not known to the experimenter (or not directly under his control), then the state after the measurement is the following mixed state:

$$\varrho' = \sum_k p_k \varrho_k = \sum_k E_k \varrho E_k^\dagger = \mathcal{E}(\varrho) \tag{4.5}$$

This is equivalent to say that the principal system is into a mixture of states ϱ_k due to the fact that someone performed a measurement on E without informing the user about the result, and this is formally indistinguishable from a deterministic quantum operation. In other terms, a deterministic quantum operation describes a general time evolution of the density operator if a measurement is not made or its outcomes are ignored [46].

4.2.3 General quantum operations

Most of the interesting operations, as quantum channels, can be thought to be deterministic, as discussed above. However it is worth to note that deterministic operations does not comprehend all possible actions that could be performed on a quantum system. Indeed, as it should be now clear, deterministic operations allows a system to *interact* with an environment, but no *selective* measurements are allowed. This means that a measurement is not performed at all or, equivalently, the outcomes are completely ignored, or unknown, to the experimenter. This is, of course, a strong a strong assumption. For this reason, this category of quantum operations are called *deterministic*.

Let then suppose to have a system Q in the state ϱ, which is free to interact with an environment in the state ϱ_E, as in section 4.2.1. However, in this case, a projective measurement $\mathcal{P}_m$ is allowed on the environment. The state of the system Q after that interaction becomes:

$$\varrho' = \frac{\mathrm{Tr}_E \left\{ \mathcal{P}_m \mathcal{U}(\varrho \otimes \varrho_E) \mathcal{U}^\dagger \mathcal{P}_m^\dagger \right\}}{\mathrm{Tr} \left\{ \mathcal{P}_m \mathcal{U}(\varrho \otimes \varrho_E) \mathcal{U}^\dagger \mathcal{P}_m^\dagger \right\}}$$

To avoid cumbersome notations and for reason that will become clear soon, it is more convenient to work with the unnormalized state:

$$\mathcal{E}(\varrho) = \mathrm{Tr}_E \left\{ \mathcal{P}_m \mathcal{U} (\varrho \otimes \varrho_E) \mathcal{U}^\dagger \mathcal{P}_m^\dagger \right\} \tag{4.6}$$

This is the generalization[3] of the deterministic quantum operation formalism (4.1), which preserves the same form. The following generalization of Theorem 4.2.1 holds:

Theorem 4.2.4 (Kraus representation [43, 44])**.** *Let ϱ_E be an arbitrary density operator on $\mathcal{H}_E$, with diagonal decomposition $\varrho_E = \sum_j \xi_j |\xi_j\rangle \langle \xi_j|$, and let $|e_j\rangle$ be an arbitrary orthonormal basis of $\mathcal{H}_E$. Then, the generalized quantum operation:*

$$\mathcal{E}(\varrho) = \mathrm{Tr}_E \left\{ \mathcal{P}_m \mathcal{U} (\varrho \otimes \varrho_E) \mathcal{U}^\dagger \mathcal{P}_m^\dagger \right\}$$

has the following representation:

$$\mathcal{E}(\varrho) = \sum_{kj} A_{kj} \varrho A_{kj}^\dagger$$

where: $A_{kj} = \sqrt{\xi_j} \langle e_k | \mathcal{P}_m \mathcal{U} | \xi_j \rangle$ is an operator on $\mathcal{H}$. In this case:

$$0 \leq \sum_{kj} A_{kj}^\dagger A_{kj} \leq I$$

Proof. The proof is formally equivalent to the one of Theorem 4.2.1, by using the Schmidt decomposition of the operator $\mathcal{X} = \mathcal{P}_m \mathcal{U}$. However, in this case, $\mathcal{X}^\dagger \mathcal{X} \leq I$, because of the operator $\mathcal{P}_m$, that is not supposed to be unitary. □

Remark 18. The operator inequality $\mathcal{U} \leq 1$ should be intended in the trace norm [22, 47], e.g. $\mathcal{U} \leq 1 \leftrightarrow \|\mathcal{U}\| \leq 1$. Thus, unless $\mathcal{P}_m = I$, a generalized quantum operation is a trace-decreasing operator.

In analogy with quantum operations, given a general quantum operation $\mathcal{E}(\varrho)$ it is always possible to find a reasonable physical model to (4.6). This is nothing else a generalization of Theorem (4.2.2):

Theorem 4.2.5 ([44])**.** *Let ϱ be a density operator in $\mathcal{H}$. Given a set of operators E_k, which describes the evolution of the system in the operator-sum representation:*

$$\mathcal{E}(\varrho) = \sum_k E_k \varrho E_k^\dagger$$

such that $0 \leq \sum_k E_k^\dagger E_k \leq I$. Then it is always possible to define an environment system $\mathcal{H}_E$, a unitary operator $\mathcal{U}$ in $\mathcal{H} \otimes \mathcal{H}_E$, and a projection operator $\mathcal{P}_m$ in $\mathcal{H}_E$, such that:

$$\mathcal{E}(\varrho) = \mathrm{Tr}_E \left\{ \mathcal{P}_m \mathcal{U} (\varrho \otimes \varrho_E) \mathcal{U}^\dagger \mathcal{P}_m^\dagger \right\}$$

[3] If $\mathcal{P}_m = I$, a deterministic operation is obtained.

Proof. If the set of operators $\{E_k\}_{k\geq 1}$ satisfies the hypothesis, then the following operator is always well-defined:

$$E_0 = \left[I - \sum_{k\geq 1} E_k^\dagger E_k \right]^{1/2}$$

So that:

$$\sum_{k\geq 0} E_k^\dagger E_k = I$$

Let suppose that the environment is a $(d+1)$-dimensional Hilbert space, where d is the number of operators in the Kraus decomposition, and let $\{|e_k\rangle\}_{k=0}^d$ be an orthonormal basis for it. Then, supposing that it is in the pure state $\varrho_E = |\xi\rangle\langle\xi|$, the following operator can be defined:

$$\mathcal{U}|\psi\rangle|\xi\rangle = \sum_{k\geq 0} E_k|\psi\rangle|e_k\rangle$$

Using the same arguments as in the proof of Theorem 4.2.1, the operator $\mathcal{U}$ could be extended to a unitary operator in $\mathcal{H}\otimes\mathcal{H}_E$. Equivalently, it turns out that:

$$\mathrm{Tr}_E\left\{\mathcal{U}(\varrho\otimes\varrho_E)\mathcal{U}^\dagger\right\} = \sum_{k\geq 0} E_k\varrho E_k^\dagger$$

However, since this decomposition comprehends the dummy operator E_0, that is not present in $\mathcal{E}(\varrho)$, the following projector must be defined:

$$\mathcal{P}_m = \sum_{j\geq 1} |e_j\rangle\langle e_j|$$

and it is straightforward to verify that:

$$\mathrm{Tr}_E\left\{\mathcal{P}_m\mathcal{U}(\varrho\otimes\varrho_E)\mathcal{U}^\dagger\mathcal{P}_m^\dagger\right\} = \sum_{k\geq 1} E_k\varrho E_k^\dagger = \mathcal{E}(\varrho)$$

□

4.2.4 Quantum channels

The formalism of quantum operations is a very useful tool to model the effect of the noise on quantum states. All quantum channels can be described by deterministic operations [17]. In this section, the most simple models are described and discussed.

The bit-flip channel

The physical interpretation of deterministic operations, as given in the previous section, could be better understood by the mean of an example, which is also an example of quantum channel. Let suppose that an unknown qubit described by ϱ passes through a channel which flips it (e.g. it performs the unitary operation σ_x) randomly with probability $1-p$, otherwise it leaves the qubit untouched. That is:

$$\varrho \xrightarrow{p} \varrho' = \varrho \qquad ; \qquad \varrho \xrightarrow{(1-p)} \varrho' = \sigma_x \varrho \sigma_x^\dagger$$

This behavior could be adducted to a two-state channel which introduces a noise in the system whenever it is on a "high" state. In some sense, this channel is the quantum equivalent of the binary simmetric channel (BSC) in classical communication theory.Using the physical interpretation of deterministic operations (4.5), the mixed state at the channel end is described by:

$$\mathcal{E}(\varrho) = (1-p)\sigma_x \varrho \sigma_x^\dagger + p\varrho$$

To write this equation in the Kraus representation form (4.4), a natural selection of operators E_0 and E_1 is the following:

$$E_0 = \sqrt{p} I$$

$$E_1 = \sqrt{1-p}\sigma_x$$

Or, equivalently, using the matrix representation:

$$\mathbf{E_0} = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad ; \quad \mathbf{E_1} = \sqrt{1-p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.7}$$

The phase-damping channel

Another simple channel, strictly related to the previous example, is the phase-damping (PD) channel. The physical interpretation is analogue to the bit-flip channel: if a qubit ϱ is sent, then with probability $1-p$ a phase-flip operator (σ_z) is applied, otherwise the qubit is left untouched. Thus:

$$\mathcal{E}(\varrho) = (1-p)\sigma_z \varrho \sigma_z^\dagger + p\varrho$$

Using the matrix representation:

$$\mathbf{E_0} = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad ; \quad \mathbf{E_1} = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{4.8}$$

The phase-damping channel is important because it gives a simple mathematical model to a typical effect of quantum mechanics: the decoherence phenomenon [48]. This phenomenon could be used to explain the so called *emergence of classicality*, that is, the classical behavior of complex quantum systems. Indeed, the predictions of quantum mechanics are undoubtedly right, however, their controversial aspects come out from the fact that it is not possible to observe such a quantum behavior on macroscopic systems [4]. Let suppose to have a generic qubit density matrix:

$$\mathbf{R} = \begin{bmatrix} \varrho_{11} & \varrho_{12} \\ \varrho_{21} & \varrho_{22} \end{bmatrix}$$

Then, by applying the Kraus operators, as defined in (4.8), the qubit becomes:

$$\mathbf{R}_1 = \begin{bmatrix} \varrho_{11} & (2p-1)\varrho_{12} \\ (2p-1)\varrho_{21} & \varrho_{22} \end{bmatrix}$$

If the same qubit traverses an arbitrary number n of phase-damping channels, then it becomes:

$$\mathbf{R}_n = \begin{bmatrix} \varrho_{11} & (2p-1)^n\varrho_{12} \\ (2p-1)^n\varrho_{21} & \varrho_{22} \end{bmatrix}$$

Let now suppose that the same qubit traverses a concatenation of infinitesimal PD channels, each of which introduce a perturbation of the state with parameter p. Let divide the time line into slices of equal amplitude δ so that, if the qubits needs t seconds to travel across the channel, it will traverse a number $n = t/\delta$ of PD channels. The phase-flip event occurs then with probability $1 - p = \Gamma\delta$, where Γ is the probability of the phase-flip event per unit time. If $\delta \to 0$, then:

$$(2p-1)^n = (1-2\Gamma\delta)^{t/\delta} \xrightarrow{\delta\to 0} e^{-2\Gamma t}$$

The evolution of a qubit that is subject to the decoherence phenomenon is thus coded by the evolution of its density matrix:

$$\mathbf{R}(t) = \begin{bmatrix} \varrho_{11} & e^{-2\Gamma t}\varrho_{12} \\ e^{-2\Gamma t}\varrho_{21} & \varrho_{22} \end{bmatrix}$$

As $t \to \infty$ (in practice $t \gg \Gamma^{-1}$), the decoherence transforms *every* state in the diagonal product state $\varrho = \varrho_{11}\left|0\right\rangle\left\langle 0\right| + \varrho_{22}\left|1\right\rangle\left\langle 1\right|$. In other terms, the decoherence phenomenon inevitably destroys entanglement. This little results can be used as a starting point to explain the emergence of classicality in macroscopic systems [4].

4.2.5 Local operations and classical communications

The theory of quantum operations is useful to describe the effect of a set of operation voluntarily applied to a quantum system. This turns out to be a very

powerful instrument when dealing with the constituent particles of an entangled system. Indeed, as it should be now clear, entanglement can not be used to perform superluminal communications, as the measurement of a particle does not affect the marginal statistic of the other. However, to perform different useful task, a classical communication channel could be used to support the desired application.

The idea to use local operations and classical communication (LOCC) trace back to the pioneering work on distillation algorithms [37], and then formalized in a subsequent work [49]. In this paradigm, two remote parties can act on their particles, performing only local quantum operations, with the help of a classical communication channel, supposed to be free from noise. This is well coded by the formalism of generalized quantum operations, that are maps of the form:

$$\varrho \to \frac{\mathcal{E}(\varrho)}{\mathrm{Tr}\left\{\mathcal{E}(\varrho)\right\}}$$

Where $\mathcal{E}(\varrho)$ has the following representation:

$$\mathcal{E}(\varrho) = \sum_k E_k \varrho E_k^\dagger$$

with $\mathrm{Tr}\left\{\mathcal{E}(\varrho)\right\} = 1$ if the map deterministic. Here, and in the following, it is assumed that ϱ is the density matrix of a bipartite quantum state in $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ represent, respectively, the state space of the particle which belongs to Alice and Bob. There are different classes [32, 33] of LOCCs, depending on the allowable operations permitted to clients:

- **local operations (LOs):** In this case, no classical communication is permitted between Alice and Bob. As they cannot tell the result of a measurement to the other, only deterministic quantum operations are permitted. Furthermore, since this operations are performed locally, the quantum operation should be a product operator:

  $$\mathcal{E} = \mathcal{E}_A \otimes \mathcal{E}_B$$

  Where $\mathcal{E}_A$ and $\mathcal{E}_B$ are deterministic quantum operation on, respectively, $\mathcal{H}_A$ and $\mathcal{H}_B$. This means [33] that there exist, respectively, two sets of operators on $\mathcal{H}_A, \mathcal{H}_B$ satisfying $\sum_i A_i^\dagger A_i = I$, $\sum_j B_i^\dagger B_i = I$, such that the joint action is described by the operator:

  $$\mathcal{M} = \sum_{ij} A_i \otimes B_j$$

  It is worth to note that this is equivalent [33] to say that Alice and Bob both perform a local generalized measurement (LGM), which comprise the case of a local unitary transformation.

- **One-way LOCC:** In this case, a classical communication is permitted only in one direction (from Alice to Bob, or viceversa). Let suppose, without loss of generality, that the allowed classical communication is from Alice to Bob (*forward*). In this particular case Alice is thus allowed to perform an arbitrary general quantum operation, while Bob is constrained to perform only deterministic operations because, otherwise, he won't be able to tell the result of his measurement to Alice. The form of the operation is thus:

$$\mathcal{E}^{\rightarrow}_{AB}(\varrho) = \sum_k A_k \otimes I \left[I \otimes \mathcal{E}^i_B \right] (\varrho) A^\dagger_k \otimes I$$

  Viceversa, in the opposite direction:

$$\mathcal{E}^{\leftarrow}_{AB}(\varrho) = \sum_k I \otimes B_k \left[\mathcal{E}^i_A \otimes I \right] (\varrho) I \otimes B^\dagger_k$$

- **Two-way LOCC:** In this case a bilateral communication is permitted between the two clients. However it turns out that a characterization of this operation is inherently hard [32, 50], simply because the parties can perform an arbitrary number of deterministic and random operations, using a proper exchange of messages. Fortunately there exist a larger [46, Sec. IIB] class of operations which has a simpler characterization and that could be used to derive performance bounds on algorithms that make use of two-way LOCCs.

- **Separable operations:** This class of operation was first introduced by Vedral and Plenio [33] as the theoretical background for the axiomatic definition of entanglement measures. In this case, the operation elements are described by product operators, e.g. $E_k = A_k \otimes B_k$. The Kraus representation of the operation is thus given by:

$$\sum_k A_k \otimes B_k \varrho A^\dagger_k \otimes B^\dagger_k$$

  It has been proved by Bennett et al. [46] that every two-way LOCC is a separable operation, but there exists separable operations that cannot be implemented using two-way LOCC.

4.2.6 Fidelity

When dealing with noisy communication channels it is necessary to quantify the effect of the noise on the transmitted signal. In classical communication channels [51], there exist different parameters that could be used for this purpose, e.g. the Hamming distance in discrete channels or the ℓ_2 norm in continuous channels. Formally

speaking, all these quantities are metrics on the signal space. There exists different distance measures that can be introduced in quantum information [17]. The most used in the field of quantum information is the fidelity, first introduced by Schumacher [23]. He used the following reasoning: let suppose that the original signal is a pure state $|\psi\rangle$ in the state $\mathcal{H}$, represented by the density operator $\varrho = |\psi\rangle\langle\psi|$. The effect of a generic quantum channel is to map the original state ϱ into the mixed state $\breve{\varrho}$. To check how close the output state is to the original one, a *validation measurement* can be performed on $\breve{\varrho}$, using the projection operator $|\psi\rangle\langle\psi| = \varrho$. This measurements has two possible outcomes: 1 if and only if the state $\breve{\varrho}$ is equal to ϱ, 0 otherwise (this also implies that $\breve{\varrho}$ is orthogonal to ϱ). The probability that $\breve{\varrho}$ passes the validation test (e.g. the result of the measurement is 1) is called *fidelity*, and it can be calculated using the postulates of quantum mechanics:

$$\mathcal{F}(\breve{\varrho}, \varrho) = \mathrm{Tr}\{\varrho\breve{\varrho}\} = \langle\psi|\,\breve{\varrho}\,|\psi\rangle \tag{4.9}$$

The fidelity F is obviously defined between 0 and 1, and it is equal to one if and only if $\breve{\varrho} = \varrho$. The definition could be clearly generalized to the case that ϱ is a mixed state (intended as an unknown *pure* state emitted by a stochastic source [23]). In this case, the fidelity is equal to the overall probability that an arbitrary signal from the source which traverses a noisy channel passes a validation test when compared to the original. Let suppose that the state ϱ_k is emitted with probability p_k by the source, then, by using the above definition and the law of total probability:

$$F = \sum_k p_k F(\breve{\varrho}_k, \varrho_k) = \sum_k p_k \,\mathrm{Tr}\{\breve{\varrho}_k\varrho_k\}$$

These considerations were later generalized by Jozsa [52], who gave a definition of fidelity for mixed states. Since this is not useful for the purposes of this Thesis, it won't be given here.

4.3 Entanglement distillation

The interaction of a quantum state with the environment inevitably perturbs the structure of the state itself. To protect the quantum state from this degradation, different strategies have been developed. In analogy with classical communication systems, quantum error-correcting codes (QECCs) can be used to a-priori protect quantum states from degradation. QECCs were initially proposed by Shor [53], and they constitutes an active field of research in the field of theoretical quantum information, but they won't be treated here. There is an alternative approach to achieve the same result of QECCs, using an a-posteriori procedure to *purify*

noisy states. This kind of protocols have no analogue in classical communication systems and are commonly referred as entanglement purification protocols (EPPs) or quantum entanglement distillation (QED) algorithms. They were originally invented by Bennett et al. in 1996 [37], who proposed two influential algorithms, now known as the recurrence algorithm and the asymptotic algorithm. The term *distillation* comes out from the fact that these algorithms requires an high amount of impure entangled states to purify a single (near-)pure state, as it analogously happens in classical chemical distillation processes. For this reason, the performance of QED algorithms are quantified with the yield of the algorithm itself, intended as the ratio between the number of output purified pairs with respect to the number of input impure pairs.

4.3.1 Bennett recurrence algorithm

The Bennett recurrence algorithm was first proposed in the pioneering work on QED [37]. The objective of the algorithm is to *distillate* the singlet state $|\psi^-\rangle$ from a set of noisy pairs. To accomplish the task, this algorithm performs LOCC on two pairs of qubits and purifies one of the pairs at the expense of the other. This procedure is applied to a pool of noisy pairs, and repeated recursively until a target fidelity is achieved, or until there are sufficient pairs available. The term *distillation* comes out from the fact that a certain amount of pairs must be sacrificed in order to produce pairs of qubits sufficiently purified. The performance of these protocols are thus evaluated in term of the yield, e.g. the ratio between the number of purified pairs with respect to the number of initial noisy pairs. To see how it works, let suppose to send the singlet state through a noisy channel, so that the received state is:

$$\varrho = F \left|\Psi^-\right\rangle \left\langle\Psi^-\right| + p_1 \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + p_2 \left|\Phi^-\right\rangle \left\langle\Phi^-\right| + p_3 \left|\Phi^+\right\rangle \left\langle\Phi^+\right|$$

The notation is chosen such that the fidelity $\mathcal{F}(\varrho) = F$. As already pointed out, the algorithm works on two independent pairs of qubits at a time ϱ_1, ϱ_2, and thus the working space is $\mathcal{Q} = \mathcal{Q}_1 \otimes \mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$. The first and the third qubits are hold by the first client (Alice) and the other ones by the second client (Bob). The algorithm proceed recursively, so that, at the k-th steps, the following actions are performed:

1. A random bilateral rotation (B_x, B_y, B_z) is performed, independently, on each pair. Each of these operations leaves the singlet state and a different triplet untouched, interchanging the remaining triplets, with the following rules:

   $$B_x : \left|\Psi^+\right\rangle \leftrightarrow \left|\Phi^+\right\rangle \quad ; \quad B_y : \left|\Phi^-\right\rangle \leftrightarrow \left|\Psi^+\right\rangle \quad ; \quad B_z : \left|\Phi^-\right\rangle \leftrightarrow \left|\Phi^+\right\rangle$$

   A random bilateral rotation is performed by applying a $\pi/2$ rotation of each qubit in the pair around the specific axis.

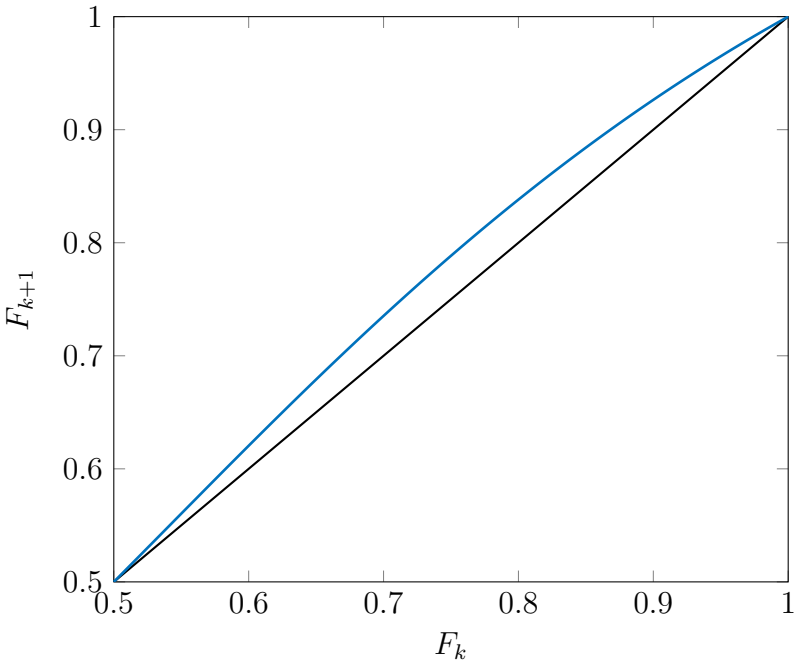

Figure 4.1: Fidelity improvement by a single round of Bennett's algorithm (blue) and its relationship with the bisecting line (black).

2. The operator σ_y is applied in the first qubit of both pairs.

3. Alice and Bob applies CNOT operators to the qubit pairs $(1, 3)$ and $(2, 4)$. This operation is called bilateral XOR (BXOR) [37].

4. A measurement σ_z is performed by Alice and Bob on the target qubit pair. The two measurements are performed locally by Alice and Bob, which than exchange and compare their observation. If the results match, the source pair is given; otherwise, it is discarded. Because the measurements collapses the state of the target pair, this is always discarded.

5. If the source pair has been kept, the operator σ_y is again applied by Alice to the first qubit.

After these operations, the fidelity of the preserved pairs, is given by:

$$F_{k+1} = \frac{F_k^2 + \frac{1}{9}(1 - F_k)^2}{F_k^2 + \frac{2}{3}F_k(1 - F_k) + \frac{5}{9}(1 - F_k)^2} \tag{4.10}$$

And the yield is:

$$Y_{k+1} = \frac{1}{2}\left[F_k^2 + \frac{2}{3}F_k(1 - F_k) + \frac{5}{9}(1 - F_k)^2\right] Y_k \tag{4.11}$$

Where $F_0 = F$ is the initial fidelity and $Y_0 = 1$. By solving these recurrence relation, it is possible to get the theoretical yield and fidelity after k rounds of the algorithm. The solution is far to be trivial, however some preliminary considerations may be done: (i) because F_{k+1} is a strictly convex function of F_k in the interval $(1/2, 1)$ then, if $F_0 > 1/2$, the algorithm is able to distillate a singlet pair with an arbitrary high purity $F < 1$, with a number of distillation rounds proportional to the desired purity; (ii) the convergence speed is very low. This could be noted by observing the Figure 4.1: the relation (4.10) is very close to the bisecting line; and (iii) Since $Y_{k+1} < Y_k$ the yield is a monotonic decreasing function in k, so the yield goes to 0 as $k \to \infty$. This consideration, combined with the previous, leads to observe that there is a strong compromise between the desired fidelity and the overall efficiency of the algorithm. This turns out to be a general problem of recurrence algorithms. Since the resolution of these equation is not trivial, the plot of this quantities can be demanded to a computer. It is possible to observe the evolution of the fidelity and the yield, with $F_0 = 0.6$, in Figures 4.2 and 4.3.

On the other side, it may also be interesting to know the fidelity and the yield of the algorithm after a fixed number of distillation rounds. This turns out to be particularly useful from an applicative point of view, since it allows to place a lower bound on the number of discarded pairs. This constraint obviously pays the price of a lower fidelity of the output pair. These considerations could be made in the light of Figures 4.4 and 4.5, where the fidelity and the yield of the algorithm in function of the initial fidelity are given after 10 rounds of distillation.

Remark. The algorithm is not deterministic: the fidelity of the singlet state after an iteration of the algorithm, as given by equation (4.10), should be intended as a mean value, due to the fact that the Werner state (4.12) is obtained through a classical *random* bilateral rotation.

Proof of equation (4.10)

Let first note that the random bilateral rotation gives the following mixed state:

$$\varrho = F \left|\Psi^-\right\rangle \left\langle\Psi^-\right| + \frac{1-F}{3} \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + \frac{1-F}{3} \left|\Phi^-\right\rangle \left\langle\Phi^-\right| + \frac{1-F}{3} \left|\Phi^+\right\rangle \left\langle\Phi^+\right| \quad (4.12)$$

This follows from the fact that, the state $|\Psi^+\rangle$ can evolve to the states $|\Psi^+\rangle, |\Phi^+\rangle$ and $|\Phi^-\rangle$ with equal probability 1/3, thus the density matrix $\tilde{\varrho} = p_1 |\Psi^+\rangle \langle\Psi^+|$ becomes $\tilde{\tilde{\varrho}} = \frac{p_1}{3}[|\Psi^+\rangle \langle\Psi^+| + |\Phi^+\rangle \langle\Phi^+| + |\Phi^-\rangle \langle\Phi^-|]$. Since the other triplet states have an analogue behavior, (4.12) follows immediately. The unilateral σ_y rotation turns ϱ into:

$$\varrho' = F \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + \frac{1-F}{3} \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + \frac{1-F}{3} \left|\Phi^-\right\rangle \left\langle\Phi^-\right| + \frac{1-F}{3} \left|\Psi^-\right\rangle \left\langle\Psi^-\right|$$

Then, the BXOR makes ϱ' evolve to:

$$\begin{aligned}\varrho'' = &|\xi_1\rangle\langle\xi_1| \otimes |\Phi^+\rangle\langle\Phi^+| + |\xi_2\rangle\langle\xi_2| \otimes |\Phi^-\rangle\langle\Phi^-| \\ &+ |\xi_3\rangle\langle\xi_3| \otimes |\Psi^+\rangle\langle\Psi^+| + |\xi_4\rangle\langle\xi_4| \otimes |\Psi^-\rangle\langle\Psi^-|\end{aligned}$$

where:

$$|\xi_1\rangle\langle\xi_1| = F^2|\Phi^+\rangle\langle\Phi^+| + F\frac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \left[\frac{1-F}{3}\right]^2|\Psi^+\rangle\langle\Psi^+| + \left[\frac{1-F}{3}\right]^2|\Psi^-\rangle\langle\Psi^-|$$

$$|\xi_2\rangle\langle\xi_2| = \left[\frac{1-F}{3}\right]^2|\Phi^+\rangle\langle\Phi^+| + F\frac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \left[\frac{1-F}{3}\right]^2|\Psi^+\rangle\langle\Psi^+| + \left[\frac{1-F}{3}\right]^2|\Psi^-\rangle\langle\Psi^-|$$

$$|\xi_3\rangle\langle\xi_3| = F\frac{1-F}{3}|\Phi^+\rangle\langle\Phi^+| + \left[\frac{1-F}{3}\right]^2|\Phi^-\rangle\langle\Phi^-| + F\frac{1-F}{3}|\Psi^+\rangle\langle\Psi^+| + F\frac{1-F}{3}|\Psi^-\rangle\langle\Psi^-|$$

$$|\xi_4\rangle\langle\xi_4| = \left[\frac{1-F}{3}\right]^2|\Phi^+\rangle\langle\Phi^+| + F\frac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \left[\frac{1-F}{3}\right]^2|\Psi^+\rangle\langle\Psi^+| + \left[\frac{1-F}{3}\right]^2|\Psi^-\rangle\langle\Psi^-|$$

The state $|\Phi^+\rangle$ of the second system is measured with probability:

$$p_1 = F^2 + F\frac{1-F}{3} + 2\left(\frac{1-F}{3}\right)^2$$

While the state $|\Phi^-\rangle$ with probability:

$$p_2 = F\frac{1-F}{3} + 3\left(\frac{1-F}{3}\right)^2$$

The overall probability to get a matching result (e.g. either $|\Phi^+\rangle$ or $|\Phi^-\rangle$) is:

$$p = p_1 + p_2 = F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2$$

In the case that the outcome is $|\Phi^+\rangle$ or $|\Phi^-\rangle$, the fidelity of the state $|\Phi^+\rangle$ (and thus the fidelity of $|\Psi^-\rangle$ after the σ_y operation of the fourth step) is

$$F' = \frac{\langle\Phi^+|\,\varrho''\,|\Phi^+\rangle}{p} = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} \tag{4.13}$$

In every iteration the probability to observe a matching result (and thus preserve the source pair) is given by p. In any case, the target particle is thrown away. Thus the yield of the algorithm after one step is:

$$Y = \frac{p}{2}$$

Expanding this expression gives the result (4.11).

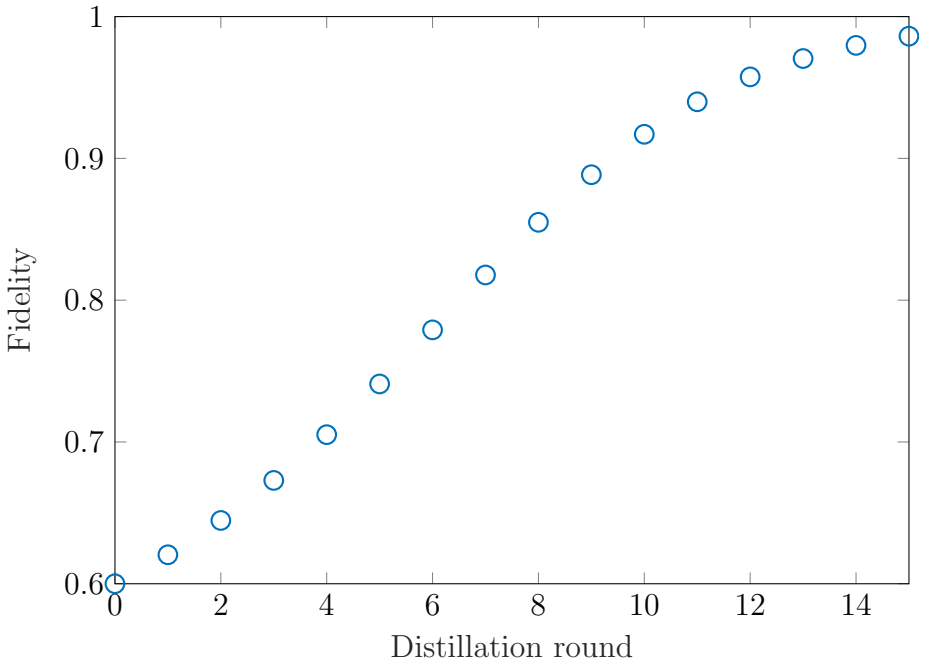

Figure 4.2: Fidelity improvement of the Bennett algorithm, with $F_0 = 0.6$.

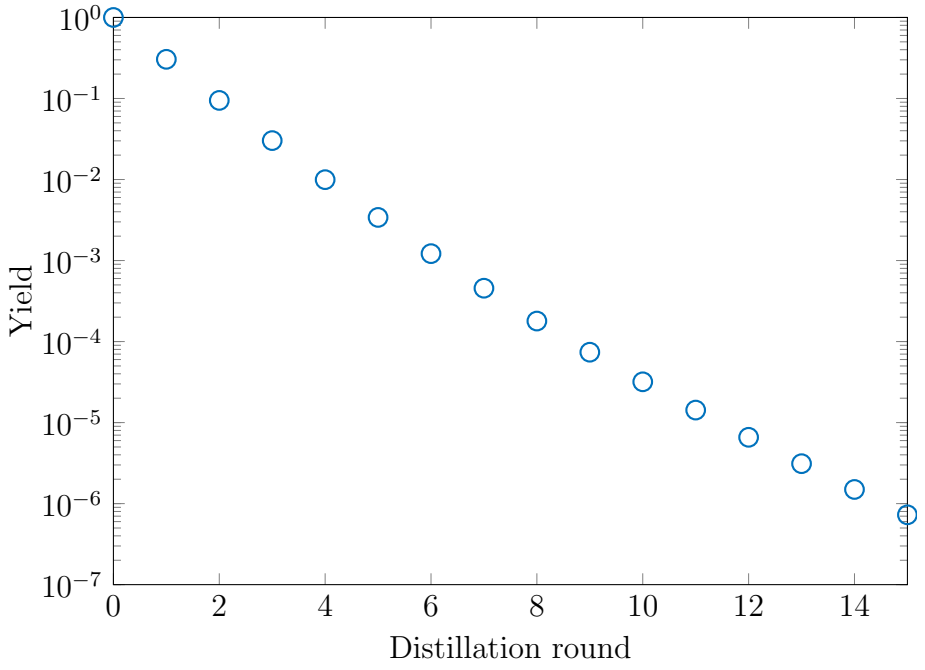

Figure 4.3: Yield of the Bennett algorithm as a function of distillation rounds, with $F_0 = 0.6$.

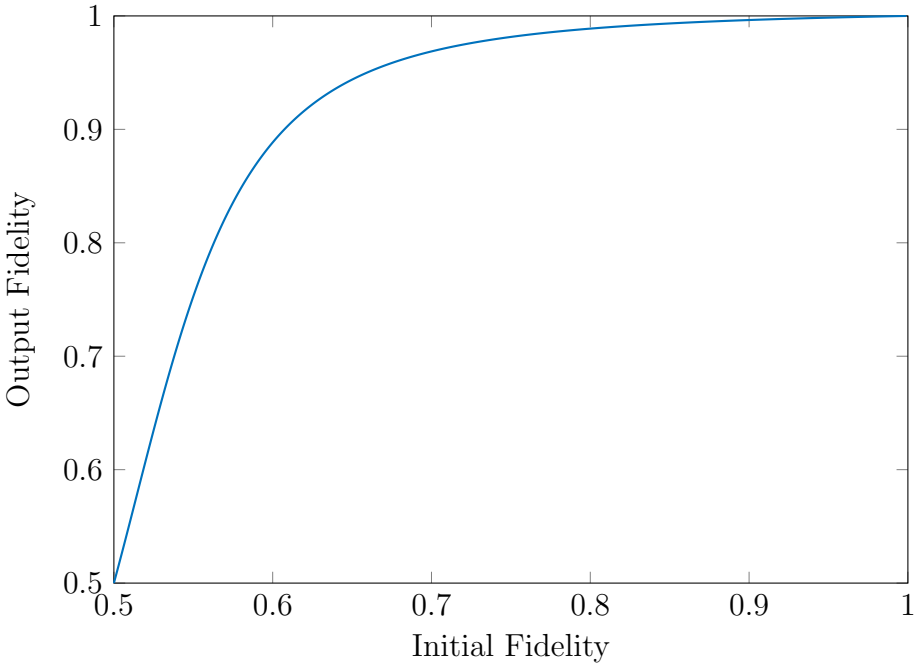

Figure 4.4: Output fidelity of the Bennett algorithm after 10 distillation rounds, in function of the initial fidelity.

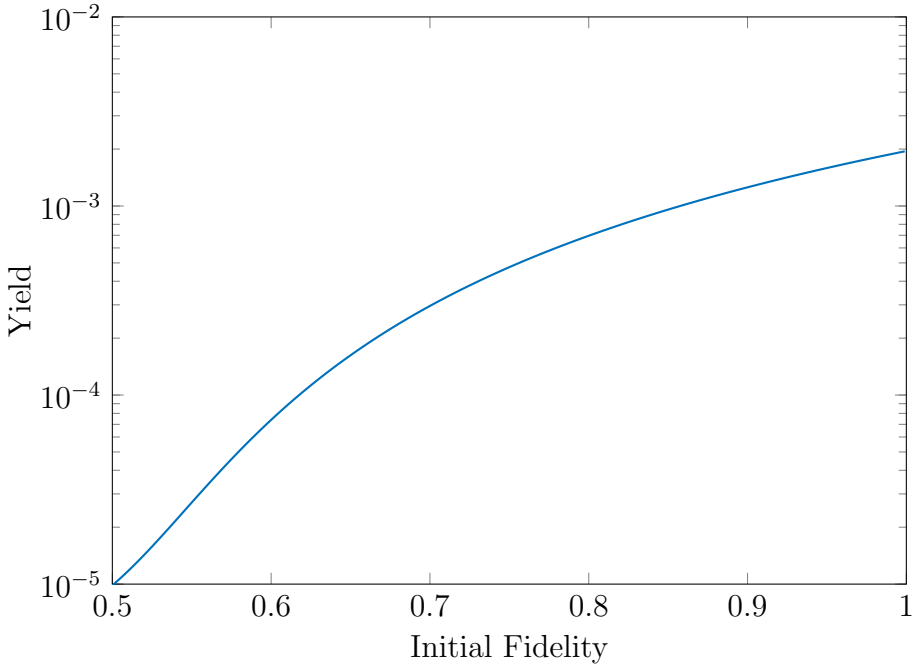

Figure 4.5: Yield of the Bennett algorithm after 10 distillation rounds, in function of the initial fidelity.

4.3.2 Efficient algorithm for phase-damping channels

The Bennett distillation algorithm can be used to purify a set of noisy entangled pairs, independently from the particular noise introduced by the channel. However, as already pointed out in the previous section, it has a very low efficiency that may limit its application in real world-scenario. This problem has recently attracted the attention of the scientific community [54, 55], with the aim to improve the algorithm performance, when applied to some specific scenarios. The first work in this direction, has been proposed by Ruan, Dai and Win in 2015 [54]. They improved Bennett's original algorithm by exploiting the specific structure of phase-damping channels. First of all, let recap the structure of the phase damping channel. As explained in section 4.2, the density operator at the channel output is described by the Kraus decomposition:

$$\varrho' = \sum_{k=1}^{2} E_k \varrho E_k^\dagger$$

where:

$$E_1 = \sqrt{F} I \quad ; \quad E_2 = \sqrt{1-F}\sigma_z$$

Due to a certain arbitrariness of the Kraus decomposition [17], sometimes the fidelity is given in term of a channel parameter p, which comes out from a different physical model of the channel, so that: $F = \frac{1+\sqrt{1-p}}{2}$. If ϱ is the density matrix of the state $|\Phi^+\rangle$, then the output of the PD channel is:

$$\varrho' = F \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + (1-F) \left|\Phi^-\right\rangle \left\langle\Phi^-\right| \tag{4.14}$$

Here the parameter $F = p$ has been used to explicit the role of the fidelity on the output of the PD channel. The first question that may arise is that if there is some limit on the maximum purification that could occur after performing LOCC, whenever the state is in the form (4.14). The answer is affirmative and has been solved in [54]:

Theorem 4.3.1. *Let suppose that Alice and Bob have two pairs of qubits with density matrix as in* (4.14)*:*

$$\varrho_{AB} = \varrho' \otimes \varrho'$$

Then, after performing an arbitrary LOCC:

$$\mathcal{F}(\tilde{\varrho}) \leq \frac{F^2}{F^2 + (1-F)^2} \tag{4.15}$$

The main contribution given by the authors in [54] is a recursive algorithm that achieves the upper bound of (4.15) after every iteration. The algorithm follows the following steps:

1. Alice and Bob locally apply an Hadamard gate to both qubits, followed by a CNOT operator on the two qubits they have at hand, as in step 3 of Bennett algorithm.

2. The two agent measure the target qubits using σ_z

3. If the measurement results match, then the source pair is preserved. Otherwise, it is discarded. Again, because the target pair is unusable after the measurement, it is always discarded.

The fidelity of the preserved pair after these operations is given by:

$$F_k = \frac{F_{k-1}^2}{F_{k-1}^2 + (1 - F_{k-1})^2} \tag{4.16}$$

And the yield by:

$$Y_{k+1} = \frac{1}{2}\Big[F_k^2 + (1 - F_k)^2\Big] Y_k \tag{4.17}$$

These formulas are proved in the original work [54]. By comparing (4.16) with (4.10) it is immediately clear that this algorithms have better performance both in terms of output fidelity and total yield. As a consequence, the convergence speed is higher. This may also be notice from a pictorial point of view, as reported in Figure 4.6. A performance plot is reported in Figure 4.7, using $p = 0.95$ as channel parameter, together with the performances of the Bennett's algorithm for comparison. Its immediate to see that this algorithm brings important improvements in terms of yield, as it permits to save precious distillation rounds with respect to the Bennett's algorithm. Of course this improvement comes at the price that this algorithms works faithfully only if the channel is phase-damping.

Remark 19. This algorithm presents a subtle difference with respect to the Bennett's algorithm. Indeed, as was previously noted, the fidelity improvement formula (4.10) of Bennett's algorithm should be intended in statistical terms, because the first operation is a *random* bilateral rotation. Conversely, all operations performed by this algorithm are deterministic, and thus the formula (4.16) is exact.

The same authors gave a generalization of the above results in case of two-Kraus-operator (TKO) channels, described by the decomposition:

$$\mathcal{E}(\varrho) = \sum_{k=1}^{2} E_k \varrho E_k^\dagger \quad ; \quad \sum_{k=1}^{2} E_k E_k^\dagger = I$$

Indeed, with similar results, it can be proven [55] that in the case of TKO channels, there exist an upper bound on the maximal fidelity achievable with LOCC, and that there exists an algorithm which reach this bound.

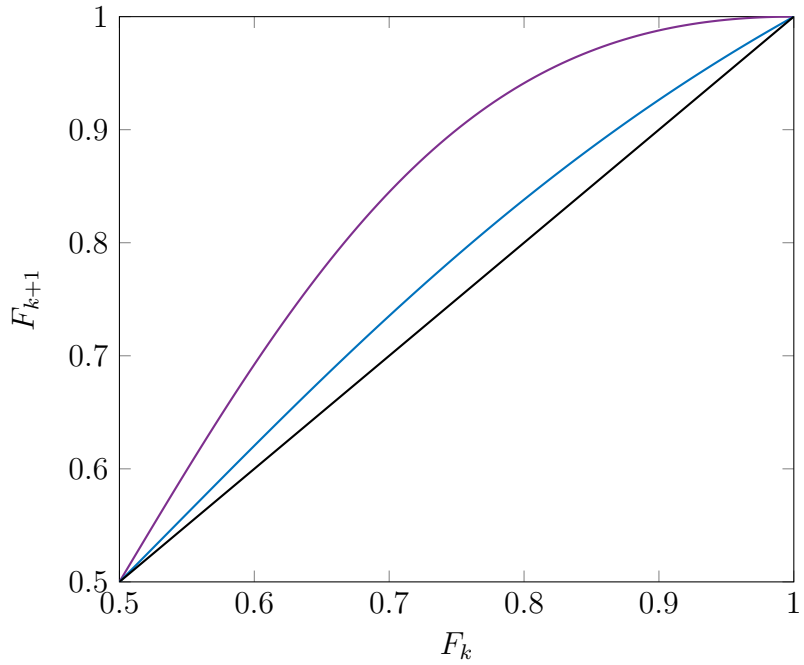

Figure 4.6: Fidelity improvement by a single round of the PD-efficient algorithm (purple), Bennett's algorithm (blue) and the bisecting line (black).

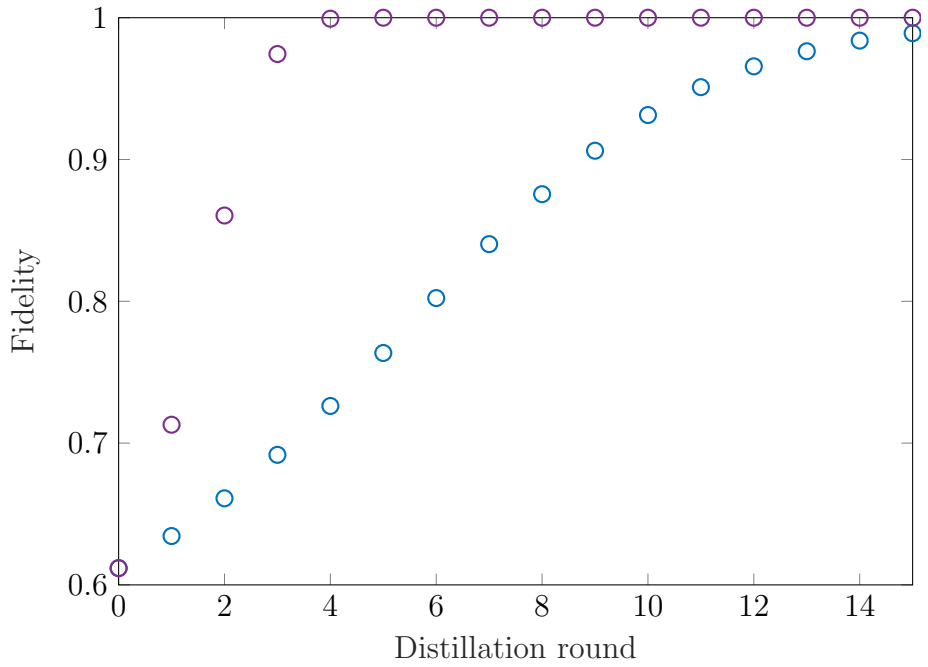

Figure 4.7: Comparison of the output fidelity of the PD-efficient algorithm (purple) and Bennett's algorithm (blue), as a function of the distillation rounds, with a channel parameter $p = 0.95$.

4.3.3 Simulation results

In order to prove and understand the theoretical results underpinning the algorithms presented here, a MATLAB^{TM} simulator has been developed for this thesis. The software consists of a set of routines which implement the postulates of quantum mechanics, using the formalism of density matrices to represent quantum states, as presented in section 2.3. Obviously, the framework can only be used to model finite-dimensional spaces, so that all the operators are also implemented as matrices while the tensor product is modeled through the Kronecker product [47].

The tool can both be used to make *predictions* about the behavior of a quantum system or, more interestingly, to *simulate* a quantum system. The latter case is of particular interest, as this allows to simulate quantum communication systems and perform Monte Carlo simulations to derive interesting statistical considerations. In particular, the tool have been used to verify and compare the performances of the EPPs presented in the previous section. To get reliable statistical results, a Monte Carlo simulation of the protocols has been ran on a set of 10^7 initial impure qubit pairs. The distillation process was stopped whenever the number of available pairs felt under 50, to avoid statistical perturbation in the samples. The results are reported in Figures 4.8 and 4.9 and unequivocally confirms the theoretical results. Furthermore, a plot of the cumulative distribution function (CDF) of the number of discarded pairs, for both algorithms, is given in Figure 4.10 and 4.11 after, respectively, one and five round of distillation. As expected, there exists a minimum amount of discarded pairs required to distillate a single purified pairs. If n is the number of distillation rounds, then the amount of discarded pairs is $N_d \geq 2^n - 1$. These plots confirm the superiority of the PD-efficient algorithm but they also show that there is an unavoidable increasing of variance within the number of rounds.

However, there are different interesting aspects which are worth to note and that could help in a better understanding of the theoretical results. First, it is interesting to compare the stochastic nature of Bennett's algorithm with the inherent deterministic nature of the efficient phase-damping QED algorithm. This is particularly visible in the right side of the plots, where the number of available pairs is not statistically representative.

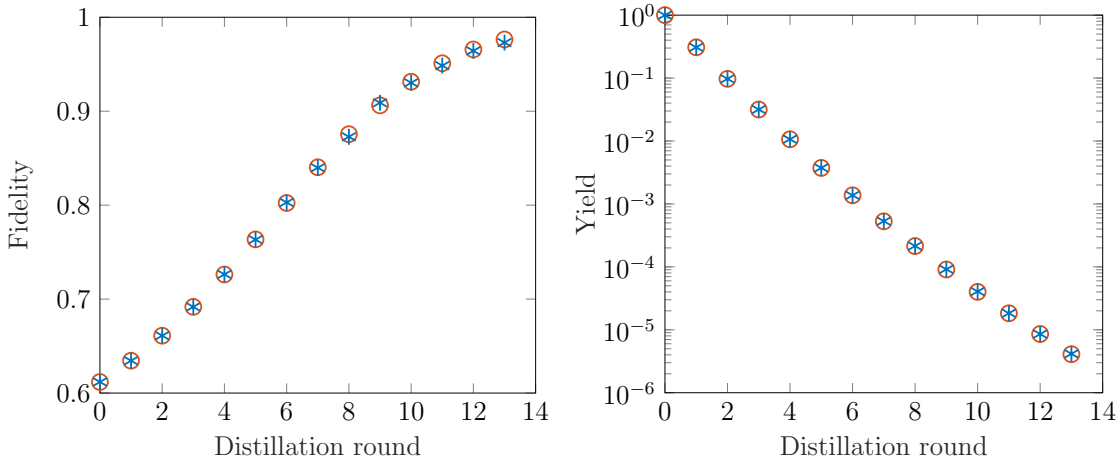

Figure 4.8: Performances of Bennett's algorithm in PD channel with $p = 0.95$. Theoretical results are marked in orange, while simulation results in blue.

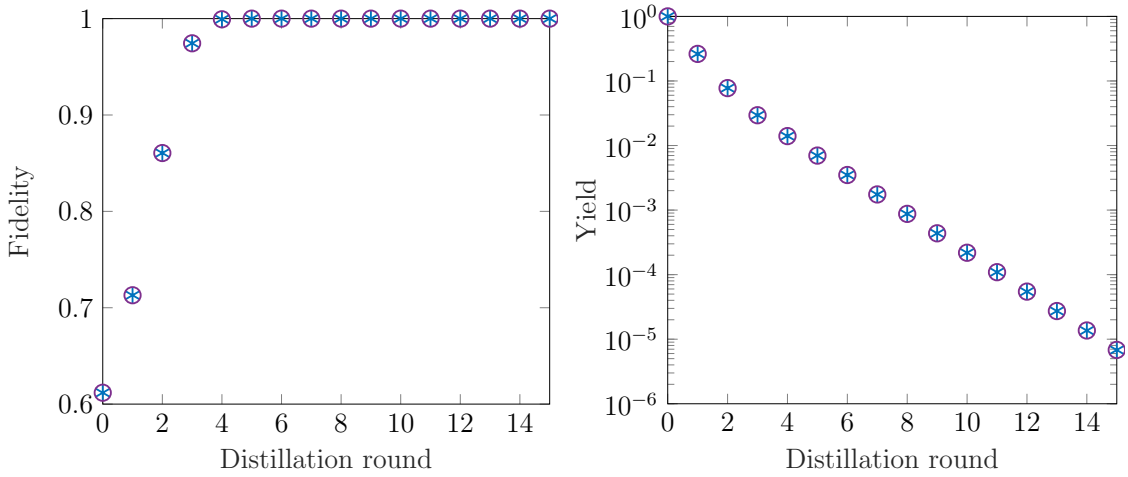

Figure 4.9: Performances of the PD-efficient algorithm in PD channel with $p = 0.95$. Theoretical results are marked in purple, while simulation results in blue.

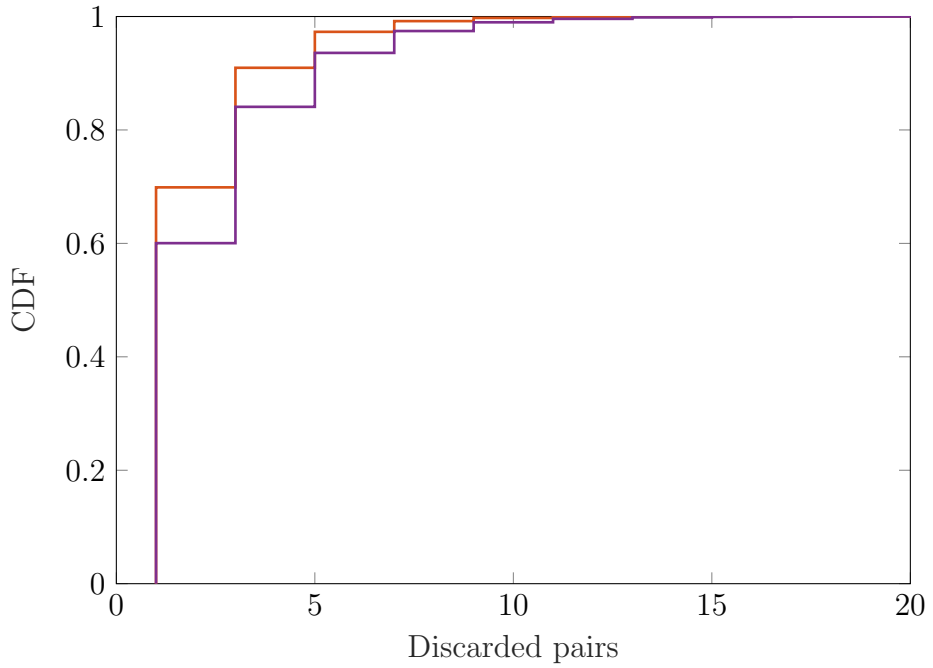

Figure 4.10: Empirical CDF of the number of discarded pairs after 1 distillation rounds with Bennett's algorithm (orange) and PD-efficient algorithm (purple).

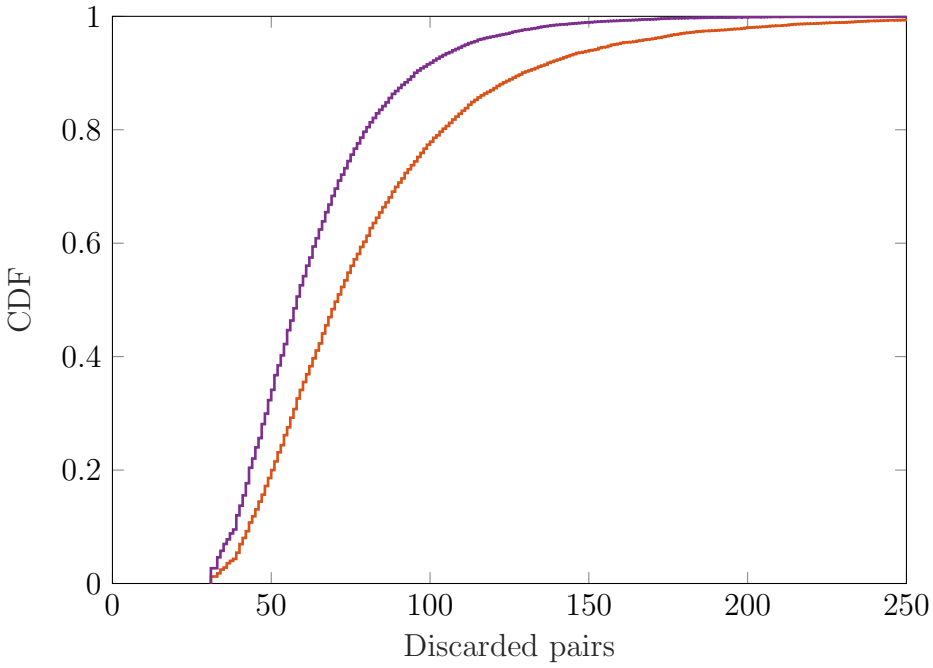

Figure 4.11: Empirical CDF of the number of discarded pairs after 5 distillation rounds with Bennett's algorithm (orange) and PD-efficient algorithm (purple).

Chapter 5

Conclusions

The field of quantum information and communications, starting from the physical background needed to face up the theory of quantum mechanics. For this reason, specific tools like density operators and generalized measurements have been introduced, together with some results that are of fundamental importance in quantum information, without losing the mathematical rigor that this tools carry on.

The entanglement phenomenon, that is so important in the applications, has been deeply analyzed both from a mathematical and phenomenological point of view. This strange effect has been source of discussions have been the born of quantum mechanics and the reasons behind these debates were illustrated. Even if these discussions seems to be pretty theoretical at a first glance, they turns out to be very important to deeply understand the nature of entanglement with an applicative point of view, as they give powerful instrument to characterize it.

The most promising application of quantum information has been detailedly exposed both from a physical and a rigorous mathematical point of view. Even if the most mature technology seems to be QKD, there is still lot of work that need to be accomplished in order to elevate the technology as a standard and get it ready for large-scale distribution. Other pretty interesting and simple effect like quantum teleportation and superdense coding are still under study in applied quantum information.

The mathematical model and the effects of quantum noise have been presented, together with some state-of-the-art techniques to mitigate these effects. It turns out that a correct modeling of the noise process also permits an ad-hoc tuning of distillation algorithms.

Finally, a framework developed to analyze quantum systems has been exposed. Some simulative results in the field of EPPs have been showed and commented in detail to compare different protocols.

Despite the success of quantum information, there are still some aspects of prac-

tical interest that needs to be further investigated. Indeed all exposed applications were thought to work in an ideal scenario, without the presence of noise or decoherence. The effect of the noise on the performances of the underlying communication system and on the distillation efficiency of EPPs is not yet clear in the literature. In particular, the quantitative effect of noise on the security of QKD protocols, intended as the capability to detect an eavesdropper on the channel, has not been addressed. Mathematically speaking, a link between the fidelity of the quantum states and the eavesdropper detection probability is expected. This would be a fundamental tool for system designers as it will permit to tune different aspects of the communication system to match the requisites of a particular scenario (e.g. the security parameters of a military network will inevitably be stronger then a civil network). On the other side, this relationship will also permit to get a link between the yield of EPPs and the security of the underlying QKD protocol, which will inevitably be anticorrelated. Because the noise is not a tunable parameter, the compromise between these two quantities is demanded to design the quantum communication system.

This is exactly what happens in classical communication systems, where different theoretical formulas can be used by engineers to tune the system parameters to match a particular performance requirement, depending on the application scenario.

The entry of engineers in quantum information, with their know-how in communication theory and systems, is expected to investigate these unexplored frontiers and to boost up quantum technology to get it ready for implementation. The big picture of this work was indeed to prepare a fertile ground upon which build a research activity.

Appendix A

Mathematical Preliminaries

There is no substitute for the process of abstracting and using mathematics to describe things which are beyond the ability to being directly visualized.

L. Susskind

Quantum mechanics is based on solid mathematical background, thanks to the works of von Neumann [16] who was the first to formalize the theory of Dirac [15] by using abstract Hilbert spaces and operators. Thanks to this formalization, it is possible to formulate the whole quantum theory starting from a set of mathematical axioms. This approach allows a powerful and formal description of physical systems but it also requires a deep understanding of the mathematics behind it.

This appendix collects some elementary definitions and theorems from functional analysis and linear algebra [56, 57, 47] that are widely used in quantum mechanics, even if they're frequently eluded, in order to avoid sweat into mathematical subtleties. However, even if this may result boring, the attentive reader must always be aware of the theoretical problems that may arise by an incorrect usage of mathematical symbols, in particular when dealing with symbolic bra-ket calculus.

It must be noted that different results are given only for finite-dimensional spaces, as their generalization may be difficult and useless for the purposes of this Thesis. Indeed qubits systems are formed by a finite composition of $2-$dimensional systems. The generalization of some results to infinite dimensional spaces requires advanced math and does not introduces nothing new from a physical point of view. The interested reader is referred to the excellent introductory treatise of Holevo [22].

The notation used in mathematical books is completely different from the one used in quantum mechanics. Dirac introduced the bra-ket notation in his pioneering work [15], and it turns out to be extremely useful when used for symbolic calculus.

A.1 Hilbert Spaces

Definition A.1.1 (Inner Product)**.** *Let $\mathcal{H}$ be a complex vector space. An inner product is a mapping:*

$$\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

such that for all $|x\rangle, |y\rangle, |z\rangle \in \mathcal{H}$, $\alpha \in \mathbb{C}$:

1) $\langle |x\rangle + |y\rangle, |z\rangle\rangle = \langle |x\rangle, |z\rangle\rangle + \langle |y\rangle, |z\rangle\rangle$

2) $\langle \alpha |x\rangle, |y\rangle\rangle = \alpha \langle |x\rangle, |z\rangle\rangle$

3) $\langle |x\rangle, |y\rangle\rangle = \langle |y\rangle, |x\rangle\rangle^*$

4) $\langle |x\rangle, |x\rangle\rangle \geq 0$

   $\langle |x\rangle, |x\rangle\rangle = 0 \iff |x\rangle = 0$

An inner product on $\mathcal{H}$ defines a norm on $\mathcal{H}$ given by:

$$\|x\| = \sqrt{\langle |x\rangle, |x\rangle\rangle}$$

Definition A.1.2 (Inner Product Space)**.** *A complex vector space X, with an inner product $\langle \cdot, \cdot \rangle$ defined on it, it's called inner product space (or pre-Hilbert space).*

A pre-Hilbert space is also a metric space, using the metric induced by the norm:

$$d(x, y) = \| |x\rangle - |y\rangle \|$$

Thus the notion of convergence is well defined:

$$\lim_{n\to\infty} |x_n\rangle = |x\rangle \iff \lim_{n\to\infty} d(|x\rangle, |x_n\rangle) = \lim_{n\to\infty} \| |x\rangle - |x_n\rangle \| = 0$$

Definition A.1.3 (Completeness)**.** *A metric space X is complete iff every Cauchy sequence is convergent in X.*

Definition A.1.4 (Hilbert Space)**.** *A pre-Hilbert space X, which is also complete, is called Hilbert Space.*

Remark 20. In quantum mechanics a completely different notation is used to denote elements in an Hilbert space. Every element $\psi \in \mathcal{H}$ is denoted with $|\psi\rangle$ (ket). This is the so called Dirac bra-ket notation which has strong advantages when it is used extensively.

A.2 Linear operators

A.2.1 Definitions

Definition A.2.1 (Linear operator)**.** *Let X,Y be vector spaces. The operator:*

$$T : \mathcal{D}(T) \subseteq X \to Y$$

is called ***linear operator*** *iff for all $|x\rangle, |y\rangle \in \mathcal{D}(T)$, $\alpha, \beta \in \mathbb{C}$:*

$$T(\alpha |x\rangle + \beta |y\rangle) = \alpha T(|x\rangle) + \beta T(|y\rangle)$$

Where $\mathcal{D}(T)$ denotes the domain of T.

Definition. The set of all linear operators defined on X with range in Y, denoted by $L(X, Y)$, is a vector space. The operations are defined as follow:

$$(L_1 + L_2)(|x\rangle) \triangleq L_1(|x\rangle) + L_2(|x\rangle)$$

$$(\alpha L_1)(|x\rangle) \triangleq \alpha L_1(|x\rangle)$$

Definition. A linear functional f is a linear operator on the vector space X whose range is in the scalar field $\mathbb{C}$

A.2.2 Dual space and the bra-ket notation

Definition. The dual space $\mathcal{H}^*$ of a normed space $\mathcal{H}$ is the set of all bounded linear functionals on $\mathcal{H}$. That is:

$$\mathcal{H}^* = \left\{ f : \mathcal{H} \to \mathbb{C} : \left| f |\psi\rangle \right| < \infty \quad \forall |\psi\rangle \in \mathcal{H} \right\}$$

Using Dirac's bra-ket notation [15], every element of the dual space is denoted by a bra: $\langle\xi|$. When a bra $\langle\xi|$ is applied to a ket $|\psi\rangle$, the result is a complex number called braket $\langle\xi|\psi\rangle$. The Riesz's Theorem [56] states that there exists a ket $|\xi\rangle$ uniquely associated to a bra $\langle\xi|$, such that for all $|\psi\rangle \in \mathcal{H}$, $\langle |\psi\rangle, |\xi\rangle \rangle = \langle\xi|\psi\rangle$. The converse could be easily proved. These results allow to use the very powerful Dirac's notation in the applications, with a strong mathematical background that formalizes it. The following rules describes the relationship between bras and kets:

$$|\psi\rangle \leftrightarrow \langle\psi|$$

$$\lambda |\psi\rangle \leftrightarrow \langle\psi| \lambda^*$$

$$|\psi_1\rangle + |\psi_2\rangle \leftrightarrow \langle\psi_1| + \langle\psi_2|$$

Let then suppose that $\{|\varphi_n\rangle\}_n$ is an orthonormal basis of $\mathcal{H}$, thus every vector $|\psi\rangle$ is spanned by such vectors, and:

$$|\psi\rangle = \sum_n c_n |\varphi_n\rangle = \sum_n \langle\varphi_n|\psi\rangle |\varphi_n\rangle$$

Since $c_n = \langle\varphi_n|\psi\rangle$ is a complex number, then:

$$|\psi\rangle = \left[\sum_n |\varphi_n\rangle \langle\varphi_n|\right] |\psi\rangle$$

This relation holds for all $|\psi\rangle$, and thus:

$$\sum_n |\varphi_n\rangle \langle\varphi_n| = I$$

where I is the identity operator. This relation expresses the completeness relation of the basis and it is very useful in proving different properties.

A.2.3 Linear operators in finite dimensional space

Finite dimensional vector spaces are simpler than infinite dimensional ones.

Lemma A.2.2. *Let X and Y be finite dimensional vector spaces and let $E = \{|e_1\rangle, |e_2\rangle, ..., |e_n\rangle\}$ and $B = \{|b_1\rangle, |b_2\rangle, ..., |b_m\rangle\}$ be the basis of, respectively, X and Y. Then, every linear operator:*

$$\mathcal{L} : X \to Y$$

can be uniquely represented by an $m \times n$ complex matrix.

Proof. Using the completeness, relation:

$$|x\rangle = \sum_i |e_i\rangle \langle e_i|x\rangle$$

$$|y\rangle = \mathcal{L}|x\rangle = \sum_j |b_j\rangle \langle b_j| \mathcal{L} |x\rangle = \left[\sum_{ij} |b_j\rangle \langle b_j| \mathcal{L} |e_i\rangle \langle e_i|\right] |x\rangle$$

Once a basis is chosen on X and Y the operator $\mathcal{L}$ is thus represented by:

$$\sum_{ij} |b_j\rangle \langle b_j| \mathcal{L} |e_i\rangle \langle e_i|$$

Which uniquely depends on the matrix $\mathbf{L}$ whose coefficients are defined by:

$$\mathbf{L}_{ji} = \langle b_j| \mathcal{L} |e_i\rangle$$

□

A.2.4 Adjoint operators

Definition. Let $\mathcal{L} : \mathcal{H} \to \mathcal{H}$ be a bounded linear operator. Then the adjoint operator $\mathcal{L}^\dagger$ of $\mathcal{L}$ is the operator:

$$\mathcal{L}^\dagger : \mathcal{H} \to \mathcal{H}$$

such that, for all $|\psi\rangle, |\xi\rangle \in \mathcal{H}$:

$$\langle\xi| \left[\mathcal{L}\,|\psi\rangle\right] = \left[\langle\xi|\,\mathcal{L}^\dagger\right] |\psi\rangle$$

It is not trivial to prove [56, Theorem 3.9-2] that $\mathcal{L}^\dagger$ always exists. The existence of the adjoint operator is another interesting property of the bra-ket notation, because it permits to apply linear operators on kets as well on bras, by keeping in mind to switch between an operator and its adjoint. In other terms they give the apparently simple property:

$$\mathcal{L}\,|\psi\rangle \leftrightarrow \langle\psi|\,\mathcal{L}^\dagger$$

If $\mathcal{L}^\dagger = \mathcal{L}$ the operator is said to be self-adjoint. From a purely formal point of view, this mean that it can be indifferently applied to a bra or a ket, as it is equal to its adjoint. These kind of operators is fundamental in quantum mechanics and they have very interesting properties:

Theorem A.2.3. *Let $\mathcal{L}$ be a self-adjoint operator in $\mathcal{H}$. Then:*

- *All the eigenvalues of $\mathcal{L}$ are real*
- *Eigenvector corresponding to numerically different eigenvalues are orthogonal*

The last property, together with the Gram-Schmidt procedure (that must be used in the case of degenerate eigenvalues), allows to find an orthonormal basis of $\mathcal{H}$ which is described by eigenvectors of $\mathcal{L}$.

The adjoint operator is used to give the important definition of unitary operator:

Definition A.2.4. *An operator $\mathcal{U}$ is said to be unitary if $\mathcal{U}^\dagger\mathcal{U} = I$.*

Theorem A.2.5 (Stone's Theorem [22])**.** *A time-dependent continuous operator $\mathcal{U}(t)$ is unitary if and only if there exists a unique self-adjoint operator H such that:*

$$\mathcal{U}(t) = \exp(itH)$$

A.2.5 Projection operators

The concept of a projection operator is of fundamental importance in quantum mechanics, and the generalizes the concept of orthogonal projections in euclidean geometry. Indeed it is possible to prove that every Hilbert space can be represented as the direct sum of a closed subspace $\mathcal{Y}$ and its orthogonal complement $\mathcal{Y}^{\perp}$, thus $\forall\, |x\rangle \in \mathcal{H}$, there exists unique $|y\rangle \in \mathcal{Y}, |z\rangle \in \mathcal{Y}^{\perp}$ (e.g. $\langle y|z\rangle = 0$) such that:

$$|x\rangle = |y\rangle + |z\rangle$$

Where $|y\rangle$ is the orthogonal projection of $|x\rangle$ in $\mathcal{Y}$. Thus the above relation defines the linear operator

$$\mathcal{P} : |x\rangle \to |y\rangle = \mathcal{P}\,|x\rangle$$

Projection operators satisfies some useful properties:

Lemma A.2.6 ([56])**.** *A bounded linear operator $\mathcal{P} : \mathcal{H} \to \mathcal{H}$ is a projection operator if and only if:*

$$\mathcal{P} = \mathcal{P}^{\dagger}$$

$$\mathcal{P} = \mathcal{P}^{2}$$

Lemma A.2.7. *Let $\mathcal{P}$ be a projection operator in $\mathcal{H}$. The eigenvalues of $\mathcal{P}$ are either 0 or 1.*

Proof. Let λ be an eigenvalue for $\mathcal{P}$, then:

$$\mathcal{P}\,|\psi\rangle = \lambda\,|\psi\rangle$$

Because $\mathcal{P}^2 = \mathcal{P}$, it follows that:

$$\mathcal{P}^2\,|\psi\rangle = \lambda^2\,|\psi\rangle = \mathcal{P}\,|\psi\rangle = \lambda\,|\psi\rangle$$

Thus:

$$(\lambda^2 - \lambda)\,|\psi\rangle = 0$$

Since $|\psi\rangle \neq 0$, it follows that $\lambda = 0$ or $\lambda = 1$. □

Projection operators are important as they can be used to decompose a self-adjoint operator, as the following theorem:

Theorem A.2.8 (Spectral Theorem)**.** *Let $\mathcal{L}$ be a self-adjoint operator in $\mathcal{H}$ and let $|\varphi_n\rangle$ be a basis in $\mathcal{H}$, then:*

$$\mathcal{L} = \sum_j \lambda_j \mathcal{P}_j$$

Where $\mathcal{P}_j$ is the projector into the eigenspace associated to λ_j

A.3 Tensor product

The tensor product is a method to merge two vector spaces into a larger one. This operation is crucial to build composite system, as according to postulate 6 the state space of a composite quantum system is the tensor product of the subspaces.

A.3.1 Definition

A vector space $\mathcal{H}$ is called the tensor product of $\mathcal{H}_1$ and $\mathcal{H}_2$:

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

if, for all $|\varphi\rangle \in \mathcal{H}_1$, $|\psi\rangle \in \mathcal{H}_2$ there exists a vector $|\xi\rangle \in \mathcal{H}$, denoted by[1]:

$$|\xi\rangle \triangleq |\varphi\rangle \otimes |\psi\rangle$$

that satisfies the following condition:

i) Linearity:
$$[\alpha\,|\varphi\rangle] \otimes [\beta\,|\psi\rangle] = \alpha\beta[|\varphi\rangle \otimes |\psi\rangle]$$

ii) Distributivity:

$$[|\varphi_1\rangle + |\varphi_2\rangle] \otimes |\psi\rangle = |\varphi_1\rangle \otimes |\psi\rangle + |\varphi_2\rangle \otimes |\psi\rangle$$

$$|\varphi\rangle \otimes [|\psi_1\rangle + |\psi_2\rangle] = |\varphi\rangle \otimes |\psi_1\rangle + |\varphi\rangle \otimes |\psi_2\rangle$$

iii) When the basis $\{|u_i\rangle\}_i$,$\{|v_k\rangle\}_k$ are chosen for, respectively, $\mathcal{H}_1$ and $\mathcal{H}_2$, the set of vectors:
$$\{|u_i\rangle \otimes |v_k\rangle\}_{i,k}$$
is a basis for $\mathcal{H}$.

iv) The scalar product in $\mathcal{H}$ is defined as:

$$\langle\varphi_1\psi_1|\varphi_2\psi_2\rangle = \langle\varphi_1|\varphi_2\rangle\,\langle\psi_1|\psi_2\rangle$$

From the property iii) it may be argued that the form of the space $\mathcal{H}$ depends on the representation basis chosen for $\mathcal{H}_1$ and $\mathcal{H}_2$. The following lemma proves that this is not true.

Lemma A.3.1. *The structure of the tensor product space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ does not depend on the choice of the basis in $\mathcal{H}_1$ and $\mathcal{H}_2$.*

[1] To simplify the notation, the tensor product $|\varphi\rangle \otimes |\psi\rangle$ is sometimes written as: $|\varphi\psi\rangle$ or $|\varphi\rangle\,|\psi\rangle$

Proof. Let $\{|i\rangle\}$,$\{|i'\rangle\}$ and $\{|j\rangle\}$,$\{|j'\rangle\}$ two different orthonormal basis for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Suppose that $\mathcal{H}$ is the product space with the $|ij\rangle$ basis, while $\mathcal{H}'$ is the product space with the $|i'j'\rangle$ basis. Then, it is possible to define the linear operator $\mathcal{U}$ as:

$$\mathcal{U}\,|ij\rangle = |i'j'\rangle$$

Which is unitary and thus invertible, and it preserves the structure of the space. This means that $\mathcal{U}$ is an isomorphism between $\mathcal{H}$ and $\mathcal{H}'$. □

There is a particular set of vectors in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ that is very important in quantum mechanics:

Definition A.3.2 (Pure vector)**.** *Let $|\psi\rangle$ be a vector in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Then $|\psi\rangle$ is a product vector if there exist $|\xi_1\rangle \in \mathcal{H}_1$,$|\xi_2\rangle \in \mathcal{H}_2$ such that:*

$$|\psi\rangle = |\xi_1\rangle \otimes |\xi_2\rangle$$

Theorem A.3.3 (Schmidt Decomposition)**.** *Let $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Then, there exist two sets of orthonormal states $\{|a_i\rangle\}_i \in \mathcal{H}_1$, $\{|b_i\rangle\}_i \in \mathcal{H}_2$ such that:*

$$|\psi\rangle = \sum_i \lambda_i\,|a_i\rangle\,|b_i\rangle \tag{A.1}$$

Proof. Every vector $|\psi\rangle$ could be written using a generic $|j\rangle\,|k\rangle$ basis in $\mathcal{H}$:

$$|\psi\rangle = \sum_{jk} c_{jk}\,|j\rangle\,|k\rangle$$

The matrix of coefficients $\mathbf{C} = \{c_{jk}\}$ could be expressed using the singular value decomposition $\mathbf{C} = \mathbf{U\Sigma V}$, where $\mathbf{\Sigma}$ is a diagonal matrix and $\mathbf{U}, \mathbf{V}$ are unitary matrices. Thus

$$c_{jk} = \sum_{ii'} u_{ji}\sigma_{ii'}v_{i'k} = \sum_i u_{ji}\sigma_{ii}v_{ik}$$

So that:

$$|\psi\rangle = \sum_{ijk} u_{ji}\sigma_{ii}v_{ik}\,|j\rangle\,|k\rangle = \sum_i \sigma_{ii}\left(\sum_j u_{ji}\,|j\rangle\right)\left(\sum_k v_{ik}\,|k\rangle\right)$$

Defining $|a_i\rangle = \sum_j u_{ji}\,|j\rangle$, $|b_i\rangle = \sum_k v_{ik}\,|k\rangle$ and $\lambda_i = \sigma_{ii}$, the form (A.1) follows immediately. The orthogonality of $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$ follows from the orthogonality of the columns in $\mathbf{U}$. □

A.3.2 Operators

The tensor product space $\mathcal{H}$ is an Hilbert space, so that it is well defined the space $L(\mathcal{H})$ of the linear operator on $\mathcal{H}$. However, since $\mathcal{H}$ is a *composition* of $\mathcal{H}_1$ and $\mathcal{H}_2$, it is possible to extend operators defined on the constituent spaces $\mathcal{H}_1$ and $\mathcal{H}_2$.

Definition A.3.4 (Extension)**.** *Let $\mathcal{L}$ be an operator in $\mathcal{H}_1$. The extension $\tilde{\mathcal{L}}$ of $\mathcal{L}$ into $\mathcal{H}$ is defined as:*

$$\tilde{\mathcal{L}}(|\varphi\rangle \otimes |\psi\rangle) \triangleq \mathcal{L}\,|\varphi\rangle \otimes |\psi\rangle$$

Remark. To avoid cumbersome notation, the extended operator is always identified by the same symbol as the original one.

Definition A.3.5 (Tensor product of operators)**.** *Let $\mathcal{A}$ be an operator in $\mathcal{H}_1$ and $\mathcal{B}$ an operator in $\mathcal{H}_2$. Their tensor product is an operator $\mathcal{A} \otimes \mathcal{B}$ on $\mathcal{H}$ defined as:*

$$(\mathcal{A} \otimes \mathcal{B})(|\varphi\rangle \otimes |\psi\rangle) \triangleq \mathcal{A}\,|\varphi\rangle \otimes \mathcal{B}\,|\psi\rangle$$

Definition A.3.6. *An operator $\mathcal{L} \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is said to be a product operator, if there exist two operators $\mathcal{A} \in \mathcal{H}_1, \mathcal{B} \in \mathcal{H}_2$, such that:*

$$\mathcal{L}(|\varphi\rangle \otimes |\psi\rangle) = \mathcal{A}\,|\varphi\rangle \otimes \mathcal{B}\,|\psi\rangle$$

If $\mathcal{L}$ is a product operator, than it is noted as $\mathcal{L} = \mathcal{A} \otimes \mathcal{B}$.

It is possible to generalize the above definitions to operators whose range is not the initial vector space. Just for completeness, the definition is reported here:

Definition A.3.7 (Tensor product of linear maps)**.** *Given the two linear maps $\mathcal{A} : \mathcal{H}_1 \to \mathcal{X}$ and $\mathcal{B} : \mathcal{H}_2 \to \mathcal{Y}$, the tensor product of the two linear maps is a linear map:*

$$\mathcal{A} \otimes \mathcal{B} : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathcal{X} \otimes \mathcal{Y}$$

defined by:

$$(\mathcal{A} \otimes \mathcal{B})(|\varphi\rangle \otimes |\psi\rangle) \triangleq \mathcal{A}\,|\varphi\rangle \otimes \mathcal{B}\,|\psi\rangle$$

Remark. Like vectors in the tensor product space, there exists operators on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ that are not product operators. However, it is not obvious that any operator on $\mathcal{H}$ could be decomposed as a linear combination of product operators.

Lemma A.3.8. *Every linear operator $\mathcal{U}$ on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ could be decomposed as:*

$$\mathcal{U} = \sum_i \sum_j c_{ij} \mathcal{A}_i \otimes \mathcal{B}_j \tag{A.2}$$

where $c_{ij} \in \mathbb{C}$ and $\{\mathcal{A}_i\}_i$, $\{\mathcal{B}_j\}_j$ are two fixed orthonormal operator bases on, respectively, $L(\mathcal{H}_1)$ and $L(\mathcal{H}_2)$.

Proof. By definition $\mathcal{U} \in L(\mathcal{H}_1 \otimes \mathcal{H}_2)$, and obviously $L(\mathcal{H}_1) \otimes L(\mathcal{H}_2) \subset L(\mathcal{H}_1 \otimes \mathcal{H}_2)$ as product operators represent a particular example of operators in $\mathcal{H}_1 \otimes \mathcal{H}_2$. To prove this lemma is sufficient to prove that $\mathcal{U} \in L(\mathcal{H}_1) \otimes L(\mathcal{H}_2)$, thus proving that $L(\mathcal{H}_1) \otimes L(\mathcal{H}_2) = L(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Indeed, the latter is the tensor product space of $\mathcal{H}_1$ and $\mathcal{H}_2$, and the decomposition follows from the definition of product space.
Let $|i\rangle |j\rangle$ be a orthonormal basis of $\mathcal{H}$. Then, from the completeness relation:

$$\sum_{ij} |i\rangle |j\rangle \langle i| \langle j| = I$$

it follows that:

$$\mathcal{U} = \sum_{ij} \sum_{i'j'} |i\rangle |j\rangle \langle i| \langle j| \mathcal{U} |i'\rangle |j'\rangle \langle i'| \langle j'|$$

where:

$$\mathbf{U}_{iji'j'} = \langle i| \langle j| \mathcal{U} |i'\rangle |j'\rangle$$

is the tensorial representation of the operator $\mathcal{U}$. Then, by rearranging the terms:

$$\mathcal{U} = \sum_{ij} \sum_{i'j'} \mathbf{U}_{iji'j'} |i\rangle |j\rangle \langle i'| \langle j'| = \sum_{ij} \sum_{i'j'} \mathbf{U}_{iji'j'} |i\rangle \langle i'| \otimes |j\rangle \langle j'|$$

and this proves that $\mathcal{U} \in L(\mathcal{H}_1) \otimes L(\mathcal{H}_2)$. □

Corollary (Schmidt decomposition of operators)**.** *Every linear operator* $\mathcal{U}$ *could be decomposed as:*

$$\mathcal{U} = \sum_i \lambda_i \mathcal{A}_i \otimes \mathcal{B}_i \tag{A.3}$$

Proof [58]. The proof is analogue to the proof of the Schmidt decomposition Theorem, since $\mathcal{U}$ could be expressed in the form of (A.2). □

A.3.3 Matrices

When dealing with different cases of practical interest in quantum information, the state space of the system is finite-dimensional. In this case the above formalism can be replaced by matrices. In particular, let $\mathcal{A}, \mathcal{B}$ be operators on, respectively, $\mathcal{H}_1$ and $\mathcal{H}_2$. If $\mathcal{H}_1$ has dimensionality n, and $\mathcal{H}_2$ dimensionality m, then, once a basis is fixed on the two spaces, the operators can be represented with the square matrices $\mathbf{A}$, which is $n \times n$ and $\mathbf{B}$, which is $m \times m$. Then, the tensor product $\mathbf{A} \otimes \mathbf{B}$ is an operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$, which is an $n \times m$-dimensional space, represented by the Kronecker product [47] of $\mathbf{A} \otimes \mathbf{B}$. The Kronecker product matrix is defined in blocks as follows:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \dots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \dots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \dots & a_{nn}\mathbf{B} \end{bmatrix} \tag{A.4}$$

In the above finite-dimensional spaces, two generic states $|\psi\rangle \in \mathcal{H}_1, |\varphi\rangle \in \mathcal{H}_2$ are represented by the column vectors $\boldsymbol{\psi} \in \mathbb{R}^n$ and $\boldsymbol{\varphi} \in \mathbb{R}^m$. Since they are a one-dimensional matrices, it thus follows that the product state $|\psi\rangle \otimes |\varphi\rangle$ is represented by a vector $\boldsymbol{\psi} \otimes \boldsymbol{\varphi}$, whose elements are defined by the Kronecker product as in (A.4).

Example

A very simple but useful example can be explained for the 2-dimensional space of qubits $\mathcal{Q}$. Let suppose to combine two qubit system together into the larger space $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. Then, if $|\psi\rangle \in \mathcal{Q}_1$ and $|\varphi\rangle \in \mathcal{Q}_2$, they are represented by:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \leftrightarrow \boldsymbol{\psi} = \begin{bmatrix} \alpha_0 & \alpha_1 \end{bmatrix}^T$$

$$|\varphi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle \leftrightarrow \boldsymbol{\varphi} = \begin{bmatrix} \beta_0 & \beta_1 \end{bmatrix}^T$$

so that:

$$|\psi\rangle \otimes |\varphi\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$$

Equivalently, the tensor product vector can be computed using the rule (A.4):

$$|\psi\rangle \otimes |\varphi\rangle \leftrightarrow \boldsymbol{\psi} \otimes \boldsymbol{\varphi} = \begin{bmatrix} \alpha_0\beta_0 & \alpha_0\beta_1 & \alpha_1\beta_0 & \alpha_1\beta_1 \end{bmatrix}^T$$

Using analogue considerations, let suppose that $\mathcal{A}$ and $\mathcal{B}$ are two operators in, respectively, $\mathcal{Q}_1$ and $\mathcal{Q}_2$. They are thus represented by the 2×2 matrices:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad ; \quad \mathbf{B} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

The product operator $\mathcal{A} \otimes \mathcal{B}$ in $\mathcal{Q}_1 \otimes \mathcal{Q}_2$ is thus represented by the 4×4 matrix obtained with the Kronecker rule (A.4):

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{11}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{21}b_{11} & a_{21}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$

Bibliography

[1] C. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[2] ——, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] J. Pieprzyk, T. Hardjono, and J. Seberry, *Fundamentals of computer security*. Springer-Verlag, 2013.

[4] W. Zurek, "Decoherence, einselection, and the quantum origins of the classical," *Reviews of Modern Physics*, vol. 75, no. 3, pp. 715–775, 2003.

[5] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[6] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, 2017.

[7] Gartner, "Gartner's 2016 hype cycle for emerging technologies," http://www.gartner.com/newsroom/id/3412017, [Online; accessed 15-July-2017].

[8] M. Mohseni *et al.*, "Commercialize quantum technologies in five years," *Nature*, vol. 543, no. 7644, pp. 171–174, 2017.

[9] D. Castelvecchi, "IBM's quantum cloud computer goes commercial," *Nature*, vol. 543, no. 7644, p. 159, 2017.

[10] L. Susskind and A. Friedman, *Quantum mechanics: the theoretical minimum*. Basic Books, 2015, vol. 2.

[11] R. Feynman, M. Sands, and R. Leighton, *The Feynman Lectures on Physics*. Addison–Wesley, 1964, vol. 3.

[12] D. J. Griffiths, *Introduction to quantum mechanics*, 2nd ed. Prentice Hall, 2004.

[13] C. Cohen-Tannoudji, B. Diu, and F. Laloe, *Quantum Mechanics*. Wiley, 1977.

[14] K. S. Lam, *Non-Relativistic Quantum Theory: Dynamics, Symmetry, and Geometry*. World Scientific Publishing Company, 2009.

[15] P. A. M. Dirac, *The principles of quantum mechanics*. Oxford University Press, 1981.

[16] J. Von Neumann, *Mathematical foundations of quantum mechanics*. Princeton University Press, 1955.

[17] M. A. Nielsen and I. L. Chuang, *Quantum information and quantum computation*. Cambridge University Press, 2000.

[18] R. B. Ash and C. Doleans-Dade, *Probability and measure theory*. Academic Press, 2000.

[19] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review*, vol. 47, no. 10, pp. 777–780, 1935.

[20] E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," *Naturwissenschaften*, vol. 23, no. 48, pp. 807–812, Nov 1935, [English translation in [21]].

[21] J. D. Trimmer, "The present situation in quantum mechanics: A translation of schrödinger's "cat paradox" paper," *Proceedings of the American Philosophical Society*, vol. 124, no. 5, pp. 323–338, 1980.

[22] A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, ser. De Gruyter Studies in Mathematical Physics. De Gruyter, 2013.

[23] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, no. 4, pp. 2738–2747, 1995.

[24] W. Wootters and W. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[25] M. Born, "The born-einstein letters," *Walker and Company, New York*, p. 158, 1971.

[26] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics*, vol. 1, pp. 195—200, 1964.

[27] "IEEE Quantum communications & information technology emerging technical subcommittee," http://qcit.committees.comsoc.org/, [Online; accessed 15-July-2017].

[28] D. Bohm, *Quantum theory*. Prentice Hall, 1951.

[29] J. S. Bell, *Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy*. Cambridge University Press, 1987.

[30] J. Clauser, M. Horne, A. Shimony, and R. Holt, "Proposed experiment to test local hidden-variable theories," *Physical Review Letters*, vol. 23, no. 15, pp. 880–884, 1969.

[31] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of Modern Physics*, vol. 86, no. 2, pp. 419–478, 2014.

[32] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics*, vol. 81, no. 2, pp. 865–942, 2009.

[33] V. Vedral and M. Plenio, "Entanglement measures and purification procedures," *Physical Review A*, vol. 57, no. 3, pp. 1619–1633, 1998.

[34] R. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," *Physical Review A*, vol. 40, no. 8, pp. 4277–4281, 1989.

[35] L. Gurvits, "Classical deterministic complexity of edmonds' problem and quantum entanglement," in *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, ser. STOC '03. New York, NY, USA: ACM, 2003, pp. 10–19.

[36] N. Gisin, "Bell's inequality holds for all non-product states," *Physics Letters A*, vol. 154, no. 5-6, pp. 201–202, 1991.

[37] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters*, vol. 76, no. 5, pp. 722–725, 1996.

[38] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[39] C. Bennett and S. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[40] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, 1984.

[41] A. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[42] H. Singh, D. Gupta, and A. Singh, "Quantum key distribution protocols: A review," *Journal of Computational Information Systems*, vol. 8, pp. 2839–2849, 2012.

[43] K.-E. Hellwig and K. Kraus, "Pure operations and measurements," *Communications in Mathematical Physics*, vol. 11, no. 3, pp. 214–220, 1969.

[44] ——, "Operations and measurements. II," *Communications in Mathematical Physics*, vol. 16, no. 2, pp. 142–147, 1970.

[45] A. Peres, "Neumark's theorem and quantum inseparability," *Foundations of Physics*, vol. 20, no. 12, pp. 1441–1453, 1990.

[46] C. Bennett, D. DiVincenzo, C. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. Wootters, "Quantum nonlocality without entanglement," *Physical Review A*, vol. 59, no. 2-3, pp. 1070–1091, 1999.

[47] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. New York, NY, USA: Cambridge University Press, 2012.

[48] J. Preskill, "Lecture notes for Physics 219: Quantum computation," 2015. [Online]. Available: http://www.theory.caltech.edu/~preskill/ph219/

[49] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[50] M. Plenio and S. Virmani, "An introduction to entanglement measures," *Quantum Information and Computation*, vol. 7, no. 1-2, pp. 1–51, 2007.

[51] J. Proakis and M. Salehi, *Digital Communications*, 5th ed. McGraw-Hill Education, 2007.

[52] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[53] P. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, pp. 2493–2496, 1995.

[54] L. Ruan, W. Dai, and M. Win, "Efficient recurrence quantum distillation algorithm for phase-damping channel," in *Proceedings of IEEE Globecom Workshops*, Dec 2015, pp. 1–6.

[55] ——, "Analysis of efficient recurrence quantum entanglement distillation," in *Proceedings of IEEE Globecom Workshops*, Dec 2016, pp. 1–6.

[56] E. Kreyszig, *Introductory Functional Analysis with Applications*. John Wiley & Sons, 1989.

[57] A. Kolmogorov and S. Fomin, *Elements of the Theory of Functions and Functional Analysis*. Dover Books, 1999.

[58] M. Nielsen, C. Dawson, J. Dodd, A. Gilchrist, D. Mortimer, T. Osborne, M. Bremner, A. Harrow, and A. Hines, "Quantum dynamics as a physical resource," *Physical Review A*, vol. 67, no. 5, pp. 523 011–5 230 119, 2003.