Chapter 1
Introduction

1.1 A Brief History of Quantum Mechanics

A Few Milestones in Quantum Mechanics

1900: Black body radiation law (Max Planck)
1905: Postulation of photons to explain photoelectric effect (Albert Einstein)
1909: Interference experiments (Geoffrey Ingram Taylor)
1913: Quantization of angular momentum of hydrogen (Niels Bohr)
1923: Compton effect (Arthur Holly Compton)
1924: Wave–particle duality extended to incorporate matter (Louis de Broglie)
1925: Matrices as basis for Quantum Mechanics (Werner Heisenberg)
1926: Probabilistic interpretation of the wavefunction (Max Born)
1926: Gilbert Lewis coined the word photon
1926: Wave equation to explain the hydrogen atom (Erwin Schrödinger)
1927: Uncertainty principle (Werner Heisenberg)
1927: Copenhagen interpretation (Niels Bohr)
1928: First solution of Quantum Mechanics explaining spin (Paul Dirac)
1930: Principles of Quantum Mechanics (Paul Dirac)
1930: Interference, how quantized light interacts with atoms (Enrico Fermi)
1932: Mathematical foundations of Quantum Mechanics (John von Neumann)
1935: EPR paradox (Einstein, Podolsky, and Rosen)
1950s: Theory of photon statistic and counting (Hanbury Brown, and Twiss)
1960s: Quantum theory of coherence (Glauber, Wolf, Sudarshan, and others)
1970: (early 1970s) Tunable lasers

G. Cariolaro, *Quantum Communications*, Signals and Communication Technology,
DOI 10.1007/978-3-319-15600-2_1

1.1.1 The Dawn

In the last decade of the nineteenth century Newton's mechanics, Maxwell's electromagnetic theory, and Boltzmann's statistical mechanics seemed capable of exhaustively explaining any relevant physical phenomenon. However, some phenomena, initially deemed as marginal, did not completely fit in the structure of these *classic* disciplines. It all began with the discoveries of a Physics student called **Max Planck** (1858–1947).[1] Planck's research was triggered by the study of the emission and absorption of light by physical bodies. At that time, the founding theory of radiation emission by a black body was based on classical electromagnetism. Applying this theory, the phenomenon was well explained for relatively low frequencies of the emitted radiation (visible or near infrared and downwards); however, for high frequencies (ultraviolet and upwards) classical theory would predict an infinite increase in the energy of the emitted radiation, which, as matter of fact, does not happen in reality. To overcome such a problem, Planck formulated the hypothesis that the radiating energy could only exist in the form of discrete quantities, or "packets", which he called **quanta**. To set the framework of Planck's problem, we must recall the previous research of the physicist **J.W. Strutt Lord Rayleigh** (1842–1919), who studied the radiation of the black body from a classical point of view, modeling it as a collection of electromagnetic oscillators, and considering the presence of the radiation at frequency ν as the consequence of the excitation of the oscillator at such frequency. With some contribution by **Sir James Hopwood Jeans** (1877–1946), he arrived at the formulation of the **Rayleigh-Jeans Law**, given by the expression

$$E(\nu) = \frac{8\pi k T \nu^4}{c^4} = \frac{8\pi k T}{\lambda^4}, \tag{1.1}$$

which gives the value $E(\nu)$ of energy density per frequency unit emitted by a black body at frequency ν. In (1.1) $k = 1.38\ 10^{-23}\mathrm{JK}^{-1}$ is Boltzmann's constant, T is the absolute temperature of the black body, c is the speed of light, and $\lambda = c/\nu$ is the wavelength. This law shows that the energy density irradiated by a black body increases linearly with temperature and with the fourth power of the frequency of the emitted radiation. Experimental measurements demonstrate that this law is perfectly adequate at low frequencies: in fact, it is well known that, with increasing temperature, the irradiated energy increases proportionally, at least up to the infrared. However, measurements carried out at higher frequencies, for example in the ultraviolet range, clearly show that the emitted energy values diverge considerably from those foreseen by the theory. In addition, from a careful analysis of Eq. (1.1), one can see that the expected result in this spectral interval has no physical meaning. In fact, this equation states that, with increasing frequency, energy density increases indefinitely. As a consequence, the equation asserts that the high-frequency oscillators (very low wavelength, corresponding to the ultraviolet radiation, to the X-rays, and to

[1] On December 14, 1900, Planck publishes his first paper on Quantum Theory in *Verh. Deut. Phys. Ges. 2,237–45.*

the γ-rays) should be excited even at room temperature. Such absurd result, which posits the emission of a large amount of energy in the high-frequency region of the electromagnetic spectrum, went under the name of *ultraviolet catastrophe*.

The solution of the problem was in fact due to Max Planck, who tackled it in mathematical terms. Instead of integrating the energies of the "elementary oscillators" (that is, in practice, of the electrons "oscillating" around the nucleus) considering them as continuous quantities, he performed a summation of the energies, hypothesizing that they could assume only discrete values, proportional to the characteristic oscillation frequency ν of the electrons, by an appropriate constant h

$$E = h\nu. \tag{1.2}$$

The relation discovered by Planck for the energy density per frequency unit of the black body turns out to be (*Planck's relation*)

$$E(\nu) = \frac{8\pi}{c^3} \frac{h\nu^3}{e^{h\nu/kT} - 1}$$

and it appears to be in perfect agreement with the experimental distribution for each temperature, assuming $h = 6.63\ 10^{-34}$ Js; h is known as *Planck's constant*.

Planck's theoretical discovery on quanta became accepted by the classical physicists only when **Albert Einstein** (1879–1955)[2] succeeded in explaining the photoelectric effect, speculating that light radiation was constituted by energy packets, subsequently called "photons". Einstein showed that, thanks to quanta, other physical phenomena could be explained, in addition to the black body emission proposed by Planck, and at that point the discrete nature of electromagnetic radiation became a fundamental and generally accepted concept.

Another problem that could not be explained by classical mechanics was the regularity of the emission spectrum of an atom, that is, the fact that it always appeared as formed by the same characteristic frequencies, independently of its origin and of possible excitation processes it had undergone, a fact that could not be convincingly explained by the model proposed by **Ernest Rutherford** (1871–1937) in 1911. The first one to address the problem in mathematical terms was **Niels Bohr** (1885–1962) in 1913. Bohr hypothesized that the lines of an atomic spectrum were originated by the transition of an electron between two discrete states of an atom. This theory correctly interpreted, for the first time, the emission and absorption properties of an atom of hydrogen.

The next step in the development of Quantum Mechanics was due to **Louis-Victor Pierre Raymond de Broglie**[3] (1892–1987), who extended to the particles with mass the *wave–particle duality* that had been evidenced for electromagnetic

[2] In 1905 he published on the *Annalen der Physik* three articles, the first on light quanta, the second on Brownian motion, which would definitely confirm the atomicity of matter, the third on the foundations of restricted relativity.

[3] After publishing a few papers, he developed in full form this original idea in his Ph.D. thesis (1924): *Recherches sur la théorie des quanta*.

radiations. Louis de Broglie surmised that not only would light, generally modeled as a wave, sometimes behave as a particle, but also electrons, usually modeled as particles, could at times behave as waves. De Broglie suggested that the key for the description of electrons in terms of wave–particle could be given by the relation

$$\lambda = \frac{h}{mv} \tag{1.3}$$

where λ is the wavelength of the wave associated to the electron, and m e v are, respectively, the mass and the velocity of the electron itself. For example, a wave is associated to an electron moving along a closed orbit around the atomic nucleus. In this particular case, the wave is stationary and its wavelength is linked to mass and velocity by relation (1.3).

We can say that de Broglie's contribution marks the end of the pioneering phase of Quantum Mechanics, whose various phenomena were examined and explained individually, without attempting to formulate a general theory.

1.1.2 The Maturity of Quantum Mechanics

Quantum Mechanics reached maturity in the 1920s and in the 1930s, moving from Quantum Theory to Quantum Mechanics, thanks to the work of Schrödinger, Heisenberg, Dirac, Pauli, and others.

Shortly after de Broglie's conjecture, almost simultaneously, Quantum Mechanics was presented by **Erwin Schrödinger** (1887–1961) and **Werner Heisenberg** (1902–1976).[4] Among the greatest physicists of the century, Schrödinger, stated the fundamental equation of Undulatory Mechanics, known nowadays as Schrödinger's equation

$$H\psi = E\,\psi, \tag{1.4}$$

where ψ is an eigenfunction describing the state of the system, H is an operator, called *Hamiltonian*, and E is the eigenvalue accounting for the system's energy.[5] This equation, stated for non relativistic energies, is the basis for the description of the various phenomena of molecular, atomic, and quantum nuclear physics.

Heisenberg, instead, introduced into Physics the uncertainty of physical entities. His *Uncertainty Principle*, in fact, asserts that it is impossible to know, simultaneously and exactly, couples of physical entities, like position and velocity of a particle. In essence, the more precisely we know the position of a particle, the less information we have on momentum, and vice versa, according to:

---

[4] In 1927, he published on *Zeitschrift fur Physik* his famous paper on the uncertainty principle, entitled: *Über den anschaulichen Inhalt der quanten theoretischen Kinematik und Mechanik.*

[5] Equation (1.4) is Schrödinger's time-independent equation, where ψ is an eigenfunction. Schrödinger's equation can also include the time to take into account system evolution.

$$\Delta x \, \Delta p \geq \frac{h}{4\pi}. \tag{1.5}$$

This principle is of general validity, but it is particularly appreciable at the atomic or subatomic scale.

The statistical laws related to the concept of probability became a reality: uncertainty is a fundamental fact, and the relations connected to the principle evidence an insuperable limit to our knowledge of nature.

> The more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa. (Heisenberg, *Uncertainty Paper*, 1927)

To conclude this historical note, we find it appropriate to mention the fundamental contribution, albeit indirect, given by the mathematician **David Hilbert** (1862–1943), since the modern version of Quantum Mechanics requires a Hilbert space as mathematical context.

1.2 Revolutionary Concepts of Quantum Mechanics

In describing reality, Quantum Mechanics presents a few concepts that appear revolutionary with respect to Classical Physics, and even seem in contrast with common sense. These concepts will be briefly summarized below.

1.2.1 Randomness

The fundamental difference between *Classical Mechanics* and Quantum Mechanics lies in the fact that, while Classical Mechanics is a deterministic theory, Quantum Mechanics envisages and formalizes indeterminate aspects of reality.

In the mathematical models of Classical Mechanics, once the initial state of a system is known, and so are the forces acting on it, the system's evolution is perfectly predictable and *deterministically measurable*. Resort to probabilistic models is then justified exclusively by the need to account for lack of information on entities characterizing the system.

In Quantum Mechanics, instead, randomness is an intrinsic element of the theory. In fact, it states that the measurements performed on a system, starting from exactly the same initial conditions, may produce different results. This is not due to measurement imprecision, but rather to the fact that the result of any measurement is intrinsically random and must be dealt with the Theory of Probability.

Randomness in Quantum Mechanics is expressed by the fact that the measure of an entity is described by a complex function (the *wave function*), whose squared modulus gives the probability density of the result (intended as a random variable).

1.2.2 Indeterminacy

Another peculiar aspect of Quantum Mechanics is that in any experiment the measurement procedure interferes with the system, altering it. In Classical Physics there is no such problem, because measurement errors can be acknowledged and estimated, but the measurement itself, if accurately performed, does not modify the system. In Quantum Mechanics this is not possible any more, because, as established by the above-mentioned Heisenberg's principle, the accuracy in the knowledge of one quantity (e.g., the position of a particle) inhibits an equal accuracy in the knowledge of another quantity (e.g., velocity). This should be interpreted not only in the sense that two quantities cannot be measured simultaneously with an arbitrary degree of accuracy. As we shall see, they are conceptually undetermined with an uncertainty whose lower bound is given by Heisenberg's inequality.

1.2.3 Complementarity

The above example of position and momentum is a typical case of *conjugate* or *complementary* entities. This corresponds to a distinctive feature of Quantum Mechanics, whose fundamental example is the case of the wave function $\psi(x)$ of position and the wave function of momentum $\tilde{\psi}(p)$: there exists no wave function $\psi(x, p)$ providing a joint statistical description of both entities. The same applies to other couples of complementary variables.

1.2.4 Quantization

Differently from Classical Mechanics, in Quantum Mechanics, the states of a quantum system can only correspond to discrete energy levels. In other words, the granular nature of matter can be extended to energy.

This fact is in good agreement with the requirements of telecommunications, where digital information is represented by quantities that can assume a finite number of values.

1.2.5 Linearity and Superposition

Paradoxically, the states of a quantum system, although characterized by discrete energy levels, have a continuous nature, in the sense that wave functions are continuous functions. In addition, if $\psi(x)$ and $\phi(x)$ are two possible wave functions, also

their linear combination $a\,\psi(x) + b\,\phi(x)$, with a and b complex numbers, is still a wave function.

Linearity is then another feature of Quantum Mechanics. The algebraic structure in which its models are represented is constituted by Hilbert spaces, that are linear spaces, and Schrödinger's equation, which governs the evolution of the state, is a linear differential equation.

Linearity and superposition, very simple mathematical concepts, are actually the basis of *Quantum Information and Computation* and have practical consequences of great importance.

1.2.6 Entanglement

The *entanglement* is a phenomenon of Quantum Mechanics in blatant contradiction with physical intuition, as Classical Physics would suggest, to the point that its meaning itself is still open to discussion.

Two particles emitted from the same source, when in the entanglement condition, show strictly correlated characteristics that are preserved even when they move away from each other. And when the state of one of them is measured, the state of the other changes immediately with a "spooky action at a distance," in total contrast with common sense.

1.3 Quantum Information

The natural field of application of Quantum Mechanics is within Physics. However, in the last 20 years (starting from the 1980s) it has exceptionally expanded into the area of Information science and technologies. The main ideas come from the *Postulates* of Quantum Mechanics, which in the last 100 years have never been disproved, and, after a substantial reformulation, envisage extremely innovative applications, like the *quantum computer*, *quantum coding*, *quantum cryptography*, and *quantum communications*. Many of these innovations, consequences of the Postulates, have already had experimental verification and are the subject of a frenzied research activity.

It is worthwhile to introduce these innovations by adding some more historical notes.

1.3.1 The Discovery of Laser and the Theory of Quantum TLC

In the 1960s, after the discovery of laser, **Ronny J. Glauber** of Harvard University formulated the quantum theory of optical coherence [1, 2]. The possibility of producing *coherent* light led Helstrom [3], and other scientists from the Massachusetts

Institute of Technology (MIT), to formulate the Theory of Quantum Telecommunications, that is, a theory where the information is related to quantum states and the analysis and design is based on the rules of Quantum Mechanics. This theory, which we will develop in Chaps. 7 and 8, aimed to realize optical transmissions in free air, as optical fibers were not yet available at that time; unfortunately it did not generate appreciable applications, because the technology was not mature enough, and mostly because the appearance of optical fibers, with their enormous throughput, obscured the interest toward quantum telecommunications. Nevertheless, these pioneering investigations may be considered the beginning of Quantum Information.

Recently, the QTLCs (Quantum Telecommunications) have been vigorously revived at the **Jet Propulsion Laboratory** (JPL) of NASA, where the Deep Space Network is in operation, and, in fact, it is in the area of deep space transmissions that Quantum Communications are expected to play a crucial role. We are dealing, for the time being, with niche applications, but it should be remembered that other fields, like the application of error-correction codes, started precisely at JPL, and they led to fully fledged applications many years later.

1.3.2 Quantum Information Based on Discrete Quantum Variables. The Qubit

To understand the motivations that, in the early 1980s, led to studying information in the context of Quantum Mechanics, we can start from *Moore's Law* of electronic circuit technology. As we know, this law, stated by Gordon Moore in 1965, asserts that the complexity of electronic circuits (chips), at equal size, doubles approximately every18 months, and this prediction has been substantially confirmed in the last 50 years. However, it assumes an indefinite reduction in the size of components, down to the limit of atomic dimensions, where quantum effects become predominant. At this point, a natural development is to try to reformulate Information Theory in the framework of Quantum Mechanics. Following this line of thought, **Benioff**, **Manin**, and **Feynman** postulated the idea of a Quantum Computer, for the simulation of Quantum Systems. Differently from the classical computer, which, as is well known, is a power-consuming device, the quantum computer, in theory, does not require power consumption (this theoretical possibility had already been demonstrated by **Charles Bennett** within IBM). Subsequently, in 1985 **David Deutsch** proved that a Quantum Computer can naturally operate in parallel mode (quantum parallelism), in the sense that it makes it possible to evaluate any function $f(x)$, for every value of x, in a single step. With this parallelism, the theoretical superiority of the quantum computer with respect to the conventional one was demonstrated.

Still around those times, **Charles Bennett** and **Gilles Brassard** explored the possibility of secure information transmission based on the laws of Quantum Mechanics. The principle is related to *quantum measurements* (Postulate 3 of Quantum Mechanics) according to which, if the information is intercepted, the receiver is automatically

and securely alerted. This marks the birth of *Quantum Cryptography*. On the other hand, in 1991 **Arthur Eckert** proposes another form of secure transmission based on entanglement, a phenomenon predicted by Postulate 4 of Quantum Mechanics.

In any case, Quantum Cryptography, as a *quantum key distribution*, is one of the most concrete applications of Quantum Mechanics in the information area, in that it already shows significant implementations.

The phenomenon of entanglement, typical of quantum mechanics, and totally unforeseen by the classical theory, gave origin to another research thread: *Superdense Coding*, according to which, by sending a single bit of quantum information (qubit), two bits of classical information can be transmitted. This originated a very promising new field, *Quantum Coding*, steadily growing, as witnessed by the numerous papers appearing on the IEEE Trans. on Information Theory. It should be noticed that, in this context, Shannon's Information Theory is being reviewed, giving way to *Quantum Information Theory*. Superdense Coding was invented by Bennett and Wiesner [4] and experimentally implemented by Mattle et al. [5].

Bennett et al. [6] found another use of entanglement, *quantum teleportation*, in which separate experiments sharing two halves of entangled systems can make use of entanglement to transfer a quantum state from one to another using only classical communications. Teleportation was later experimentally realized by Boschi et al. [7] using optical techniques and by Bouwmeester et al. [8] using photon polarization.

Going back to Quantum Computing, we must mention the milestone achieved by **Peter Shor** of AT&T in 1994, who demonstrated that a Quantum Computer can decompose an integer number into prime factors with polynomial complexity, whereas it is conjectured that the classic computer requires exponential complexity. It is an alarming discovery, because the majority of current cryptographic security systems are based on the (exponential) difficulty of prime factor decomposition. On the other hand, this confirms the importance of investing in ideas and resources on Quantum Cryptography.

The above history (1990–2010) on quantum computers, quantum cryptography, and quantum teleportation refers to the manipulation of individual quanta of information, known as quantum bits or *qubits*; in other words, based on *discrete* quantum variables.

1.3.3 Quantum Information Based on Continuous Quantum Variables

Very recently it was realized that the use of *continuous* quantum variables, instead of qubits, represents a powerful alternative to quantum information processing [9]. In this context, on the theoretical side, simple analytical tools are available (Gaussian states, Gaussian operators, and Gaussian measurements) and, on the practical side, the corresponding laboratory implementation is readily available. Hence, the continuous state approach opens the way to a variety of tasks and applications, in competition

with the discrete state approach. Furthermore, these new possibilities provide a new challenge to the implementation of Quantum Communications systems.

In conclusion, Quantum Information comes in two forms, discrete and continuous. From a historic viewpoint, the continuous form was developed in pioneering works for Quantum Communications systems (1970) and the discrete form in the last two decades, but now continuous and discrete forms are in competition.

1.4 Content of the Book

This book is a collection of ideas for an "educational experiment" on the teaching of Quantum Information and particularly Quantum Telecommunications to students of the Departments of Engineering and Physics, hence with the twofold objective of opening a cross-disciplinary field of study and possibly providing a common background for scientific collaboration.

Part I: Fundamentals

Chapter 2: Hilbert Spaces

This chapter contains the mathematical foundations required to understand Quantum Mechanics, which develops over Hilbert spaces on complex numbers. Many notions (vector spaces, and inner product vector spaces) are already known to students, others, like the spectral decomposition of a Hermitian operator, are less known and represent a fundamental subject in Quantum Measurements.

In any case, the collection provides a run-through and a symbolism acquisition, useful to come to grips with the subsequent subjects.

Chapter 3: Elements of Quantum Mechanics

The formulation of these elements is presented following in sequence the four *Postulates* of Quantum Mechanics. The development is partly parallel to Nielsen and Chuang's book [10]. However, herein to the four postulates are given different emphasis; in particular, Postulate 3 on Quantum Measurements is developed in great detail, as it represents the most interesting part with respect to Quantum Communications.

Part II: Quantum Communications

Chapter 4: Introduction to Quantum Communications

The general foundations of telecommunications systems are introduced and the difference between Classical and Quantum Communications systems is explained.

In the second part of the chapter we introduce the foundations of *optical classical communications*, which is the necessary prologue to *optical quantum communications* developed in the subsequent chapters. The mathematical framework is given by Poisson processes, and more specifically by doubly stochastic Poisson processes.

Chapter 5: Quantum Decision Theory: Analysis and Optimization

Only data transmission is considered, starting from the description and analysis of a general scheme, shown in Fig. 1.1. For a general K-ary system, the rules are given to calculate the transition probabilities and the error probabilities, obviously in terms of quantum parameters. Then we develop, in a fully general way, the best choice of quantum measurements that minimize the error probability (optimization).

Two important topics are also introduced: the geometrically uniform symmetry (GUS) of a constellation of states and the compression of quantum states.

Chapter 6: Quantum Decision Theory: Suboptimization

Optimization in quantum decision is very difficult, and exact solutions are only known in few cases. To overcome such a difficulty *suboptimization* is considered. In quantum communications the most important suboptimal decision is called square-root measurement (SRM), because its solution is based on the square root of an operator. Particularly attractive is the SRM combined with the GUS of quantum states.

Chapter 7: Quantum Communications Systems

In this chapter, the general Quantum Decision Theory is applied to systems in which digital information is carried by the monochromatic radiation produced by a laser (*coherent states*). As a preliminary, *classic* optical telecommunications systems are outlined in order to provide the background and the inspiration for the transition from classic to *quantum* optical telecommunication systems. The quantum version differs mainly at the receiver, where the analysis and the design are carried out using the Postulates of Quantum Mechanics.

Then the theory is explicitly applied to the more popular systems, like OOK (on off keying), PSK (phase shift keying), PPM (pulse position modulation), and QAM (quadrature amplitude modulation). Anyhow, we shall eventually demonstrate the *net gain in terms of performance that can be obtained by the quantum versions compared to the classic schemes*.

Chapter 8: Quantum Communications Systems in the Presence of Thermal Noise

In the analysis of Chap. 7, the background noise (or thermal noise) is neglected, and the uncertainty of the result (the message) is only due to the randomness arising in

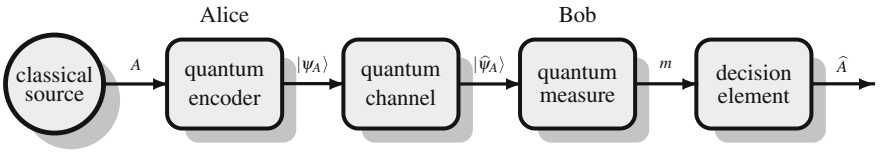

Fig. 1.1 Quantum Communications system for digital transmission. A symbol to be transmitted, $|\psi_A\rangle$ quantum state prepared by Alice, $|\widehat{\psi}_A\rangle$ received quantum state, m outcome of the quantum measurement, and $\widehat{A}$ decided symbol

quantum measurements. In this chapter, the analysis of the main quantum transmission systems, developed in Chap. 7, takes into account background noise, which is always present in real-world systems.

Chapter 9: Implementation of Quantum Communications Systems

While Quantum Communications theory is reaching a steady state, the implementation of the corresponding systems is still at an early stage. The chapter describes the implementations realized so far around the world, a few promising ideas, and some open problems.

Part III: Quantum Information

Chapter 10: Introduction to Quantum Information

Quantum Information exhibits two forms, discrete and continuous. Discrete quantum information is based on *discrete variables*, the best known example of which is the quantum bit or, briefly, *qubit*. Continuous quantum information is based on *continuous variables*, the best known example of which is provided by the quantized harmonic oscillator, which represents the fundamental tool in quantum optics and is the basis for the introduction of coherent states and more generally of Gaussian states.

An important remark is that most of the operations in quantum information processing can be carried out both with discrete and continuous variables (this last possibility is a quite recent discovery).

Chapter 11: Fundamentals of Quantum Continuous Variables

In Quantum Mechanics formulation of Chaps. 2 and 3 we have considered some fundamentals, as bases, eigendecompositions, measurements, and operators, in the *discrete* case. Specifically, we assumed the bases consisting of finite or enumerable sets of vectors, the operator eigendecompositions having a finite or enumerable spectrum, and quantum measurements having a finite set (alphabet) of possible outcomes. This formulation was sufficient because in the subsequent chapters we limit ourselves to the development of *digital* Quantum Communications.

In this chapter, for a full development of Quantum Information, we extend the above fundamentals to the continuous case, where the sets become a continuum. A particular relevance is given to Gaussian states and Gaussian transformations.

Chapter 12: Quantum Information Theory

Information Theory was born in the field of Telecommunication in 1948 with the revolutionary ideas developed by Shannon [11]. Its purpose is mainly: (1) to define *information* mathematically and quantitatively, (2) to represent information in an efficient way (data compression) for storage and transmission, and (3) to ensure information protection (encoding) in the presence of noise and other impairments. Recently, with the interest in quantum information processing, Information Theory was extended to Quantum Mechanics. Of course, Quantum Information Theory, is based on quantum mechanical principles and in particular on its intriguing phenomena, like entanglement.

The chapter provides an overview of Quantum Information Theory starting from Classical Information Theory, which represents a necessary preliminary. Thus, each of the three items listed above are developed in the framework of Quantum Mechanics, starting from the classical case.

Chapter 13: Applications of Quantum Information

The list of topics that will be developed in this chapter is:

- quantum random number generation,
- quantum key distribution,
- teleportation,

considered with both discrete and continuous variables.

1.5 Suggested Paths

As mentioned in the Preface, the book is meant to address readers from Physics and Telecommunications, both graduate students and researchers, providing that they are familiar with Linear Vector Spaces and Probability Theory. In order to account for the different backgrounds and academic levels, two different paths through the book are suggested, as illustrated in Fig. 1.2, with the indication of the difficulties[6] probably encountered in each chapter.

Graduate students should begin by checking their mathematical background while studying carefully Chap. 2, and solving some specific exercises to get familiarity and confidence with the topic. In the study of Part III, they can skip, at least at the first reading, the description of quantum systems in terms of *density operators*. In fact, the formulation in terms of *pure states* is adequate to tackle the essence of Quantum Communications and the comparison with classic optical systems. Therefore Chap. 8 can be completely omitted (the content of this chapter may be regarded as a very advanced topic). Once completed the comprehension of Part II, students will have reached a reasonable and adequate mastering level on the subject. But they might as well consider moving on to the more advanced topics of Part III, if they have enough time and spirit of inquiry.

Researchers could avoid the study of Part I (or they could quickly browse through it to acquire the symbolism and references for the next chapter). They will have to study simultaneously the developments based on pure-state and density-operator representations. In particular, Chap. 8, which is very advanced, may offer them stimulating hints for original research. Eventually, they will complete their path with the last three chapters.

[6] Of course, the difficulty scale strongly depends on the preparation and on the personality of the reader.

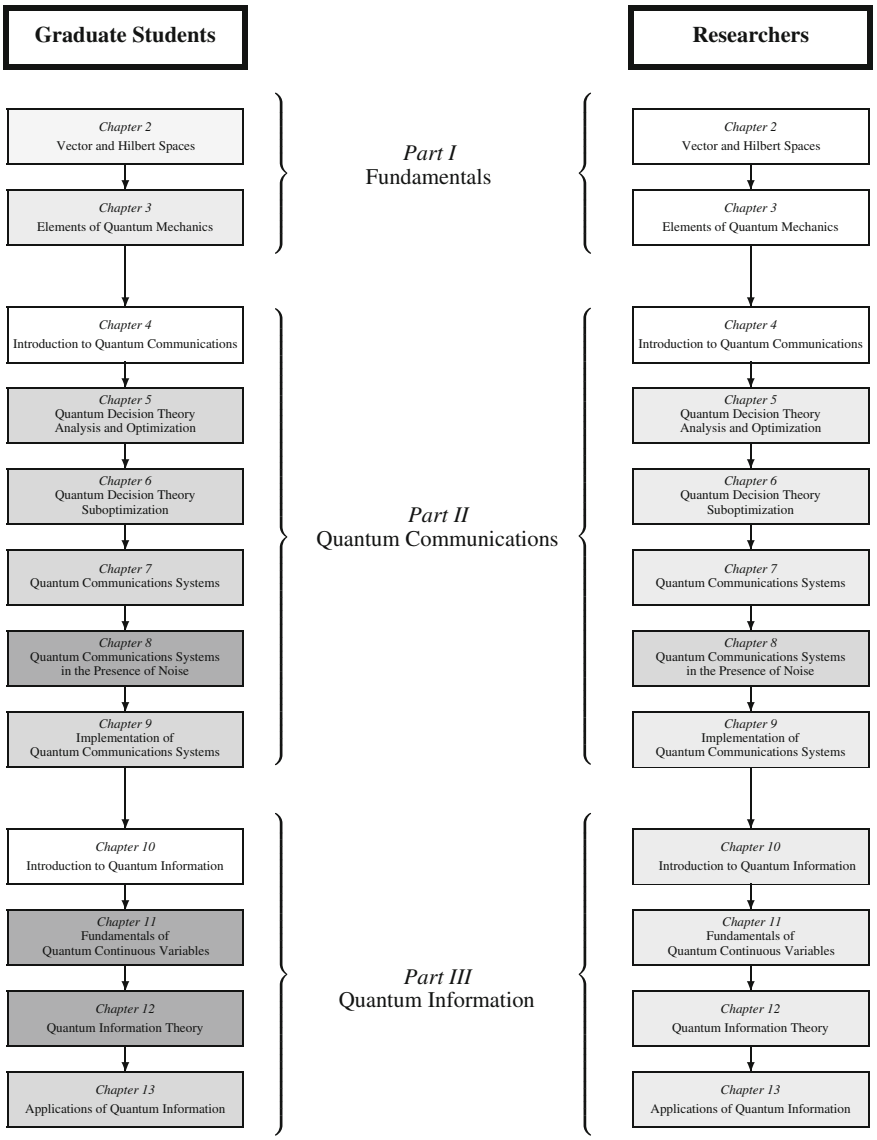

Fig. 1.2 The two suggested paths with the difficulties indicated by a gray level in the blocks

1.6 Conventions on Notation

Sections of advanced topics that can be omitted at the first reading are marked by ⇓. Problems are marked by asterisks indicating difficulty (* = easy, ** = medium, *** = difficult). Sections and problems marked with the symbol ▽ require notions that are developed further on.

Throughout the book, notations are explicitly specified at the first use and are frequently recalled. Matrices and operators are denoted by uppercase letters, e.g., A, Ψ. For quantum states, Dirac's notation *bra* and *ket* is used, as $\langle x|$ and $|x\rangle$.

List of Symbols

$:=$	Equal by definition
$\otimes$	Tensor product
$\oplus$	Direct sum
$\mathrm{Tr}[\cdot]$	Trace
$\mathrm{Tr}_A[\cdot]$	Trace over the subsystem A
$\mathrm{E}[\cdot]$	Expectation (of a random variable)
$\mathrm{P}[\cdot]$	Probability (of an event)
$q_i := \mathrm{P}[A = i]$	Source probabilities
$p_c(j\|i)$ or $p(j\|i)$	Transition probabilities
$\mathcal{V}$	Vector space
$\mathcal{H}$	Hilbert space
$\mathbb{Z}$	Set of integer numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers
$\mathcal{A}$	Alphabet (source)
$\mathcal{M}$	Alphabet of a quantum measurement
$\|x\rangle$	Ket
$\langle x\|$	Bra
$\langle x\|y\rangle$	Inner product of vectors $\|x\rangle$ and $\|y\rangle$
$\|x\rangle\langle y\|$	Outer product of vectors $\|x\rangle$ and $\|y\rangle$
$\|x\rangle \perp \|y\rangle$	$\|x\rangle$ and $\|y\rangle$ are orthogonal ($\langle x\|y\rangle = 0$)
$\|\|x\|\|$	Norm of vector $\|x\rangle$
$[x_{ij}]$	Matrix with entries x_{ij}
$[A, B]$, $\{A, B\}$	Commutator and anticommutator of operators A and B
$I_{\mathcal{H}}$	Identity operator of $\mathcal{H}$
I_n	Identity matrix of size n
$\|z\|$	Absolute value of complex number z
$\|\mathcal{A}\|$	Dimension of set $\mathcal{A}$
z^*	Conjugate of complex number z
A^*	Adjoint of operator A or conjugate transpose of matrix A
A^{T}	Transpose of matrix A
a, a^*	Annihilator and creation operators
q, p	Quadrature operators
δ_{ij}	Kronecker's symbol
$\delta(x)$	Dirac delta function
h	Planck's constant

$\hbar := h/(2\pi)$	Reduced Planck's constant
k	Boltzmann's constant
$W_N := \mathrm{e}^{\mathrm{i}\,2\pi/N}$	Nth radix of unity
$W_{[N]}$	DFT matrix of order N

- for the list of symbols on Continuous Variables, see the beginning of Chap. 11
- for the list of symbols on Information Theory, see the beginning of Chap. 12

List of Acronyms

A/D	Analog-to-digital
D/A	Digital-to-analog
CFT	Complex Fourier transform
CSP	Convex semidefinite programming
DFT	Discrete Fourier transform
EID	Eigendecomposition
EPR	Einstein-Podolsky-Rosen
FT	Fourier transform
GUS	Geometrically uniform symmetry
IID	Independent Identically Distributed
LMI	Linear matrix inequality
OOK	On–off keying
POVM	Positive Operator-Valued Measurements
PSD	Positive semidefinite
PSK	Phase shift keying
BPSK	Binary PSK
PPM	Pulse position modulation
QAM	Quadrature amplitude modulation
QKD	Quantum Key Distribution
SNR	Signal to noise ratio
SRM	Square root measurement
SVD	Singular-value decomposition
TLC	Telecommunications

References

1. K.E. Cahill, R.J. Glauber, Ordered expansions in Boson amplitude operators. Phys. Rev. **177**, 1857–1881 (1969)
2. R.J. Glauber, The quantum theory of optical coherence. Phys. Rev. **130**, 2529–2539 (1963)
3. C.W. Helstrom, J.W.S. Liu, J.P. Gordon, Quantum-mechanical communication theory. Proc. IEEE **58**(10), 1578–1598 (1970)
4. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Experimental quantum cryptography. J. Cryptol. **5**(1), 3–28 (1992)
5. K. Mattle, H. Weinfurter, P.G. Kwiat, A. Zeilinger, Dense coding in experimental quantum communication. Phys. Rev. Lett. **76**, 4656–4659 (1996)

6. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
7. D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **80**, 1121–1125 (1998)
8. D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Experimental quantum teleportation. Nature **390**, 575–579 (1997)
9. C. Weedbrook, S. Pirandola, R. Garcí a Patrón, N.J. Cerf, T.C. Ralph, J.H. Shapiro, S. Lloyd, Gaussian quantum information. Rev. Mod. Phys. **84**, 621–669 (2012)
10. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)
11. C.E. Shannon, A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423 (1948)