CAMBRIDGE

国外信息科学与技术优秀图书系列 电子学与通信技术

经典与量子信息论

Classical and Quantum Information Theory

（英文版）

〔法〕 Emmanuel Desurvire 著

科学出版社

国外信息科学与技术优秀图书系列

经典与量子信息论

（英文版）

Classical and Quantum Information Theory

〔法〕 Emmanuel Desurvire 著

科学出版社
北 京

图字：01-2012-4535

内容简介

本书完整地叙述了经典信息论和量子信息论，首先介绍了香农熵的基本概念和各种应用，然后介绍了量子信息和量子计算的核心特点。本书从经典信息论和量子信息论的角度，介绍了编码、压缩、纠错、加密和信道容量等内容，采用非正式但科学的精确方法，为读者提供了理解量子门和电路的知识。

本书自始至终都在向读者介绍重要的结论，而不是让读者迷失在数学推导的细节中，并且配有大量的实践案例和章后习题，适合电子、通信、计算机等专业的研究生和科研人员学习参考。

Classical and Quantum Information Theory, 0101 (978-0-521-88171-5) by Emmanuel Desurvire first published by Cambridge University Press 2009.

图书在版编目(CIP)数据

经典与量子信息论 = Classical and quantum information theory : 英文 / (法) 德叙维勒 (Desurvire,E.) 著. —北京：科学出版社，2013.1
(国外信息科学与技术优秀图书系列)
ISBN 978-7-03-036510-1
Ⅰ. ①经… Ⅱ. ①德… Ⅲ. ①信息论-英文 Ⅳ.TN911.2
中国版本图书馆 CIP 数据核字(2013)第 012677 号

责任编辑：朱雪玲 / 责任校对：李 影 / 责任印制：张 倩 / 封面设计：刘可红

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2013 年 1 月第 一 版 开本：787×1092 1/16
2013 年 1 月第一次印刷 印张：44 1/2
字数：712 000

定价：158.00 元

（如有印装质量问题，我社负责调换）

推荐序

《经典与量子信息论》是一本很有特色的信息论专著，旨在面向那些未受过系统的量子力学和信息论专业训练的读者，尤其是通信领域的科技工作者。全书深入浅出地介绍了经典信息论和量子信息论的基本原理、主要内容和应用场景。

本书在结构上分为两部分，分别介绍经典信息论和量子信息论。其中，量子信息论正是在Shannon经典信息论基础上，藉由量子力学对人类带来的革命性变化而发展起来的。介绍经典信息论的第一部分包括第1~14章：第1、2章介绍一些基本的概率论知识；第3章引入信息度量的原始想法；第4~6章逐步深化为信息熵的概念；第7章用Komologorov复杂度进一步阐释信息熵；第8~10章研究编码问题；第11章考虑纠错方法；第12~14章讲述信道和信道容量的相关问题。第二部分介绍了量子信息论：第15章探讨计算可逆性问题；第16章介绍量子比特和量子逻辑门操作；第17章概述量子测量操作；第18章介绍量子纠缠；第19~20章给出了常见的量子算法；第21~24章把第8~14章中经典信息论的相关结论逐一放在量子情形下重新检视；最后的第25章介绍了通信的安全性，深入探讨了经典和量子情形下的保密通信问题。

本书的作者Emmanuel Desurvire博士，现任法国THALES公司物理研发组主任，毕业于法国尼斯大学，曾先后供职于美国斯坦福大学、贝尔实验室、哥伦比亚大学和法国阿尔卡特公司，是光与量子通信领域的著名专家，有超过25年的丰富研究经历，拥有超过200项技术发明和30多项专利，在掺铒光纤放大器（EDFA）和高速波分复用（WDM）光通信等方向做出过杰出贡献，并因此获得了一系列学术奖励，包括1994年国际光学学会（ICO）年度奖、1998年Benjamin Franklin工程奖章、2005年William Streifer科技进步奖、2007年美国电气和电子工程师协会（IEEE） John Tyndall奖和年度工程师奖，以及由法国科学院颁发的法国电信奖，2008年千禧技术进步奖等。

本书的最大特色在于这是一本面向通信领域科技工作者的信息论专著，作者在全书的正文主体内容中有意回避了过于艰深、繁复的数学推导和物理理论，将其放在了附录、脚注和相应的引文扩展中，代之以大量翔实、清楚的通信领域的应用实例，用这些例子清晰准确、深入浅出地勾勒出经典和量子信息论的基本概念、整体思路、主要内容和一般方法，同时提供了大量不同难度的习题。对于那些对信息论尤其是量子信息论感兴趣、却又苦于一般信息论文献中过多的数学和物理技巧的读者，包括通信领域的工作者、一般工程技术人员和从事科技管理领域的工作者等来说，这本书是他们深入学习理解信息论的不可多得的优秀教材；对于从事经典和量子信息相关领域学习和研究的读者，这也是一本值得一读的参考书。

郭　弘

二〇一二年六月于燕园

Foreword

It is always a great opportunity and pleasure for a professor to introduce a new textbook. This one is especially unusual, in a sense that, first of all, it concerns two fields, namely, classical and quantum information theories, which are rarely taught altogether with the same reach and depth. Second, as its subtitle indicates, this textbook primarily addresses the telecom scientist. Being myself a quantum-mechanics teacher but not being conversant with the current Telecoms paradigm and its community expectations, the task of introducing such a textbook is quite a challenge. Furthermore, both subjects in information theory can be regarded by physicists and engineers from all horizons, including in telecoms, as essentially academic in scope and rather difficult to reconcile in their applications. How then do we proceed from there?

I shall state, firsthand, that there is no need to convince the reader (telecom or physicist or both) about the benefits of Shannon's classical theory. Generally unbeknown to millions of telecom and computer users, Shannon's principles pervade all applications concerning data storage and computer files, digital music and video, wireline and wireless broadband communications altogether. The point here is that classical information theory is not only a must to know from any academic standpoint; it is also a key to understanding the mathematical principles underlying our information society.

Shannon's theory being reputed for its completeness and societal impact, the telecom engineer (and physicist within!) may, therefore, wonder about the benefits of quantum mechanics (QM), when it comes to *information*. Do we really need a quantum information theory (QIT), considering? What novel concepts may be hiding in there, really, that we should be aware of? Is quantum information theory a real field with any engineering worth and perspectives to shape the future, or some kind of fashionable, academic fantasy?

The answer to the above questions first comes from realizing the no-less phenomenal impact of *quantum physics* in modern life. As of today, indeed, there is an amazing catalog of paradigms, inventions, applications, that have been derived from the quantum physics of the early twentieth century. Suffice it to mention the *laser*, whose extraordinary diversity of applications (global communications, data storage, reprography, imaging, machining, robotics, surgery, energy, security, aerospace, defense . . .) has truly revolutionized our society and – already – information society. As basic or innocuous as it may now seem to anyone, the laser invention yet remains a quantum physics jewel, a man-made wonder, which finds no explanation outside quantum mechanics principles. How did all this happen?

Following some 20 years of experimental facts, intuitions and hypotheses, and first foundations, by mind giants, such as Planck, Einstein, or Bohr, the structure of quantum mechanics was finally laid down within a pretty short period of time (1925–1927). At this time, the actual fathers of this revolutionary "worldview" formalism, e.g., de Broglie, Heisenberg, Schrödinger, or Dirac, could certainly not foresee that future armies of physicists and engineers would use quantum mechanics as an "Everest base camp" to conquer many higher summits of knowledge and breakthroughs.

There is practically no field of physics and advanced engineering that has not been revolutionized from top to bottom by quantum mechanics. Nuclear and particle physicists used quantum mechanics principles to foresee (and then discover experimentally) the existence of new elementary particles, thus lifting some of the microscopic world mysteries. Astrophysics and cosmology were also completely rejuvenated as quantum mechanics formalism proposed explanations for new macroscopic objects, such as white dwarfs or supernovae. Black body emission, one of the earliest experimental evidences of the very origin of quantum physics, was also found to explain the electromagnetic signature of the background of our Universe, telling us about the history of the Big Bang. The discipline where quantum mechanics had more impact on today's life was, however – by and large – solid-state physics. Quantum theory led to the understanding of how electrons and nucleons are organized in solids, how this microscopic world can evolve, interact with light or X-rays, transport heat, respond to magnetic fields, or self-organize at atomic scales. Nowadays, quantum chemistry explores the energy levels of electrons in complex molecules, and explains its spectroscopic properties in full intimacy. Mechanical, thermal, electric, magnetic, and optical properties of matter were first understood and then engineered. In the second half of the last century, transistors, storage disks (magnetic and optical), laser diodes, integrated semiconductor circuits and processors were developed according to an exponential growth pattern. Computers, telecommunication networks, and cellular phones changed everyone's life. All sectors of human activity were deeply influenced by the above technologies. Globalization and a booming of economy were observed during these decades. Neither a physicist, nor an economist, nor the last mad sci-fi novel writer, could have foreseen, one century ago, such a renewal of knowledge, of production means, and of global information sharing. This consideration illustrates how difficult it is to anticipate the future of mankind, since major changes can originate from the most basic or innocuous academic discoveries.

In spite of the difficulty of safe predictions, it is the unwritten duty of a physicist to try to probe this dark matter: the future. While quantum mechanics were revealed to be phenomenally beneficial to humankind, some physicists believe today that all this history is nothing but a first, inaugural, chapter. The first chapter would have "only" consisted of rethinking our world and engineering by introducing a first class of quantum ingredients: quantification of energy or momentum, wave functions, measurement probabilities, spin, quarks . . . Alain Aspect from France's Institut d'Optique, for example, envisions a "second revolution" of quantum mechanics. This second revolution paradigm will move the perspective one step further thanks to the ambitious introduction of a new stage of *complexity*. A way to approach such a complexity is *entanglement*, as I shall further explain.

Entanglement, which is the key to understanding the second quantum mechanics paradigm, is, in fact, an old concept that resurfaced only recently. Although entanglement was questioned by the famous 1935 joint paper by Einstein, Podolski, and Rosen,[1] it became clear over recent years that the matter represented far more than an academic discussion, and, furthermore, that it offered new perspectives. What is entanglement? This property concerns a group of particles that cannot be described separately, despite their physical separation or difference. A classical view of entanglement is provided by the picture of two magic dice, which always show up the same face. You may roll the pair of dice at random as many times as wished, but you will get the same result as with any single die, namely, a probability of 1/6 each to show up any spot patterns between 1 and 6, but with a strange property: the same random result is obtained by the two dice altogether. If one die comes out with six spots, so does the other one. Although this phenomenon of entanglement has no equivalent in the classical world as we normally experience it, it becomes real and tangible at the atomic scale. And unbeknown to large and even scientifically cultivated audiences, physicists have been playing with entanglement for about 20 years.

By means of increasingly sophisticated tools making it possible to manipulate single atoms, electrons, or photons, physicists are now beginning, literally, to "engineer" entangled states of matter. The Holy Grail they are after is building a practical toolbox for quantum entanglement. It is not clear at present which approach may show efficient, resilient, and environment-insensitive entanglement, while at the same time remaining "observable" and, furthermore, lending itself to external manipulation. To darken the picture, it is not at all clear either what could be the maximum size of an entangled system. Such questions come close to the actual definition of the boundary between the quantum and classical worlds, as emphasized by the famous *Schrödinger's cat paradox*. We may find ourselves in a situation similar to that of solid-state physics after World War II: quantum physics and many solid-state physics concepts were duly established, but the transistor remained yet to be invented. To the same extent that the revolutionary concepts of electronic wave functions, band theory, and conductivity led to the development of modern electronics and computers, the concept of entanglement, which stands at the core of quantum information, is now waiting for a revolutionary outcome. The parallel evolution between the different constitutive elements of entangled systems indeed offers huge opportunities to build radically new computing machines, with unprecedented characteristics and performance.

What does entanglement have to do with *complexity*? Whereas basic mechanics laws can predict the trajectory of a ball, the oscillation period of a pendulum, the lift of a plane, complexity characterizes systems where the overall properties cannot be derived from that of the constituent subsystems. For the philosopher Edgar Morin, it is not the number of the components that defines the complexity of any system. More components certainly call for more computing power to calculate the system's behavior, but the problem remains tractable in polynomial time (e.g., quadratic in the number of components): it

---

[1] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, **47** (1935), 777–80.

is referred to as a "P" problem. Complexity is another story: "complex" has a different meaning here from "complicated." It is, rather, the intimate nature of the interaction between the different components (including, for instance, recursion) that governs the emergence of novel types and classes of macroscopic behavior. Complex systems show properties that are not predictable from the single analysis of their constitutive elements, just as the properties of entangled particles cannot be understood from the simple inference of single particule behaviors.

In the last decades, complex systems have caused many developments in fields as varied as physics, astrophysics, chemistry, and biology. New mathematical tools, chaos, nonlinear physics, have been introduced. From the dynamics of sand dunes to schools of fishes, from ferrofluids to traffic jams, complexity never results from a simple extrapolation of classical individual behaviors. Hence, the challenge of understanding and harnessing entanglement is the possibility of extending the perspectives of quantum mechanics in the same way that macroscopic physics was renewed by the introduction of complexity. *Entanglement is the complexity of quantum mechanics.*

Considering this, it is not surprising that Shannon's *classical* theory of information (CIT) and quantum physics, with the emerging field of *quantum* information theory (QIT), have many background concepts in common. The former classical theory of information was a revolution in its own times, just as quantum mechanics, but with neither conceptual links, nor the least parallelism whatsoever with the latter. The great news is that the two fields have finally reached each other, in most unexpected and elegant ways. It is at the very interface of these two fields and cultures, classical and quantum information theory, that this textbook takes a crucial place and also innovates in the descriptive approach. I have spent so much time as Head of the Physics Department in my University convincing students and researchers to kick against the partitioning between physics and science in general, that I am very pleased to welcome this work of Emmanuel Desurvire, which is a model of scientific "hybridization."

Combining the cultures of a physicist (as a researcher), an academic (as a former professor and author of several books), and an engineer (as a developer and project manager) from the telecom industry, Emmanuel Desurvire attempts here to bridge the gap between the CIT and QIT cultures. On the CIT side, fundamentals, such as information, entropy, mutual entropy, and Shannon capacity theorems, are reviewed in detail, using a wealth of practical and original application examples. Worth mentioning are the reputedly difficult notions of *Kolmogorov complexity* and *Turing machines*, which were developed independently from Shannon during the same historical times, described herewith with thrust and clarity, again with original examples and illustrations. The mind-boggling (and little-known) conclusion to be retained is that Kolmogorov complexity and Shannon entropy asymptotically converge towards each other, despite fundamentally different ground assumptions. Then, under any expectation for a textbook in this subject, comes a detailed (and here quite vivid) description of various principles of *data compression* (coding optimality, integer, arithmetic, and adaptive compression) and *error-correction coding* (block and cyclic codes). Shannon's classical theory of information then moves on and concludes with the *channel-capacity theorems*, including the most elegant *Shannon–Hartley theorem* of incredibly simple and universal formulation, $C = \log(1 + SNR)$, which relates the channel capacity (C) to the signal-to-noise ratio (SNR) available at the channel's end.

The second part of Emmanuel Desurvire's book is about quantum information theory. This is where the telecom scientist, together with the author, is taken out to a work tour that she or he may not forget, hopefully a most stimulating and pleasurable one. With the notion of *reversible computation* and the *Landauer Principle*, the reader gets a first hint that "information is physical." It takes a quantum of heat kT to tamper with a single classical bit. From this point on, we begin to feel that quantum mechanics realities are standing close behind. Then come the notions of *quantum bits* or *qubits* and their logic gates to form elementary quantum circuits. Such an innocuous introduction, in fact, represents the launching pad of a rocket destined to send the reader into QIT orbit. In this adventurous journey, no spot of interest is neglected, from *superdense coding*, *teleportation*, the *Deutsch–Jozsa algorithm*, *quantum Fourier transform* and *Grover's Quantum Database Search*, to the mythical *Shor factorization* algorithm. Here, the demonstration of Shor's algorithm turns out to be very interesting and useful. Most physicists have heard about this incredible possibility, offered by quantum computing, of factorizing huge numbers within a short time, but have rarely gone into the explanatory detail. Shor's algorithm resembles the green flash: heard of by many, seen by some, but understood by few. The interest continues with a discussion of the computing times required for factorization with classical means, and to meet the various RSA challenges offered on the Internet.

The conclusive chapter on cryptography is also quite original in its approach and conclusions. First, it includes *both* classical and quantum cryptography concepts, according to the author's view that there is no point in addressing the second if one has not mastered the first. Cryptography, a serious matter for network security and privacy, is treated here with the very instructive and specific view of a telecom scientist. Forcefully and crudely stated, "The world is ugly out there," in spite of Alice and Bob's "provably secure" key exchanges (quantum key distribution, QKD). Let one not be mistaken as to the author's intent. Quantum key distribution is most precious as an element in the network security chain; Emmanuel Desurvire is only reminding the community, now with the authority of a telecom professor, that Alice and Bob are exposed, in turn, to higher-level network attacks, and that unless the Internet becomes quantum all the way through, there is no such a thing as "absolute" network security. It is only with this type of cross-disciplined book that elementary truths of the like may be spelled out.

A pervasive value and flavor of this book is that the many practical examples and illustrations provided help the reader to *think concrete*. Both the classical and quantum sides of information theory may seem difficult, rusty, oblivious, if not forthright mysterious to many engineers and scientists since long-past school graduation. More so with the quantum side, which is actually a recent expansion of knowledge (as dated after the Shor algorithm "milestone"), and that only a few engineers and scientists had the privilege to be exposed to so far, prior to beginning their professional careers. Hence, this book represents a first attempt at reconciling old with new knowledge, as destined primarily to mature engineers and scientists, particularly from, but not limited to, the telecom circle. Decision makers from government and industry, investors, and entrepreneurs may also reap some benefit by being better acquainted with the reality of quantum mechanics and the huge application potentials of QIT, apart from any timeliness consideration. Progress in quantum information theory may be a (very) long-term view indeed, but its future is confined to today's humble steps; called awareness, discipline, imagination, creativity and patience.

Thanks to Emmanuel Desurvire's book, many concepts such as quantum information theory, and the reconciliation and familiarity thereof, will be shared by both engineers and physicists, within the telecom community and hopefully far beyond. It is our deep conviction that such cross-border knowledge sharing is necessary to engage in this second revolution of quantum physics.

Professor Vincent Berger
Université Paris-Diderot, Paris 7
February 29, 2008

Introduction

In the world of telecoms, the term *information* conveys several levels of meaning. It may concern individual bits, bit sequences, blocks, frames, or packets. It may represent a message payload, or its overhead; the necessary extra information for the network nodes to transmit the message payload practically and safely from one end to another. In many successive stages, this information is encapsulated altogether to form larger blocks corresponding to higher-level network protocols, and the reverse all the way down to destination. From any telecom-scientist viewpoint, information represents this uninterrupted *flow of bits*, with network intelligence to process it. Once converted into characters or pixels, the remaining message bits become meaningful or valuable in terms of acquisition, learning, decision, motion, or entertainment. In such a larger network perspective, where information is well under control and delivered with the quality of service, what could be today's need for any *information theory* (IT)?

In the telecom research community indeed, there seems to be little interest for information theory, as based on the valid perception that there is nothing new to worry about. While the occasional evocation of *Shannon* invariably raises passionate group discussions, the professional focus is about the exploitation of bandwidth and network deployment issues. The telecom scientist may, however, wonder about the potentials of *quantum information* and *computing*, and their impact. But not only does the field seem intractable to the nonspecialist, its applications are widely believed to belong to the far-distant future. Then what could be this community's need for any *quantum information theory* (QIT)? While some genuine interest has been raised by the outcome of *quantum cryptography*, or more accurately, *quantum key distribution* (QKD), there is at present not enough matter of concern or driving market factor to bring QIT into the core of telecoms.

The situation is made even more confused through the fact that information theory and quantum information theory appear to have little in common, or that the parallels between the two can be established only at the expense of advanced specialization. The telecom scientist is thus left with unsolved questions. For instance, what is quantum information, and how is it different from Shannon's theorem? How is information carried by *qubits*, as opposed to classical bits? How do IT theorems translate into QIT? What are the ultimate algorithms for quantum information compression, error correction, and encryption, and what benefit do they provide, compared with classical approaches? What are the main conceptual realizations of quantum information processing? The curious might peruse reference books, key papers, or Internet cross-references and tutorials, but this endeavor leaves little chance of reaching satisfying conclusions, let alone acquiring solid grounds for pointing to future research directions.

To summarize, on one hand, we find the old-and-forgotten IT field, with its wealth of very mature applications in all possible areas of information processing. On the other hand, we find the more recent and poorly known QIT field, showing high promise, but little potential of application within reasonable sight. In between, the difficulty for nonspecialists to make sense of any parallels between the two, and the lack of motivation to dig into what appears an austere or intractable bunch of mathematical formalism.

The above description suggests the reason why this book was written, and its key purpose. Primarily, it is my belief that IT is incomplete without QIT, and that the second should not be approached without a fair assimilation of the first. Secondly, the mathematical difficulties of IT and QIT can, largely, be alleviated by making the presentation less formal than in the usual academic reference format. This does not mean oversimplification, but rather skipping many academic caveats, which flourish in most reference textbooks, and which make progression a tedious and risky adventure. Our portrayed telecom scientist only needs the fundamental concepts, along with supporting proof at a satisfactory level. Also, IT and QIT can be made far more interesting and entertaining by use of many illustrations and application examples.

With these goals in mind, this book has been organized as a sequence of *chapters*, each of which can be presented in two or three hour courses or seminars, and which the reader should be able to teach in turn! Except at the beginning, the sequence of chapters presents a near-uniform level of difficulty, which rapidly assures the reader that she or he will be able to make it to the very end. For the demanding, or later reference, the most advanced demonstrations have been relegated into as many Appendices. To lighten the text, an extensive use of footnotes is made. These footnotes also contain useful Internet links, and sometimes bibliographical references. Finally, lots of original exercises with difficulty levels graded as basic (B), medium (M), or tricky (T) are proposed, the set of solutions being available to class teachers from Cambridge University Press. As to the Internet links, one is aware that they do not have the value of permanent references, owing to the finite lifetime of most websites or their locators or addresses (URL). To alleviate this problem, the Publisher has agreed with the author to keep up an updated list of URLs on the associated website: www.cambridge.org/9780521881715, along with errata information.

What about the book contents?

The first two chapters (1 and 2) concern basic recalls of *probability theory*. These are purposefully entertaining to read, while the advanced reader might find useful teaching ideas for undergraduate courses.

Chapter 3 addresses the tricky concept of *information measure*. We learn something that everyone intuitively knows, namely, that there is no or little information in events that are certain or likely to happen. Uncertainty, on the other hand, is associated with high information contents.

When several possible events are being considered, the correct information measure becomes *entropy* (Chapters 4–6). As shown, Shannon's entropy concept in IT is not without strong but subtle connections with the world of Boltzmann's thermodynamics. But

IT goes a step further with the key notion of *mutual information*, and other useful entropy definitions (joint, conditional, relative), including those related to continuous random variables (differential). Chapter 7, on *algorithmic entropy* (or equivalently, *Kolmogorov complexity*), is meant to be a real treat. This subject, which comes with its strange *Turing machines*, is, however, reputedly difficult. Yet the reader should not find the presentation level different from preceding material, thanks to many supporting examples. The conceptual beauty and reward of the chapter is the asymptotic convergence between Shannon's entropy and Kolmogorov's complexity, which were derived on completely independent assumptions!

Chapters 8–10 take on a tour of *information coding*, which is primarily the art of compressing bits into shorter sequences. This is where IT finds its first and everlasting success, namely, *Shannon's source coding theorem*, leading to the notion of *coding optimality*. Several coding algorithms (Huffmann, integer, arithmetic, adaptive) are reviewed, along with a daring appendix (Appendix G), attempting to convey a comprehensive flavor in both *audio* and *video standards*.

With Chapter 11, we enter the magical world of *error correction*. For the scientist, unlike the telecom engineer, it is phenomenal that bit errors coming from random physical events can be corrected with 100% accuracy. Here, we reach the concept of a *communication channel*, with its own imperfections and intrinsic *noise*. The chapter reviews the principles and various families of *block codes* and *cyclic codes*, showing various capabilities of error-correction performance.

The communication channel concept is fully disclosed in the description going through Chapters 12–14. After reviewing *channel entropy* (or mutual information in the channel), we reach Shannon's most famous *channel-coding theorem*, which sets the ultimate limits of *channel capacity* and error-correction potentials. The case of the *Gaussian channel*, as defined by continuous random variables for signal and noise, leads to the elegant *Shannon–Hartley theorem*, of universal implications in the field of telecoms. This closes the first half of the book.

Next we approach QIT by addressing the issue of *computation reversibility* (Chapter 15). This is where we learn that information is "physical," according to *Landauer's principle* and based on the fascinating "Maxwell's demon" (thought) experiment. We also learn how *quantum gates* must differ from classical *Boolean logic gates*, and introduce the notion of *quantum bit*, or *qubit*, which can be manipulated by a "zoo" of elementary quantum gates and circuits based on *Pauli matrices*.

Chapters 17 and 18 are about *quantum measurements* and *quantum entanglement*, and some illustrative applications in *superdense coding* and *quantum teleportation*. In the last case, an appendix (Appendix P) describes the algorithm and quantum circuit required to achieve the *teleportation of two qubits* simultaneously, which conveys a flavor of the teleportation of more complex systems.

The two former chapters make it possible in Chapters 19 and 20 to venture further into the field of *quantum computing (QC)*, with the *Deutsch–Jozsa* algorithm, the *quantum Fourier transform,* and, overall, two famous QC algorithms referred to as the *Grover Quantum Database Search* and *Shor's factorization*. If, some day it could be implemented in a physical quantum computer, Grover's search would make it possible to explore databases with a quadratic increase in speed, as compared with any classical computer. As to Shor's factorization, it would represent the end of classical cryptography in global use today. It is, therefore, important to gain a basic understanding of both Grover and Shor QC algorithms, which is not a trivial task altogether! Such an understanding not only conveys a flavor of QC power and potentials (as due to the property of quantum parallelism), but it also brings an awareness of the high complexity of quantum-computing circuits, and thus raises true questions about practical hardware, or massive or parallel quantum-gates implementation.

Quantum information theory really begins with Chapter 21, along with the introduction of *von Neumann entropy*, and related variants echoing the classical ones. With Chapters 22 and 23, the elegant analog of Shannon's channel source-coding and channel-capacity theorems, this time for quantum channels, is reached with the *Holevo bound* concept and the so-called *HSW theorem*.

Chapter 24 is about quantum error correction, in which we learn that various types of single-qubit errors can be effectively and elegantly corrected with the *nine-qubit Shor code* or more powerfully with the equally elegant, but more universal *seven-qubit CSS code*.

The book concludes with a hefty chapter dedicated to *classical* and *quantum cryptography* together. It is the author's observation and conviction that quantum cryptography cannot be safely approached (academically speaking) without a fair education and awareness of what cryptography, and overall, network security are all about. Indeed, there is a fallacy in believing in "absolute security" of one given ring in the security chain. Quantum cryptography, or more specifically as we have seen earlier, *quantum key distribution* (QKD), is only one constituent of the security issue, and contrary to common belief, it is itself exposed to several forms of potential attacks. Only with such a state of mind can cryptography be approached, and QKD be appreciated as to its relative merits.

Concerning the QIT and QC side, it is important to note that this book purposefully avoids touching on two key issues: the effects of *quantum decoherence*, and the *physical implementation of quantum-gate circuits*. These two issues, which are intimately related, are of central importance in the industrial realization of practical, massively parallel *quantum computers*. In this respect, the experimental domain is still at a stage of infancy, and books describing the current or future technology avenues in QC already fill entire shelves.

Notwithstanding long-term expectations and coverage limitations, it is my conviction that this present book may largely enable telecom scientists to gain a first and fairly complete appraisal of both IT and QIT. Furthermore, the reading experience should substantially help one to acquire a solid background for understanding QC applications and experimental realizations, and orienting one's research programs and proposals accordingly. In large companies, such a background should also turn out to be helpful to propose related positioning and academic partnership strategy to the top management, with confident knowledge and conviction.

Contents