A SHORT INTRODUCTION TO QUANTUM INFORMATION AND QUANTUM COMPUTATION

Quantum information and computation is a rapidly expanding and cross-disciplinary subject. This book gives a self-contained introduction to the field for physicists, mathematicians and computer scientists who want to know more about this exciting subject. After a step-by-step introduction to the quantum bit (qubit) and its main properties, the author presents the necessary background in quantum mechanics. The core of the subject, quantum computation, is illustrated by a detailed treatment of three quantum algorithms: Deutsch, Grover and Shor. The final chapters are devoted to the physical implementation of quantum computers, including the most recent aspects, such as superconducting qubits and quantum dots, and to a short account of quantum information.

Written at a level suitable for undergraduates in physical sciences, no previous knowledge of quantum mechanics is assumed, and only elementary notions of physics are required. The book includes many short exercises, with solutions available to instructors through solutions@cambridge.org.

Michel Le Bellac is Emeritus Professor at the University of Nice, and a well known elementary particle theorist. He graduated from Ecole Normale Supérieure in 1962, before conducting research with CNRS. In 1967 he returned to the University of Nice, and was appointed Full Professor of Physics in 1971, a position he held for over 30 years. His main fields of research have been the theory of elementary particles and field theory at finite temperatures. He has published four other books in French and three other books in English, including *Thermal Field Theory* (Cambridge, 1996), *Equilibrium and Non-Equilibrium Statistical Thermodynamics* with Fabrice Mortessagne and G. George Batrouni (Cambridge, 2004) and *Quantum Physics* (Cambridge, 2006).

A SHORT INTRODUCTION TO QUANTUM INFORMATION AND QUANTUM COMPUTATION

Michel Le Bellac

Translated by Patricia de Forcrand-Millard

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Published in the United States of America by Cambridge University Press, New York

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521860567

First published as *Introduction à l'information quantique* by Editions Belin 2005
First published in English 2006
First published 2011
Second Edition 2012
Reprinted 2013

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-86056-7 Hardback

Contents

Foreword

Quantum physics is well known for being counter-intuitive, or even bizarre. Quantum correlations have no equivalence in classical physics. This was all well known for years. But several discoveries in the 1990's changed the world. First, in 1991 Artur Ekert, from Oxford University, discovered that quantum correlations could be used to distribute cryptographic keys. Suddenly physicists realized that quantum correlations and its associated bizarre non-locality, could be exploited to achieve a useful task that would be impossible without quantum physics. What a revolution! And this was not the end. Three years later, Peter Shor, from the AT&T Laboratories, discovered an algorithm that breaks the most used public key crypto-systems. Shor's algorithm requires a quantum computer, yet another bizarre quantum device, a kind of computer that heavily exploits the quantum superposition principle. The following year, in 1995, a collaboration between six physicists and computer scientists from three continents led to the discovery of quantum teleportation, a process with a science-fiction flavour.

These discoveries and others led to the emergence of a new science, marrying quantum physics and theoretical computer science, called quantum information science. Today, a steadily growing community of physicists, mathematicians and computer scientists develop the tools of this new science. This leads to new experiments and new insights into physics and information theory. It is a fascinating time.

Quantum information is still a very young science. In particular, the technology required to build a quantum computer is still unknown. Only quantum key distribution has reached a certain level of maturity, with a few start-ups already offering complete systems. Nevertheless, quantum information has been widely recognised as a source for truly innovative ideas and disruptive technologies.

In this context Michel Le Bellac's book is especially welcome. It provides a concise, yet precise, introduction to quantum information science. The book will be of great help to anyone who would like to understand the basics of quantum information. It is accessible to non-physicists and to physicists not at ease with quantum oddities. It will contribute to bringing together the different communities that are joining forces to develop this science of the future. For this purpose one needs to get used to concepts such as entanglement, non-locality, teleportation and superpositions of seemingly exclusive state of affairs, etc. A demanding but very joyful exploration for all readers!

Nicolas Gisin
Geneva, November 2005

Preface

This book originated in a course given first to computer scientists at the University of Nice–Sophia Antipolis in October 2003, and later to second-year graduate students at the same University.

Quantum information is a field which at present is undergoing intensive development and, owing to the novelty of the concepts involved, it seems to me it should be of interest to a broad range of scientists beyond those actually working in the field. My goal here is to give an elementary introduction which is accessible not only to physicists, but also to mathematicians and computer scientists desiring an initiation into the subject. This initiation includes the essential ideas from quantum mechanics, and the only prerequisite is knowledge of linear algebra at the undergraduate level and some physics background at the high school level (except in Chapter 6 where I discuss the physical implementations of quantum computers and more physics background is required). In order to make it easier for mathematicians and computer scientists to follow, I give an elementary presentation of the Dirac notation. Quantum physics is an extremely large subject, and so I have attempted to limit the introductory concepts to the barest minimum needed to understand quantum information.

In Chapter 2, I introduce the concept of the quantum bit or qubit using the simplest possible example, that of the photon polarization. This example allows me to present the essential ideas of quantum mechanics and explain quantum cryptography. Chapter 3 generalizes the concept of qubit to other physical systems like spin 1/2 and the two-level atom, and explains how qubits can be manipulated by means of Rabi oscillations. Quantum correlations, which are introduced in Chapter 4, certainly represent the situation where the classical and quantum concepts most obviously diverge. Several ideas such as entanglement and the concept of state operator (or density operator) which are essential for what follows are introduced in the same chapter.

After dealing with the indispensable preliminaries, in Chapter 5 I reach the core of the subject, quantum computing. The quantum logic gates are used to construct quantum logic circuits which allow specific algorithms to be realized and illustrate quantum parallelism. Three algorithms are explained in detail: the Deutsch algorithm, the Grover search algorithm, and the Shor factorization algorithm. Chapter 6 describes four possible physical realizations of a quantum computer: computers based on NMR, trapped ions, Josephson junctions (superconducting qubits), and quantum dots. Finally, in Chapter 7 I give a brief introduction to quantum information: teleportation, the von Neumann entropy, and quantum error-correction codes.

I am very grateful to Joël Leroux of the Ecole Supérieure in Computing Sciences of Sophia Antipolis for giving me the opportunity to teach this course. I also thank Yves Gabellini for rereading the manuscript and Jean-Paul Delahaye for his comments and especially for his essential aid in the writing of Section 5.9. This book has come into existence thanks to the support of Patrizia Castiglione and Annick Lesne of Éditions Belin, and also Simon Capelin and Vince Higgs of Cambridge University Press, whom I take this opportunity to thank. Finally, I am very grateful to Patricia de Forcrand-Millard for the excellence of her translation and to Nicolas Gisin for his foreword.