



A Short Introduction to Quantum Information and Quantum

Computation, Michel Le Bellac, Cambridge University Press, 2006, pp:167, ISBN 0-521-86056-3; Price: \$60.00 (hc)

Anyone teaching or taking an introductory course on quantum information or computation would do well to consider this book. It is applicable to multi-disciplinary settings as it is aimed at physicists, computer scientists, and mathematicians. Any senior undergraduate student in physics will have few difficulties extending his or her knowledge of quantum mechanics by applying it to the concepts presented, which should also be accessible to anyone with a background in linear algebra and a willingness to accept at face value the physical principles involved. By design the book teaches very little about quantum mechanics, choosing rather to concentrate on its application to the relatively new fields of quantum information and quantum computation. While certain concepts from physics such as light polarization and dipoles in external fields appear throughout the book, prior knowledge of them is neither assumed nor required, apart from one stand-alone chapter.

After a short introduction the book starts by describing the concept of a quantum bit, or qubit, via the example of orthogonal polarization states of single photons. Dirac notation is also introduced at this point, assuming that the reader is familiar with linear algebra. These two ideas are then combined in a section that formulates the original quantum key distribution (QKD) scheme of Bennet and Brassard, the famous BB84 protocol. While most applications of quantum information and computation are left for later in the book, the discussion of QKD at this early point provides an excellent opportunity to become familiar with the relevant notation and language. Furthermore, since QKD is experimentally realizable, and in fact commercially available, it is also a good motivator for what follows.

The next two chapters deal with the mathematical description of qubits and quantum correlations. The Bloch sphere for pure states of spin $\frac{1}{2}$ particles is introduced using only geometrical arguments. This gives rise to the obvious mapping of the computational basis onto the poles of the Bloch sphere, allowing a qubit to be described independently of a physical system. The unitary evolution of such a qubit is then explored, which shows how Rabi oscillations can be employed to transform or manipulate qubits. The principles of NMR and MRI are described, but again little to no prior knowledge of the physics involved is required. Important results such as the no-cloning theorem and Bell's inequalities are discussed and explained, as well as the problem of decoherence and how to describe its effects theoretically.

According to the title of this book its goal is to introduce the reader to quantum computing and quantum information; with the first four chapters providing the necessary background, Chapters 5 and 7 do just that (Chapter 6 is the stand-alone physics-based chapter mentioned earlier). The computational basis for an n -qubit Hilbert space is defined, as well as the need for reversible evolution in the standard proposals for quantum computation. This is in contrast to classical computing, in which fundamental operations such as NAND and COPY are irreversible processes. The quantum analogues to these operations, performed by Toffoli and CNOT gates respectively, are stated and investigated before moving on to examples of

quantum algorithms. The first of these algorithms was also the first quantum algorithm to be discovered, Deutsch's algorithm for determining if an unknown function is constant without having to evaluate it at each possible input. While not particularly exciting as an algorithm, it provides an excellent demonstration of the abilities of quantum parallelism and also has historical significance. The other two algorithms investigated are of greater practical value: Grover's search algorithm and the quantum Fourier transform. The end of Chapter 5 also provides an excellent discussion of algorithm classification, so any physicists reading it may gain an understanding of what computer scientists mean when they ask whether 'P=NP?' or say that a problem is 'NP complete.'

With half of the title taken care of in Chapter 5 the other half, quantum information, is the subject of Chapter 7. Quantum teleportation is derived to elucidate the concept of information that is clearly not classical, thus motivating the need for quantum information as a distinct concept. A brief review of Shannon entropy and classical information theory is provided in order to set the stage for von Neumann entropy, which is investigated in detail. The chapter ends with a discussion of quantum error correction.

For those with a background in physics, Chapter 6 contains an overview of existing techniques that have the potential to one day contribute to a quantum computer, with sections on NMR, trapped ions, superconducting qubits, and quantum dots. These sections introduce their systems and discuss how the relevant states can be mapped to the computational basis, as well as how to realize a CNOT gate in each case. This chapter contains no prerequisite material for Chapter 7.

Throughout the book Le Bellac uses rigor when it is necessary without getting bogged down in it, and combines this with a good sense of humour and the occasional reference to pop culture and everyday life. The result is a text book that is pleasantly easy to read but which doesn't gloss over any important details. The problems at the end of each chapter are interesting, instructive, and directly related to the text. Concepts that can be useful but which are not central to the text, such as Maxwell's demon or the mathematics of RSA encryption, are separated from the main body as boxed asides that are as clear and informative as the rest of the book for those who wish to spend time on them. This is a book that definitely achieves the goal it aims for, and at under 160 pages of text it would be ideal for a single-semester course or an independent reading project.

M.S. Underwood,
Calgary, AB