The book is intended for researchers as well as advanced undergraduate students in physics, chemistry, mathematics and computer science. It may be used as a supplement to standard textbooks. It will be also of interest for any philosopher interested in quantum mechanics. A reviewer cannot do complete justice to a book in which every new approach, every step and practically every word obey the motto of consistency and cleanliness. I can only say that I admire it. I think it should be strongly recommended to all these different categories of readers, and often read again to get rid of past obscurities.

Roland Omnès
Department of Physics
University of Paris
Paris, France
E-mail address: roland.omnes@th.u-psud.fr

doi:10.1016/S1355-2198(03)00010-8

The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation
D. Bouwmeester, A. Ekert and A. Zeilinger (Eds.); Germany, 2000, 314pp, US$ 54, ISBN 3-540-66778-4

Quantum information theory and quantum computation theory have progressed enough in the last decade to warrant several introductory texts on those topics: Nielsen and Chuang (2000) or Lo, Popescu, and Spiller (1998). Given the availability and quality of these texts, one might question the decision to introduce yet another. However, a cursory glance at *The Physics of Quantum Information* will remove any such notions. The Bouwmeester, Ekert, and Zeilinger volume complements the introductory literature on quantum information and quantum computation by paying special attention to the experimental aspects of those subjects. Not a chapter goes by without discussion of experiments implementing new theoretical ideas or prospects for doing so.[1]

Chapter one is an introduction to the basic theoretical tools of quantum information theory. Each theoretical topic that is introduced is accompanied by an introduction to its experimental realization. Superposition is discussed in the context of the double-slit experiment; single qubit operations are discussed in relation to beam splitters, interferometers, and phase shifters; methods of producing entanglement follow immediately after writing down a triplet state.

Chapter two is an exceptional introduction to quantum cryptography. The pedagogical skills of the authors of this chapter should be especially noted. This chapter begins with a discussion of primitive cryptographic techniques. The authors

[1]Although other texts discuss experimental implementation, such as Nielsen and Chuang (2000), none seem to be as detailed and comprehensive.

discuss the development of more sophisticated techniques and the challenges that each faces. This successfully introduces the reader to the working concepts of cryptography. The most important concept for cryptography is the secure distribution of keys. It is here where the authors think that quantum cryptography can play a key role. (Pun intended!) They suggest that quantum cryptography is an area of physics where "…a border between blue sky and down-to-earth research is quite blurred" (p. 25). In particular, they are referring to results that in the past have been mainly of foundational and not practical significance such as the no cloning theorem and Bell's theorem. Now they play a role in ensuring cryptographic success. As with any theoretical result, a host of problems arise when an attempt is made to put such a result to use in the physical world. The authors discuss key distribution schemes with single particles and entangled particles, the difficulties each faces, and potential solutions. This chapter concludes with a discussion of the experimental realization of quantum cryptographic schemes and assures us that it is no longer a question of whether quantum cryptography *can* be successful, but rather *when* quantum cryptography can be used as a standard way to protect messages.

Quantum dense coding and quantum teleportation are the topics of the next chapter. For the theoretician, such topics are almost trivial, but they present the experimentalist with a host of difficulties. This chapter goes to some lengths to discuss such difficulties. There are two important pieces of equipment that are needed for teleportation and dense coding. The first is a source of entangled photons.[2] This chapter discusses time, momentum, and polarization entanglement and their production. The second essential piece of equipment is the Bell state analyzer, and it too is discussed. After laying the theoretical and experimental groundwork for teleportation and dense coding, several experiments are discussed, including dense coding, conventional teleportation, teleportation of continuous quantum variables, and teleportation of entanglement.

Chapters four and five are devoted to quantum computation. Chapter four begins with a general, non-technical description of the basic concepts of quantum computation. David Deutsch and Artur Ekert coauthor this section, and Deutsch's well-known philosophical predilections are evident. For example, consider their analysis of Grover's algorithm. Grover's algorithm is capable of searching an unsorted list of N items in $\sqrt{N}$ steps. On average, a classical computer requires $N/2$ steps to perform such a feat. The authors attribute the success of such an algorithm to a quantum computer's ability to examine each entry on the list simultaneously; a massive, parallel computation taking place in N universes simultaneously. Whether an explanation of the success of quantum computation is dependent on a many-worlds type interpretation is an open issue (Steane, 2000).

In the next section of this chapter, Richard Jozsa provides a more technical introduction to quantum algorithms. Jozsa begins by describing what has become known as *quantum parallelism*: the seeming ability of a quantum computer to compute all values of a function in a single step. For convenience, let us adopt the following notation: $|x\rangle$ is a tensor product of qubits, two-level quantum systems,

[2]Photons per se are not required, but this is the quantum system used in experimental practice.

which represent the number x in binary. For example, $|3\rangle = |1\rangle|1\rangle$. Suppose that we have a function f: $\{0,1\}^n \to \{0,1\}$, and a quantum gate, U_f, that performs the following evolution:

$$|x\rangle|y\rangle \overset{U_f}{\to} |x\rangle|f(x) \otimes y\rangle,$$

where $\otimes$ is addition mod 2. $|x\rangle$ will be referred to as the input register, and $|y\rangle$ as the output register. The U_f gate takes the number represented in the input register and changes the state of the output register to match the value of the function f at x. Consider the following unitary evolution which is an example of quantum parallelism:

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \overset{U_f}{\to} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle. \tag{1}$$

By using a superposition of n qubits as the initial input, every number from 0 to $2^n - 1$ is represented. Using one pass through the unitary gate, U_f, each value of the function from 0 to $2^n - 1$ is stored in the qubits used for the computation, albeit they are in a superposition. There appear to be no classical algorithms with corresponding behavior. Unfortunately, not all values of the function are accessible. A measurement of the input register will randomly yield one of the 2^n states represented in the initial superposition with probability $1/2^n$. A subsequent measurement of the output register will reveal the value of the function at that point. All states $|x\rangle$ and $|x'\rangle$, where $x \neq x'$, are orthogonal to one another and hence no further measurements may be done on the input register that will reveal other values of the function.

The philosophical question concerning quantum parallelism is obvious: does process (1) count as a computation of 2^n values of the function, even when in principle at most one value of the function can be known? The answer is far from obvious. The issue is complicated by the fact that some global properties of functions, for example, if they are constant, can be determined with certainty in some instances. In addition to quantum parallelism, Jozsa identifies the *principle of local operations* as another reason for quantum algorithms being faster than their classical correlates. The principle is: "a single local unitary operation on a subsystem of a large entangled system processes the embodied information by an amount which would generally require an exponential effort to represent in classical computation terms"(p.108). Jozsa has the following in mind: A one-qubit unitary gate acting on a large system of entangled qubits will count as one computational step on a quantum computer. The classical description of such an evolution would correspond to matrix multiplication of the following type:

$$a_{i_1,\ldots,i_n} = \sum_j U^j_{i_1} a_{ji_2,\ldots,i_n}. \tag{2}$$

The state is described by $a_{i_1,\ldots,i_n}$ where each i_m is 0 or 1 and U is a 2×2 unitary matrix. The matrix multiplication must be performed 2^{n-1} times.

Jozsa suggests that the above phenomena indicate "a bizarre new distinction between classical and quantum physics"(p. 109). "From our point of view of

information processing, time evolution in quantum physics is seen to be intrinsically more complex than classical time evolution… "(p. 105). Surely, quantum computers allow new and interesting ways to perform computations; however, does this point to a new distinction between classical and quantum *physics*, or rather a distinction between the typical algorithms implemented on quantum and classical computers? It is difficult to accept the former without additional support, for the comparison between classical and quantum systems is severely restricted. Only two-state classical systems have been considered. Unless one can establish that the computational abilities of two-state classical systems are the same as the computational abilities of *any* classical system, the stronger distinction would seem to lack support. Barring my previous objections to Jozsa, the rest of his section in this chapter is very informative. It describes in detail Deutsch's algorithms, Fourier transforms, which are essential parts of several quantum algorithms, Shor's algorithm, and Grover's algorithm. The remainder of this chapter is devoted to quantum computation via trapped ions.

Chapter five discusses several experimental approaches to quantum computation including cavity QED experiments, Linear ion traps, and NMR experiments. The remaining chapters cover the topics of multi-particle entanglement, entanglement purification, and quantum error correction, all of which are essential to the actual realization of a quantum computer. All in all, *The Physics of Quantum Information* is an excellent introductory text covering all essential areas of quantum information and computation with a distinct bent for helping the reader grasp the experimental foundations of the field.

References

Lo, H.-K. L., Popescu, S., & Spiller, T. (1998). *Introduction to quantum computation and information*. Singapore: World Scientific.

Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge: Cambridge University Press.

Steane, A. M. (2000). A quantum computer only needs one universe. Preprint quant-ph/00030845.

Armond Duwell
History and Philosophy of Science
University of Pittsburgh
Pittsburgh, PA 15260, USA
E-mail address: aduwell@hotmail.com

doi:10.1016/S1355-2198(03)00012-1

Holism in philosophy of mind and philosophy of physics
Michael Esfeld, Dordrecht, 2001, pp. xiv + 366, US $113, ISBN 0-7923-7003-1

Quine's work made holism a focus of attention in the philosophy of mind and language. More recently, philosophers of physics have debated the extent and