1
Introduction

Quantum information is concerned with using the special features of quantum physics for the processing and transmission of information. It should, however, be clearly understood that any physical object when analyzed at a deep enough level is a quantum object; as Rolf Landauer has succinctly stated, “A screwdriver is a quantum object.” In fact, the conduction properties of the metal blade of a screwdriver are ultimately due to the quantum properties of electron propagation in a crystalline medium, while the handle is an electrical insulator because the electrons in it are trapped in a disordered medium. It is again quantum mechanics which permits explanation of the fact that the blade, an electrical conductor, is also a thermal conductor, while the handle, an electrical insulator, is also a thermal insulator. To take an example more directly related to information theory, the behavior of the transistors etched on the chip inside your computer could not have been imagined by Bardeen, Brattain, and Shockley in 1947 were it not for their knowledge of quantum physics. Although your computer is not a quantum computer, it does function according to the principles of quantum mechanics!

This quantum behavior is also a *collective* behavior. Let us give two examples. First, if the value 0 of a bit is represented physically in a computer by an uncharged capacitor while the value 1 is represented by the same capacitor charged, the passage between the charged and uncharged states amounts to the displacement of 10^4 to 10^5 electrons. Second, in a classic physics experiment, sodium vapor is excited by an electric arc, resulting in the emission of yellow light, the well known “yellow line of sodium.” However, it is not actually the behavior of an individual atom that is observed, as the vapor cell typically contains 10^{20} atoms.

The great novelty since the early 1980s is that physicists now know how to *manipulate and observe individual quantum objects* – photons, atoms, ions, and so on – and not just the collective quantum behavior of a large number of such objects. It is this possibility of manipulating and observing individual quantum objects which lies at the foundation of quantum computing, as these quantum objects can

https://doi.org/10.1017/CBO9780511755361.003

be used as the physical support for quantum bits. Let us emphasize, however, that no new fundamental concept has been introduced since the 1930s. If the founding fathers of quantum mechanics (Heisenberg, Schrödinger, Dirac, ...) were resurrected today, they would find nothing surprising in quantum information, but they would certainly be impressed by the skills of experimentalists, who have now learned how to perform experiments which in the past were referred to as "gedanken experiments" or "thought experiments."

It should also be noted that the ever-increasing miniaturization of electronics will eventually be limited by quantum effects, which will become important at scales of tens of nanometers. *Moore's law*[1] states that the number of transistors which can be etched on a chip doubles every 18 months, leading to a doubling of the memory size and the computational speed (amounting to a factor of 1000 every 15 years!). The extrapolation of Moore's law to the year 2010 implies that the characteristic dimensions of circuits on a chip will reach a scale of the order of 50 nanometers, and somewhere below 10 nanometers (to be reached by 2020?) the individual properties of atoms and electrons will become predominant, so that Moore's law may cease to be valid ten to fifteen years from now.

Let us take a very preliminary look at some characteristic features of quantum computing. A classical bit of information takes the value 0 or 1. A quantum bit, or *qubit*, can not only take the values 0 and 1, but also, in a sense which will be explained in the following chapter, all intermediate values. This is a consequence of a fundamental property of quantum states: it is possible to construct linear superpositions of a state in which the qubit has the value 0 and of a state in which it has the value 1.

The second property on which quantum computing is based is *entanglement*. At a quantum level it can happen that two objects form a single entity, even at arbitrarily large separation from each other. Any attempt to view this entity as a combination of two independent objects fails, unless the possibility of signal propagation at superluminal speeds is allowed. This conclusion follows from the theoretical work of John Bell in 1964, inspired by the studies of Einstein, Podolsky, and Rosen (EPR) in 1935, and from the experiments motivated by these studies (see Section 4.5 below). As we shall see in Chapter 5, the amount of information contained in an entangled state of N qubits grows exponentially with N, and not linearly as in the case of classical bits.

The combination of these two properties, linear superposition and entanglement, lies at the core of *quantum parallelism*, the possibility of performing a large number of operations in parallel. However, the principles of quantum parallelism differ fundamentally from those of classical parallelism. Whereas in a classical

[1] Moore's law is not a law based on theory, but rather an empirical statement which has been observed to hold over the last forty years.

https://doi.org/10.1017/CBO9780511755361.003

computer it is always possible to know (at least in principle) what the internal state of the computer is, such knowledge is *in principle* impossible in a quantum computer. Quantum parallelism has led to the development of entirely new algorithms such as the Shor algorithm for factoring large numbers into primes, an algorithm which by its nature cannot be run on a classical computer. It is in fact this algorithm which has stimulated the development of quantum computing and has opened the door to a new science of algorithms.

Quantum computing opens up fascinating perspectives, but its present limitations should also be emphasized. These are of two types. First, even if quantum computers were available today, the number of algorithms of real interest is at present very limited. However, there is nothing which prevents others from being imagined in the future. The second type of limitation is that we do not know if it will someday be possible to construct quantum computers large enough to manipulate hundreds of qubits. At present, we do not know what the best physical support for qubits will be, and we know at best how to manipulate only a few qubits (a maximum of seven; see Chapter 6). The Enemy Number One of a quantum computer is *decoherence*, the interaction of qubits with the environment which blurs the delicate linear superpositions. Decoherence introduces errors, and ideally a quantum computer must be completely isolated from its environment. This in practice means the isolation must be good enough that any errors introduced can be corrected by error-correcting codes specific to qubits.

In spite of these limitations, quantum computing has become the passion of hundreds of researchers around the world. This is cutting-edge research, particularly that on the manipulation of individual quantum objects. This work, in combination with entanglement, permits us to speak of a “new quantum revolution” which is developing into a veritable quantum engineering. Another application might be the building of computers designed to simulate quantum systems. And, as has often happened in the past, such fundamental research may also result in new applications completely different from quantum computing, applications which we are not in a position to imagine today.

https://doi.org/10.1017/CBO9780511755361.003