Cambridge University Press
978-0-521-86056-7 - A Short Introduction to Quantum Information and Quantum Computation
Michel Le Bellac Translated by Patricia de Forcrand-Millard
Excerpt
More information

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 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.

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.

2

What is a qubit?

2.1 The polarization of light

Our first example of a qubit will be the polarization of a photon. First we briefly review the subject of light polarization. The *polarization of light* was demonstrated for the first time by the Chevalier Malus in 1809. He observed the light of the setting sun reflected by the glass of a window in the Luxembourg Palace in Paris through a crystal of Iceland spar. He showed that when the crystal was rotated, one of the two images of the sun disappeared. Iceland spar is a birefringent crystal which, as we shall see below, decomposes a light ray into two rays polarized in perpendicular directions, while the ray reflected from the glass is (partially) polarized. When the crystal is suitably oriented one then observes the disappearance (or strong attenuation) of one of the two rays. The phenomenon of polarization displays the vector nature of light waves, a property which is shared by shear sound waves: in an isotropic crystal, a sound wave can correspond either to a vibration transverse to the direction of propagation, i.e., a shear wave, or to a longitudinal vibration, i.e., a compression wave. In the case of light the vibration is only transverse: the electric field of a light wave is orthogonal to the propagation direction.

Let us recall the mathematical description of a planar and monochromatic scalar wave traveling in the z direction. The amplitude of vibration $u(z,t)$ as a function of time t has the form

$$u(z,t) = u_0 \cos(\omega t - kz),$$

where ω is the vibrational frequency, k is the wave vector ($k = 2\pi/\lambda$, where λ is the wavelength), related by $\omega = ck$, where c is the propagation speed, here the speed of light. It can be immediately checked that a maximum of $u(z,t)$ moves at speed $\omega/k = c$. In what follows we shall always work in a plane at fixed z, for example, the $z = 0$ plane where

$$u(z=0,t) := u(t) = u_0 \cos \omega t.$$

Cambridge University Press
978-0-521-86056-7 - A Short Introduction to Quantum Information and Quantum Computation
Michel Le Bellac Translated by Patricia de Forcrand-Millard
Excerpt
More information

When an electromagnetic wave passes through a polarizing filter (a *polarizer*), the vibration transmitted by the filter is a vector in the xOy plane transverse to the propagation direction:

$$E_x = E_0 \cos\theta \cos\omega t,$$
$$E_y = E_0 \sin\theta \cos\omega t, \tag{2.1}$$

where θ depends on the orientation of the filter. The light intensity (or energy) measured, for example, using a photoelectric cell is proportional to the squared electric field $I \propto E_0^2$ (in general, the energy of a vibration is proportional to the squared vibrational amplitude). The unit vector[1] $\hat{p}$ in the xOy plane

$$\hat{p} = (\cos\theta, \sin\theta), \quad \vec{E} = E_0 \hat{p} \cos\omega t, \tag{2.2}$$

characterizes the *(linear) polarization* of the electromagnetic wave. If $\theta = 0$ the light is polarized in the x direction, and if $\theta = \pi/2$ it is polarized in the y direction. Natural light is *unpolarized* because it is made up of an *incoherent* superposition (this important concept will be defined precisely in Chapter 4) of 50% light polarized along Ox and 50% light polarized along Oy.

We shall study polarization quantitatively using a *polarizer–analyzer ensemble*. We allow the light first to pass through a polarizer whose axis makes an angle θ with Ox, and then through a second polarizer, called an analyzer, whose axis makes an angle α with Ox (Fig. 2.1), and write

$$\hat{n} = (\cos\alpha, \sin\alpha). \tag{2.3}$$

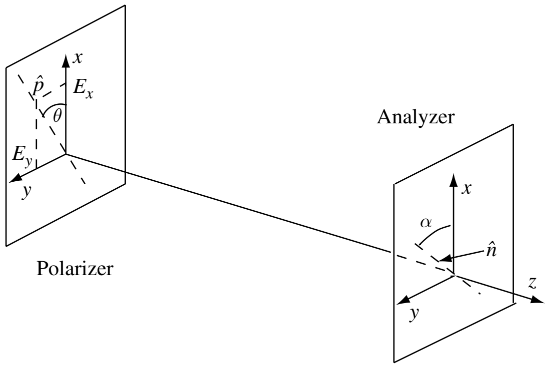

Figure 2.1 A polarizer–analyzer ensemble.

[1] Throughout this book, unit vectors of ordinary space $\mathbb{R}^3$ will be denoted by a hat: $\hat{p} = \vec{p}/p$, $\hat{n} = \vec{n}/n, \ldots$.

Cambridge University Press
978-0-521-86056-7 - A Short Introduction to Quantum Information and Quantum Computation
Michel Le Bellac Translated by Patricia de Forcrand-Millard
Excerpt
More information

At the exit from the analyzer the electric field $\vec{E}'$ is obtained by projecting the field (2.1) onto $\hat{n}$:

$$\begin{aligned}\vec{E}' &= (\vec{E}\cdot\hat{n})\hat{n} = E_0 \cos\omega t(\hat{p}\cdot\hat{n})\hat{n} \\ &= E_0\cos\omega t(\cos\theta\cos\alpha + \sin\theta\sin\alpha)\hat{n} \\ &= E_0\cos\omega t\cos(\theta-\alpha)\hat{n}.\end{aligned} \tag{2.4}$$

From this we obtain the *Malus law* for the intensity at the exit from the analyzer:

$$I' = I\cos^2(\theta-\alpha). \tag{2.5}$$

Linear polarization is not the most general possible case. *Circular polarization* is obtained by choosing $\theta = \pi/4$ and shifting the phase of the y component by $\pm\pi/2$. For example, for right-handed circular polarization we have

$$\begin{aligned} E_x &= \frac{E_0}{\sqrt{2}}\cos\omega t, \\ E_y &= \frac{E_0}{\sqrt{2}}\cos\left(\omega t - \frac{\pi}{2}\right) = \frac{E_0}{\sqrt{2}}\sin\omega t.\end{aligned} \tag{2.6}$$

The electric field vector traces a circle of radius $|E_0|/\sqrt{2}$ in the xOy plane. The most general case is that of elliptical polarization, where the tip of the electric field vector traces an ellipse:

$$\begin{aligned} E_x &= E_0\cos\theta\cos(\omega t-\delta_x) = E_0\,\mathrm{Re}\left[\cos\theta\, \mathrm{e}^{-\mathrm{i}(\omega t-\delta_x)}\right] = E_0\,\mathrm{Re}\left(\lambda\,\mathrm{e}^{-\mathrm{i}\omega t}\right), \\ E_y &= E_0\sin\theta\cos(\omega t-\delta_y) = E_0\,\mathrm{Re}\left[\sin\theta\, \mathrm{e}^{-\mathrm{i}(\omega t-\delta_y)}\right] = E_0\,\mathrm{Re}\left(\mu\,\mathrm{e}^{-\mathrm{i}\omega t}\right).\end{aligned} \tag{2.7}$$

It will be important for what follows to note that *only the difference* $\delta = (\delta_y - \delta_x)$ *is physically relevant*. By a simple change of time origin we can, for example, choose $\delta_x = 0$. To summarize, the most general polarization is described by a *complex* vector normalized to unity (or a *normalized vector*) in a two-dimensional space with components

$$\lambda = \cos\theta\,\mathrm{e}^{\mathrm{i}\delta_x}, \quad \mu = \sin\theta\,\mathrm{e}^{\mathrm{i}\delta_y},$$

and $|\lambda|^2 + |\mu|^2 = 1$. Owing to the arbitrariness in the phase, a vector with components (λ', μ'),

$$\lambda' = \lambda\,\mathrm{e}^{\mathrm{i}\phi}, \quad \mu' = \mu\,\mathrm{e}^{\mathrm{i}\phi},$$

Cambridge University Press
978-0-521-86056-7 - A Short Introduction to Quantum Information and Quantum Computation
Michel Le Bellac Translated by Patricia de Forcrand-Millard
Excerpt
More information

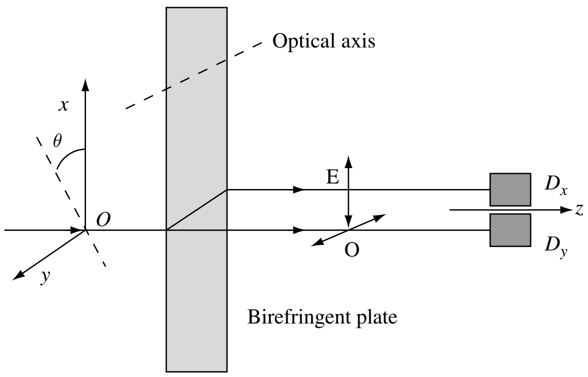

Figure 2.2 Decomposition of the polarization by a birefringent plate. The ordinary ray O is polarized horizontally and the extraordinary ray E is polarized vertically.

represents the same polarization as (λ, μ). It is more correct to say that the polarization is represented mathematically by a *ray*, that is, by a vector up to a phase.

Remarks

- A birefringent plate (Fig. 2.2) can be used to separate an incident beam into two orthogonal polarization states, and one can repeat the Malus experiment by checking that a suitably oriented polarizing filter absorbs one of the two polarizations while allowing the orthogonal one to pass through.
- Let us consider a crossed polarizer–analyzer ensemble, for example, with the polarizer aligned along Ox and the analyzer along Oy. No light is transmitted. However, if we introduce an intermediate polarizer whose axis makes an angle θ with Ox, part of the light is transmitted: the first projection gives a factor $\cos\theta$ and the second gives a factor $\sin\theta$, so that the intensity at the exit of the analyzer is

$$I' = I \cos^2\theta \sin^2\theta,$$

which vanishes only for $\theta = 0$ or $\theta = \pi/2$.

2.2 Photon polarization

Ever since the work of Einstein (1905), we have known that light is composed of photons or light particles. If the light intensity is reduced sufficiently, it should be possible to study the polarization of individual photons which can easily be detected using photodetectors, the modern version of which is the CCD (Charge Coupling Device) camera.[2] Let us suppose that $\mathcal{N}$ photons are detected in an

[2] A cell of the retina is sensitive to an isolated photon, but only a few percent of the photons entering the eye reach the retina.

experiment. When $\mathcal{N} \to \infty$ it should be possible to recover the results of wave optics which we have just stated above. For example, let us perform the following experiment (Fig. 2.2). A birefringent plate is used to separate a light beam whose polarization makes an angle θ with Ox into a beam polarized along Ox and a beam polarized along Oy, the intensities respectively being $I\cos^2\theta$ and $I\sin^2\theta$. We reduce the intensity such that the photons arrive one by one, and we place two photodetectors D_x and D_y behind the plate. Experiment shows that D_x and D_y are never triggered simultaneously,[3] i.e., an entire photon reaches *either* D_x *or* D_y: a photon is never split. On the other hand, experiment shows that the probability $\mathsf{p}_x(\mathsf{p}_y)$ that a photon is detected by $D_x(D_y)$ is $\cos^2\theta(\sin^2\theta)$. If $\mathcal{N}$ photons are detected in the experiment, we must have $\mathcal{N}_x(\mathcal{N}_y)$ photons detected by $D_x(D_y)$:

$$\mathcal{N}_x \simeq \mathcal{N}\cos^2\theta, \quad \mathcal{N}_y \simeq \mathcal{N}\sin^2\theta,$$

where $\simeq$ is used to indicate statistical fluctuations of order $\sqrt{\mathcal{N}}$. Since the light intensity is proportional to the number of photons, we recover the Malus law in the limit $\mathcal{N} \to \infty$. However, in spite of its simplicity this experiment raises two fundamental problems.

- **Problem 1** Is it possible to predict whether a given photon will trigger D_x or D_y? The response of quantum theory is NO, which profoundly shocked Einstein ("God does not play dice!"). Some physicists have tried to assume that quantum theory is incomplete, and that there are "hidden variables" whose knowledge would permit prediction of which detector a given photon reaches. If we make some very reasonable hypotheses to which we shall return in Chapter 4, we now know that such hidden variables are experimentally excluded. The probabilities of quantum theory are *intrinsic*; they are not related to imperfect knowledge of the physical situation, as is the case, for example, in the game of tossing a coin.
- **Problem 2** Let us recombine[4] the two beams from the first birefringent plate by using a second plate located symmetrically relative to the first (Fig. 2.3) and find the probability for a photon to cross the analyzer. A photon can choose path E with probability $\cos^2\theta$. Then it has probability $\cos^2\alpha$ of passing through the analyzer, or a total probability $\cos^2\theta\cos^2\alpha$. If path O is chosen, the probability of passing through the analyzer will be $\sin^2\theta\sin^2\alpha$. The total probability is obtained by adding the probabilities of the two possible paths:

$$\mathsf{p}'_{\text{tot}} = \cos^2\theta\cos^2\alpha + \sin^2\theta\sin^2\alpha. \tag{2.8}$$

[3] Except in the case of a "dark count," where a detector is triggered spontaneously.
[4] With some care, as the difference between the ordinary and extraordinary indices of refraction must be taken into account; *cf.* Le Bellac (2006), Exercise 3.1.

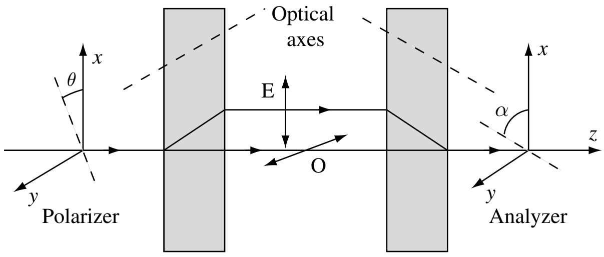

Figure 2.3 Decomposition and recombination of polarizations by means of birefringent plates. The photon can choose path E (extraordinary), where it is polarized along Ox, or path O (ordinary), where it is polarized along Oy.

This result is FALSE! In fact, we know from classical optics that the intensity is $I\cos^2(\theta-\alpha)$, and the correct result, confirmed by experiment, is

$$\mathsf{p}_{\text{tot}} = \cos^2(\theta-\alpha), \tag{2.9}$$

which is not at all the same thing!

In order to recover the results of wave optics it is necessary to introduce into quantum physics the fundamental notion of a *probability amplitude* $a(\alpha \to \beta)$. A probability amplitude is a complex number, the squared modulus of which gives the probability: $\mathsf{p}(\alpha \to \beta) = |a(\alpha \to \beta)|^2$. In the preceding example, the relevant probability amplitudes are

$$a(\theta \to x) = \cos\theta, \quad a(x \to \alpha) = \cos\alpha,$$
$$a(\theta \to y) = \sin\theta, \quad a(y \to \alpha) = \sin\alpha.$$

For example, $a(\theta \to x)$ is the probability amplitude that the photon polarized along the direction θ chooses the E path, where it is polarized along Ox. Then, a basic principle of quantum physics is that one must *add the amplitudes for indistinguishable paths*:

$$a_{\text{tot}} = \cos\theta\cos\alpha + \sin\theta\sin\alpha = \cos(\theta-\alpha),$$

which allows us to recover (2.9):

$$\mathsf{p}_{\text{tot}} = |a_{\text{tot}}|^2 = \cos^2(\theta-\alpha).$$

The superposition of probability amplitudes in a_{tot} is the exact analog of the superposition of wave amplitudes: the laws for combining quantum amplitudes are exact copies of those of wave optics, and the results of the latter are recovered in the limit of a large number of photons. Let us suppose, however, that we have some way of knowing whether a photon has followed path E or path O (this is impossible in our case, but similar experiments to determine the path, termed