Undergraduate Lecture Notes in Physics

A. I. Lvovsky

Quantum Physics

An Introduction Based on Photons

Springer

A. I. Lvovsky

Quantum Physics

An Introduction Based on Photons

Springer

A. I. Lvovsky
University of Calgary and Russian
Quantum Center
Calgary, AB
Canada

A solutions manual for this book is available for download at https://www.springer.com/gp/book/9783662565827

ISSN 2192-4791 ISSN 2192-4805 (electronic)
Undergraduate Lecture Notes in Physics
ISBN 978-3-662-56582-7 ISBN 978-3-662-56584-1 (eBook)
https://doi.org/10.1007/978-3-662-56584-1

Library of Congress Control Number: 2018933016

Printed on acid-free paper

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Contents

Chapter 1
The quantum postulates

1.1 The scope of quantum mechanics

Perhaps the first thing to understand about quantum mechanics is that it has as much to do with mechanics as with, say, electrodynamics, optics, condensed-matter, or high-energy physics. Rather than describing a particular class of physical phenomena, quantum mechanics provides a *universal theoretical framework* that can be used in *all* fields of physics — akin to a computer's operating system that provides a foundation upon which other applications can run. The term "quantum mechanics" emerged historically, because the first successful applications of the quantum framework were in studies of the mechanical motion of electrons in an atom. A better term would be "quantum physics" or "quantum theory".

So the scope of quantum physics is global: it covers all physical phenomena in the universe. However, a quantum treatment is *practical* only in the case of very small (microscopic) physical systems. The behavior of larger systems is very well approximated by the laws of classical physics, which are much simpler and more intuitive, at least for beings that have evolved on that length scale.

Let me illustrate this by an example. You have probably heard of Heisenberg's uncertainty principle: $\Delta p \Delta x \gtrsim \hbar/2$. That is, a particle's position and momentum cannot be measured precisely and simultaneously: the product of the uncertainties is at least $\hbar/2 \approx 5 \times 10^{-35}$ kg·m^2/s. For a macroscopic object with a mass on a scale of a kilogram, reaching the quantum uncertainty limit would require measuring either the position with a precision on a scale of at least $\sim 10^{-17}$ m or the velocity with precision $\sim 10^{-17}$ m/s. This is, of course, unrealistic, so for all practical purposes we may as well forget about the uncertainty principle and treat the position and momentum as precise quantities. But for an electron of mass $\sim 10^{-30}$ kg, the product of the position and velocity uncertainties will be about 5×10^{-5} m^2/s, which is well within experimentally attainable measurement precision and must be taken into account.

So the predictions of quantum theory are different from classical ones only for relatively simple, microscopic objects. This explains why quantum mechanics was

A solutions manual for this chapter is available for download at https://www.springer.com/gp/book/9783662565827

A. I. Lvovsky, *Quantum Physics*, Undergraduate Lecture Notes in Physics, https://doi.org/10.1007/978-3-662-56584-1_1

not discovered until the early 20th century. Before then, we (who ourselves are macroscopic entities) only dealt with macroscopic objects. But as soon as we developed tools to probe the microscopic world deeply enough, quantum phenomena became manifest.

This is an example of the *correspondence principle*: a philosophical maxim that states that any new, more modern, theory should reproduce the results of older well-established theories in those domains where the old theories have been tested. Here is another example of this principle. As long as we had to do with objects that move much more slowly than light, Newtonian mechanics was sufficient to describe the world around us. But as soon as we became able to observe bodies that move quickly (e.g., the Earth around the sun in the Michelson-Morley experiment), we began to see discrepancies and were compelled to develop the theory of relativity. This theory is distinctly different from Newtonian mechanics — yet it is consistent with the latter in the limiting case of low velocities. It would be unwise to use special relativity to describe, for example, a tractor transmission, because the classical approximation is in this case both sufficient and tremendously simpler. Similarly, using quantum physics to describe macroscopic phenomena would in most cases be overcomplicated and unnecessary.

In classical physics, we deal with *quantities*: a rock flying at a speed of 10 meters per second, a circuit carrying a current of 0.2 amperes, and so on. Even if we do not know a physical quantity exactly, we can work on improving our theory and experiment to predict and measure it with ever increasing precision. In other words, *the classical world is infinitely knowable*. In quantum physics, the situation is different: some knowledge (such as the simultaneous values of the position and momentum) is “sacred”: it cannot be attained even in principle. And this situation can no longer be described in terms of quantities alone. Instead, we must use the concept of the *quantum state* of a physical system. As we shall see, this concept incorporates the boundary between the knowledge that is possible and the knowledge that is impossible to obtain. We can learn precisely what state the system is in, but each state is associated with fundamental limits on the precision with which physical quantities can be known.

Because quantum mechanics has this role as a general framework, we will study it in a fairly rigorous, mathematical fashion. I will introduce definitions and axioms, then predict phenomena that arise from them, and then illustrate these phenomena with examples from different fields of physics, primarily from optics.

The main mathematical tool of quantum mechanics is linear algebra. Appendix A of this book teaches the concepts of this discipline that are relevant to quantum physics. So if you feel comfortable with your linear algebra, please proceed to the next section. Otherwise I would recommend that you study the first four sections of Appendix A before moving on.

1.2 The Hilbert Space Postulate

Let me first give a succinct formulation of the Postulate[1], and then explain its meaning in more detail.

a) Possible states of a physical system form a Hilbert space over the field of complex numbers.
b) Incompatible quantum states correspond to orthogonal vectors.
c) All vectors that represent physical quantum states are normalized.

This Postulate contains two notions that have not been defined: quantum state and physical system. They are so basic that their rigorous definition is difficult[2]. So let me try to explain these notions intuitively, using examples.

A *physical system* is an object, or even one or several degrees of freedom of an object, that can be studied independently of other degrees of freedom and other objects. For example, if our object is an atom, quantum mechanics can study its motion as a whole (one physical system) or the motion of its electrons around the nucleus (another physical system). On the other hand, if we wish to study the formation of a molecule out of two atoms, motional states of both the atoms and the electrons therein affect each other, so we must consider all these degrees of freedom as one physical system. For a molecule itself, quantum mechanics can study its center of mass motion (one physical system), rotational motion (another physical system), vibration of its atoms (a third system), quantum states of its electrons (a fourth system), and so on.

To grasp the notion of a state, consider the following physical system: a massive particle that can move along the x coordinate axis. One can define its quantum state by saying "the particle's coordinate is exactly $x = 5$ meters". This is a valid definition; we would denote this state as $|x=5\,\mathrm{m}\rangle$. Another valid state would be $|x=3\,\mathrm{m}\rangle$. These states are orthogonal ($\langle x=5\,\mathrm{m}|\, x=3\,\mathrm{m}\rangle = 0$) because they are "incompatible": if a particle's coordinate is definitely known to be 5 meters, it cannot be detected at $x = 3$ meters. On the other hand, the particle can be in the state "moving at a speed $v = 4$ meters per second". This is also a valid quantum state. Because the momentum of the particle is certain in this state, the position is completely uncertain, which means that the particle in this state can, with some probability, be detected at $x = 5$ m. Hence the inner product $\langle x=5\,\mathrm{m}|\, v=4\,\mathrm{m}/s\rangle$ does not vanish; these states are not incompatible.

The Postulate also says that if $|x=5\,\mathrm{m}\rangle$ and $|x=3\,\mathrm{m}\rangle$ are valid quantum states, then $(|x=5\,\mathrm{m}\rangle + |x=3\,\mathrm{m}\rangle)/\sqrt{2}$ (where $1/\sqrt{2}$ is the normalization factor — see Ex. 1.1 for the explanation) is also a valid state. It is called a *superposition* state.

[1] There are no universally accepted postulates of quantum mechanics. If you say "This follows from Newton's Second Law", people will understand you, but if you say "This follows from the First Postulate of quantum mechanics", they won't. You should instead say, for example, "It follows from the linearity of the quantum Hilbert space".

[2] As in geometry, which is an extremely rigorous science, despite the fact that its primary notions such as the point, straight line, and plane are not defined.

More spectacularly, if $|\text{living cat}\rangle$ and $|\text{dead cat}\rangle$ are valid states of the physical system "cat", so is the superposition of these states[3].

Are superposition states a mathematical abstraction or do they manifest themselves in their physical behavior? The answer is, certainly, the latter. As we shall see shortly, if we subject, e.g., a cat in states $(|\text{living cat}\rangle + |\text{dead cat}\rangle)/\sqrt{2}$, $(|\text{living cat}\rangle - |\text{dead cat}\rangle)/\sqrt{2}$ and just a probabilistic mixture of either $|\text{living cat}\rangle$ or $|\text{dead cat}\rangle$ to a *quantum measurement*, we will observe distinctly different results.

Another natural question to ask here is the following. We don't see superposition states in everyday life — and yet they are fully compatible with the canons of quantum mechanics. Why is that so? As we shall see in the next chapter, this is because superpositions of macroscopically distinct states are extremely fragile and quickly transform into one of their components — in the case of Schrödinger's cat, into either the dead state or the alive state. In the microscopic world, on the other hand, superposition states are relatively robust and are necessary for its physical description. The need to deal with entities whose very existence is in conflict with our everyday experience is one of the reasons why quantum mechanics is so difficult to comprehend.

Exercise 1.1. What is the normalization factor $\mathcal{N}$ of the state of the Schrödinger cat $|\psi\rangle = \mathcal{N}\,[2\,|\text{alive}\rangle + \mathrm{i}\,|\text{dead}\rangle]$ that ensures that $|\psi\rangle$ is a physical state?

Exercise 1.2. What is the dimension of the Hilbert space associated with one motional degree of freedom of a massive particle?
Hint: If you think the answer is obvious, check the solution.

1.3 Polarization of the photon

We will begin studying quantum mechanics with one of the simplest physical systems: the polarization of the photon[4]. The dimension of its Hilbert space is just two, yet it is quite sufficient to show how amazing the world of quantum mechanics can be.

Suppose we can isolate a single particle of light, a photon, from a polarized wave. The photon is a microscopic object and must be treated quantum-mechanically. We begin this treatment by defining the associated Hilbert space. We first notice that the horizontally polarized photon state, which we denote by $|H\rangle$, is incompatible with its vertical counterpart, $|V\rangle$: an $|H\rangle$ photon can never be detected in a $|V\rangle$ state. That is, if we prepare a horizontally polarized photon and send it through a polarizing beam splitter (with the properties described in Sec. C.2), it will always be transmitted and never reflected. This means that states $|H\rangle$ and $|V\rangle$ are orthogonal.

[3] This state is sometimes called Schrödinger's cat, after one of the founding fathers of quantum physics, Erwin Schrödinger. But in fact, Schrödinger discussed a more complex entity, see Box 2.5.

[4] If you are not familiar with the polarization of an electromagnetic wave, this is a good place to read the first two sections of Appendix C.

Box 1.1 Discovery of the photon

Max Planck

In 1900, *Max Planck* explained the experimentally observed spectrum of blackbody radiation by introducing the quantum of light, now known as the photon[*]. He found that a good agreement between theory and experiment can be obtained if one assumes that the energy of the photon is proportional to the frequency ω of the light wave. The proportionality coefficient, $\hbar = 1.054\,571\,48 \times 10^{-34}$, became known as Planck's constant.

In 1905, *Albert Einstein* reconfirmed the validity of Planck's formula

$$E = \hbar\omega$$

by using it to explain quantitatively the experimental results on the photoelectric effect (see Box 4.6 for more details)[**]. Later, in 1916, Einstein argued that, since it is known from classical electrodynamics[***] that an electromagnetic wavepacket carrying energy E also carries momentum $p = E/c$, the same must be true for photons. From Planck's formula he found[†] $p = \hbar\omega/c$. Expressing the frequency of the wave in terms of its wavelength, $\omega = 2\pi c/\lambda$, he then wrote

$$p = 2\pi\hbar/\lambda.$$

Arthur Compton

Arthur Holly Compton used Einstein's findings in 1923 to provide a theoretical explanation for his own experiments in which he studied the scattering of X rays on free electrons[††]. By treating X ray photons as high-energy particles, he applied the laws of momentum and energy conservation to the collision between a photon and an electron to calculate the scattered photon energy as a function of the scattering angle. He then related that energy to the wavelength, thereby obtaining a theoretical fit to his experimental data. The excellent agreement he observed serves as an explicit proof of the photon's existence.

Curiously, the term "photon" did not exist at that time. It was introduced later, in 1926, by the physical chemist Gilbert Lewis.

[*] M. Planck, *Über das Gesetz der Energieverteilung im Normalspectrum*, Annalen der Physik **4**, 553 (1901).

[**] A. Einstein, *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt*, Annalen der Physik **17**, 132 (1905).

[***] This phenomenon manifests itself, in particular, through the effect of radiation pressure, which was observed experimentally by Peter Lebedev in 1900.

[†] The expression for the photon momentum can also be obtained as follows. Using Einstein's famous relation $E = Mc^2$ together with Planck's formula, we can calculate the mass of the photon, $M = \hbar\omega/c^2$. The photon moves with the speed of light, and hence its momentum is $p = Mc = \hbar\omega/c$.

[††] A. H. Compton, *A Quantum Theory of the Scattering of X-Rays by Light Elements*, Physical Review **21** 483 (1923).

[†††] G. N. Lewis, *The conservation of photons*, Nature **118**, 874 (1926).

A light wave whose electric field is given as a function of space and time by [see Eq. (C.2)]

$$\vec{E}(z,t)=\mathrm{Re}[(A_H \mathrm{e}^{\mathrm{i}\varphi_H}\hat{\imath}+A_V \mathrm{e}^{\mathrm{i}\varphi_V}\hat{\jmath})\mathrm{e}^{\mathrm{i}kz-i\omega t}] \tag{1.1}$$

(with real $A_{H,V}$ and $\varphi_{H,V}$) consists of photons in the state[5]

$$|\psi\rangle=\frac{1}{\sqrt{A_H^2+A_V^2}}\left(A_H \mathrm{e}^{\mathrm{i}\varphi_H}\,|H\rangle+A_V \mathrm{e}^{\mathrm{i}\varphi_V}\,|V\rangle\right)\mathrm{e}^{-\mathrm{i}\omega t}. \tag{1.2}$$

For example, if $A_H=A_V$ and $\varphi_H=\varphi_V=0$, the associated classical wave is $\vec{E}=\mathrm{Re}[A_H(\hat{\imath}+\hat{\jmath})\mathrm{e}^{ikz-\mathrm{i}\omega t}]$, i.e., linearly polarized at +45°. Accordingly, the state $(|H\rangle+|V\rangle)/\sqrt{2}$ (where the factor of $\sqrt{2}$ is due to normalization) denotes a single photon with +45° linear polarization. Some further examples are listed in Table 1.1[6].

It follows that states $|H\rangle$ and $|V\rangle$ form an orthonormal basis in the Hilbert space of photon polarization states — so this space is two-dimensional. To begin with, these states are orthogonal and thus linearly independent (Ex. A.17). Furthermore, any polarized classical wave can be written in the form (1.1), so any polarization state of the photon can be written in a similar way to (1.2), i.e., as a linear combination of the states $|H\rangle$ and $|V\rangle$. We will call the basis $\{|H\rangle,|V\rangle\}$ the *canonical* basis of our Hilbert space.

Table 1.1 Important polarization states.

state	matrix	description	notation
$\vert H\rangle$	$\begin{pmatrix}1\\0\end{pmatrix}$	horizontal	$\vert H\rangle$
$\vert V\rangle$	$\begin{pmatrix}0\\1\end{pmatrix}$	vertical	$\vert V\rangle$
$\cos\theta\,\vert H\rangle+\sin\theta\,\vert V\rangle$	$\begin{pmatrix}\cos\theta\\\sin\theta\end{pmatrix}$	linear polarization at angle θ to horizontal	$\vert\theta\rangle$
$\frac{1}{\sqrt{2}}(\vert H\rangle+\vert V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	diagonal, +45° polarization	$\vert{+45^\circ}\rangle$ or $\vert+\rangle$
$\frac{1}{\sqrt{2}}(\vert H\rangle-\vert V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	(anti-)diagonal, −45° polarization	$\vert{-45^\circ}\rangle$ or $\vert-\rangle$
$\frac{1}{\sqrt{2}}(\vert H\rangle+\mathrm{i}\,\vert V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	right circular polarization	$\vert R\rangle$
$\frac{1}{\sqrt{2}}(\vert H\rangle-\mathrm{i}\,\vert V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$	left circular polarization	$\vert L\rangle$

[5] It may appear surprising that Eq. (1.2) carries no information about the position of the photon along the z axis. The reason is that the photon, as a quantum particle, is smeared across space and time, potentially to a large extent. Among the factors affecting the spread are the properties of the source, as well as the "quantization volume" chosen for the theoretical analysis. In the case of a coherent laser beam, the photon length is limited by the coherence length of the laser, which can be many kilometers. In this book, we will usually assume that the photons are spread over a distance that is much larger than the size of any apparatus, and can therefore be treated as infinitely long.

[6] See footnote 1 on page 289 for a discussion of conventions for circularly polarized states.

We have come to an apparent contradiction. On the one hand, we know that a classical wave, which consists of photons, divides. On the other hand, every individual photon is indivisible. How can these two imperatives be upheld at the same time?

It seems that the only way to solve the conundrum is to postulate that the outcome will be *random*: the photon will be transmitted through the PBS with probability $\mathrm{pr}_H = A_H^2/(A_H^2 + A_V^2) = |\langle H|\,\psi\rangle|^2$, and reflected with probability $\mathrm{pr}_V = A_V^2/(A_H^2 + A_V^2) = |\langle V|\,\psi\rangle|^2$. In this way, if a large number N of photons are incident on the PBS, the number ratio of the transmitted and reflected energies will be A_H^2/A_V^2, as expected classically (see Sec. C.2). And yet, no individual photon is divided.

As we know, the part of the classical wave that is transmitted through the PBS is horizontally polarized — that is, all photons making up the wave are of horizontal polarization. The same is true for the reflected wave: all its photons are vertically polarized. But then, the same must be true if the photons are sent to the PBS one-by-one. Not only will the photon randomly choose its path, but also, in a quite Orwellian fashion, it will *change its state* to conform with the path chosen. After the PBS, the photon state in the transmitted channel will become $|H\rangle$, and in the reflected channel $|V\rangle$. If we place a series of additional PBS's in the transmitted channel of the first PBS, the photon will be transmitted through all of these PBS's — there will be no further randomness.

The process I just described constitutes the *polarization state measurement* of a photon. To complete it, we place single-photon detectors (Box 1.2) into both output channels of the PBS. Of these two detectors, only one will click, thereby providing us with the information about the photon's polarization [Fig. 1.2(a)].

The above measurement apparatus is designed to distinguish between the horizontal and vertical polarizations. One can think of other designs as well. For example, by tilting the PBS by 45°, we can have it transmit $|+\rangle$ and reflect $|-\rangle$, so if we send an arbitrary state $|\psi\rangle$, it will transmit or reflect with probabilities $\mathrm{pr}_+ = |\langle +|\,\psi\rangle|^2$ and $\mathrm{pr}_- = |\langle -|\,\psi\rangle|^2$, respectively. More generally, we can construct a measurement apparatus that would distinguish between any two polarization states, as long as these states are orthogonal to each other.

We are now ready to formulate our Postulate.

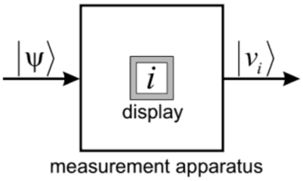


Fig. 1.1 A theoretician's picture of a quantum measurement.

Measurement Postulate. An idealized measurement apparatus is associated with some orthonormal basis $\{|v_i\rangle\}$. After the measurement, the apparatus will randomly, with probability

$$\mathrm{pr}_i = |\langle v_i|\ \psi\rangle|^2, \tag{1.3}$$

where $|\psi\rangle$ is the initial state of the system, point to one of the states $|v_i\rangle$. The system, if not destroyed, will then be converted (*projected*) onto state $|v_i\rangle$ (Fig. 1.1).

A quantum measurement that proceeds in accordance with the above Postulate is called a *projective measurement*. The projection of the state measured onto one of the basis elements is also called *collapse* of the quantum state. Equation (1.3) is called *Born's rule*.

The probabilistic behavior of quantum objects led to a lot of controversy at the time quantum mechanics was founded. This is because, by the end of the 19th century, the principle of *determinism* was universally accepted: physicists believed that, if the initial conditions of a given quantum system are known precisely enough, its future evolution can be predicted arbitrarily well. Quantum physics breached this fundamental belief, and many physicists found it extremely difficult to accept. For example, Albert Einstein made a famous statement that "God does not play dice" and came up with a brilliant *Gedankenexperiment*[7] showing that the postulates of quantum mechanics are in contradiction with common sense. We will study this Gedankenexperiment in the next chapter and see that quantum randomness can be attributed to observers themselves being quantum objects, but not being able to verify their own quantum nature experimentally. For now, however, let us accept quantum randomness as a postulate corroborated by vast experimental evidence.

Exercise 1.6. Show mathematically that, for a state $|\psi\rangle$, the sum of detection probabilities (1.3) for all basis elements is $\langle\psi|\ \psi\rangle$, i.e., it equals 1 if the state is physical.

Exercise 1.7. Show that applying an overall phase factor to a quantum state will not change the probabilities of its measurement results — in agreement with the fact that this phase has no influence on the physics of a state, as discussed in the previous section.

1.4.2 Polarization measurements

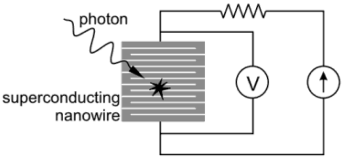
Above, we discussed the fact that one can rotate the PBS to modify the apparatus of Fig. 1.2(a) so that it can measure the polarization in a non-canonical, linearly polarized basis. However, the photon reflected from the PBS will not propagate in the horizontal direction, and this is not convenient in a practical tabletop experiment (Box 1.3). Therefore most experimentalists take advantage of the optical element called a waveplate[8] which interconverts polarization states of a photon from one to another. Here are some examples.

Exercise 1.8. Show that:

[7] "Gedankenexperiment" is the German for "thought experiment".

[8] This is a good place to read the third section of Appendix C.

Box 1.2 How to detect a photon?



A photon detector is a device that converts a photon into a "click" — a macroscopic pulse of electric current or voltage. Making such an extremely sensitive device is a challenging technological task. This figure sketches one of the modern ways of addressing this challenge: the superconducting single-photon detector.

The sensitive area of the detector is a nanowire that is cooled down to a superconducting state, with a small constant current flowing in it. The nanowire is so thin that, when it absorbs even a single photon, it warms up enough to become resistive in part of its length. The current will then heat up this area as predicted by Joule's law, further destroying superconductivity around it. In this way, a kind of avalanche process develops, in such a way that the entire nanowire becomes resistive for some time. This resistance leads to a pulse in the voltage across the nanowire that is easily detectable.

This detector suffers from a few imperfections that are typical of practical photon detectors. First, the detector is *non-discriminating*: its response to a pulse containing multiple photons is the same as its response to a single photon. This is because the entire nanowire will lose superconductivity and acquire the same resistance no matter how many photons are absorbed. Second, a photon incident on the detector may get reflected, thereby generating no click. The probability that a click will occur in response to a photon is known as the *quantum efficiency* of the detector. In some modern detectors, this parameter exceeds 99%. Finally, a detector may produce a click even in the absence of a photon. The frequency of such *dark counts* is another important technical characteristic of this device.

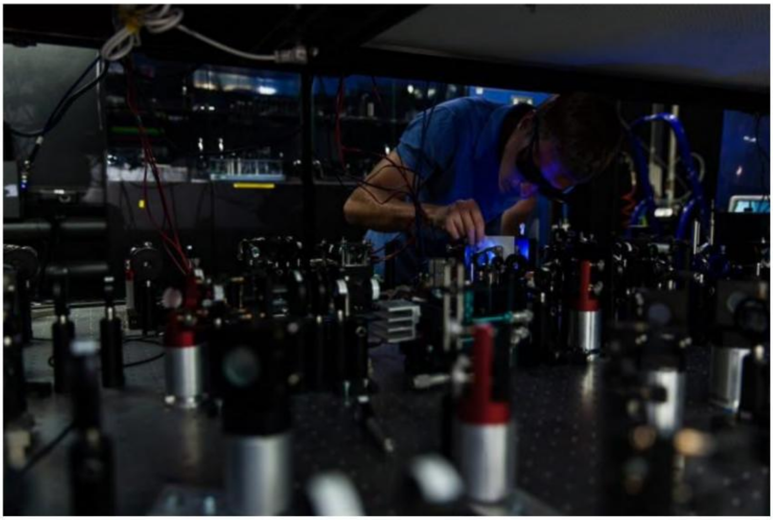
a) the setup in Fig. 1.2(b) performs the photon polarization measurement in the diagonal ($|\pm 45^\circ\rangle$) basis;
b) the setup in Fig. 1.2(c) performs the measurement in the circular ($\{|R\rangle, |L\rangle\}$) basis.

Hint: When a piece of apparatus described in the Measurement Postulate is measuring one of its own basis states $|v_i\rangle$, the measurement will point to that state with probability 1. Conversely, if the apparatus can distinguish a particular orthonormal set of states with certainty, we can conclude that this set is the measurement basis of the apparatus. Therefore, to solve this exercise, it is enough to show that the basis states [i.e., $|\pm 45^\circ\rangle$ in (b) and $|R\rangle, |L\rangle$ in (c)], when sent onto the PBS, will generate clicks in different photon detectors.

Exercise 1.9§. Each of the states $|H\rangle, |V\rangle, |+\rangle, |-\rangle, |R\rangle, |L\rangle$ is measured in

a) canonical,
b) diagonal,
c) circular

Box 1.3 Optical table



This photograph shows a typical quantum optical experiment. It is performed on an *optical table* — a massive metal plate upon which one mounts various optical elements, such as lenses, mirrors, lasers, crystals, and detectors. The beams typically run horizontally, at the same level throughout the entire table.

bases. Find the probabilities of the possible outcomes for each case.
Answer: For each state, when the measurement is performed in the basis to which the state belongs, the probabilities are 0 and 1. If the state does not belong to the measurement basis, the probabilities of both outcomes are $\frac{1}{2}$.

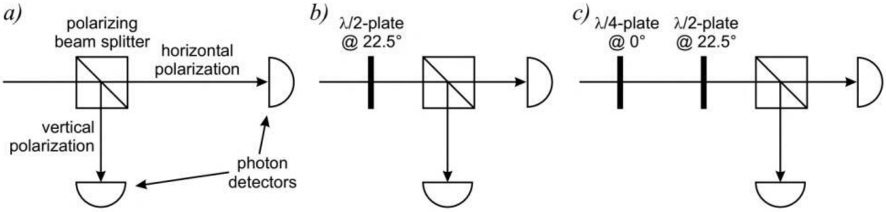


Fig. 1.2 Photon polarization measurements in the canonical $\{|H\rangle, |V\rangle\}$ (a), diagonal $\{|+\rangle, |-\rangle\}$ (b), and circular $\{|R\rangle, |L\rangle\}$ (c) bases.

Exercise 1.10. Propose a scheme for a quantum measurement in the basis $\{|\theta\rangle, \left|\frac{\pi}{2}+\theta\right\rangle\}$.

Exercise 1.11. Propose a scheme for a quantum measurement in the basis $\{|R\rangle, |L\rangle\}$ that would use just one waveplate.

Exercise 1.12. Consider a photon that is not in a superposition state, but in a random *statistical mixture*, or *ensemble*[9]: *either* $|H\rangle$ with probability $1/2$ *or* $|V\rangle$ with probability $1/2$. The polarization of this photon is measured in

a) canonical,
b) diagonal,
c) circular

bases. Find the probabilities of the possible outcomes for each case.

Exercise 1.13. A photon is prepared with a linear polarization 30° to horizontal. Find the probability of each outcome if its polarization is measured in (a) the canonical, (b) the diagonal, and (c) the circular basis.

Exercise 1.14. A photon in state $|\psi\rangle = (|H\rangle + e^{i\varphi}|V\rangle)/\sqrt{2}$ is measured in the diagonal basis. Find the probability of each outcome as a function of φ.

This exercise, along with Ex. 1.7, shows once again the important difference between a phase factor applied to a part of a quantum state or applied to the whole. In the former case the added phase has an effect on the measurable properties of the object; in the latter, it doesn't.

Although a single measurement provides us with some information about the initial state of a quantum system, this information is very limited. For example, suppose we have measured a photon in the canonical basis and found that it has been transmitted through the PBS. Does this tell us that the initial photon was in the state $|H\rangle$? No. It could have been in any state $\psi_H|H\rangle + \psi_V|V\rangle$; as long as $\psi_H \neq 0$, there is some probability of getting a click in the transmitted channel. So the only thing we learn from this measurement is that the photon was not vertically polarized.

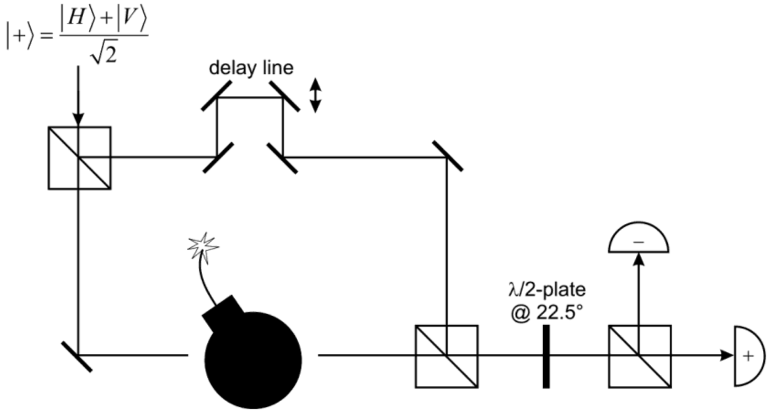
Suppose now we have performed the same measurement many times, every time preparing our photon in the same state[10]. Now we know much more! We know how many clicks we obtained from the "horizontal" detector, and how many from the "vertical" one — that is, we have *measurement statistics*. From these, we can calculate, with some error, $\mathrm{pr}_H = |\psi_H|^2$ and $\mathrm{pr}_V = |\psi_V|^2$, i.e., learn about the absolute values of the state components. But both ψ_H and ψ_V are complex numbers, and their arguments are still unknown. For example, if we observe $\mathrm{pr}_H = \mathrm{pr}_V = 1/2$, the state $|\psi\rangle$ could be $|R\rangle$ or $|L\rangle$ or $|+\rangle$ or $|-\rangle$, or many other options. What can we do about this?

As you will see in the following exercise, it is helpful to perform additional sets of measurements in other bases. From the statistics acquired, we obtain additional equations, which can be solved to find ψ_H and ψ_V up to an uncertainty associated with a common phase factor.

[9] Such *mixed states* are not elements of the quantum Hilbert space. More detail on this in Sec. 2.2.4.

[10] Although we don't know what the state is, we can make sure we can repeatedly prepare the photon in the same state by setting up identical experimental conditions.

Box 1.4 Quantum weapon inspection



Here is an exciting paradox associated with the single-photon interference experiment discussed in Sec. 1.5*. Suppose there is a “bomb” equipped with a photon sensor, so that it will explode if even a single photon interacts with it. Can we detect the presence of the bomb in one of the arms of our interferometer without detonating it?

Let us set up the delay line in our single-photon interferometer (Fig. 1.3) such that $\varphi = 0$. Then, if the bomb is *absent*, every incoming photon will leave the interferometer polarized at $+45^\circ$ and cause an event in detector “$+$”. Detector “$-$”, on the other hand, will never click.

Now if the bomb is *present*, as shown in the figure above, it may explode or not, depending on which way the photon goes. In this way, the bomb implements a Welcher-Weg measurement. Accordingly, the photon will behave like a particle that goes randomly into either the lower or the upper part of the interferometer. If it goes into the lower path, the bomb will explode. But if it goes into the upper part, the bomb will remain intact and the photon will exit the interferometer in the vertical polarization state. When measured in a diagonal basis, this photon will be equally likely to generate an event in either of the two detectors.

Hence, if the bomb is present, there will be a nonzero probability of hearing a click in detector “$-$”. Moreover, this detector can click *only* in the presence of the bomb. If this detector does click, we know for certain that the bomb is present — without having interacted with it!

The above setup is not a perfect tool for weapon inspection, as it does not guarantee a conclusive result, nor that the bomb will not detonate (Ex. 1.17). However, if one places the bomb in a high-finesse Fabry-Perot interferometer rather than a Mach-Zehnder interferometer, one can achieve an efficiency close to 100%. In this case, the photon will likely pass through the interferometer when the bomb is absent, but reflect if the bomb is present.

*A. C. Elitzur, L. Vaidman, *Quantum mechanical interaction-free measurements*, Foundations of Physics **23**, 987 (1993).

components of the superposition that play the role of the two waves in the classical experiment, interfering with each other. This is known as the *wave-particle duality* of quantum particles[14].

So, in a sense, the photon does get divided between the two interferometer channels. However, this wavelike behavior is only possible if the components remain in the superposition state. To illustrate this, let us suppose that we place non-destructive detectors in both interferometer arms, able to register the presence of the photon without destroying it. Every time a photon is sent into the interferometer, one of these detectors will "click", indicating whether the photon went through the upper or the lower path. In this way, as the founding fathers of quantum mechanics would say, we obtain *Welcher-Weg* (which-way) information about the photon.

Obtaining Welcher-Weg information means *measuring* the location of the photon. As we learned in the previous section, such a measurement will collapse the superposition state onto the photon being either in the upper or lower path of the interferometer. By looking at the Welcher-Weg detector, the observer is able to tell with certainty whether the photon will leave the interferometer in the horizontal or vertical state. In either case, a subsequent measurement of that photon in the diagonal basis will yield either outcome with probability $1/2$, with no dependence on the path-length difference. The Welcher-Weg measurement destroys the wavelike property of the photon and makes it behave like a particle.

This is, of course, the case even if the observer does not look at the Welcher-Weg detectors. The photon is then in a mixed state of being *either* in the upper or lower path of the interferometer with probability $1/2$, but no longer in the superposition state. That is, we are now in the situation of Ex. 1.12 rather than 1.14. The photon state has lost its *quantum coherence* — a well-defined phase relation between the superposition terms. Hence it is no longer able to exhibit interference.

This Gedankenexperiment demonstrates *quantum complementarity* — a general principle of quantum physics stating that objects may have complementary properties which cannot be observed or measured at the same time. We can have either the Welcher-Weg information or interference, but not the two together.

Exercise 1.17. In the setting of Box 1.4, what are the probabilities of

a) detecting a bomb without detonating it,
b) detonating the bomb,
c) obtaining an inconclusive result without detonating the bomb?

1.6 Quantum cryptography

We can now discuss the first application of quantum physics in this course. This application is to *cryptography* — the art of exchanging secret messages over insecure channels.

[14] This is probably why popular quantum books like to describe superposition states as ones in which "an object is in two different places at the same time".

Box 1.5 Classical cryptography

Cryptography is easily implemented if the communication parties, which we call Alice and Bob, share a prearranged, secret data set (a sequence of 0's and 1's) known as *secret key* or *one-time pad*. With this resource available, a cryptographic protocol can proceed as follows. Alice chooses a piece of the secret key which has the same length (i.e., the same number of bits) as the message she wishes to send to Bob. She then applies an XOR (exclusive OR, or bitwise sum modulo 2) operation to every bit of her message and the corresponding bit of her secret key:

$$\begin{array}{r} \text{original message } \texttt{01110011...} \\ \text{XOR} \\ \text{secret key } \texttt{10011010...} \\ \hline \text{encrypted message } \texttt{11101001...} \end{array}$$

In this way she obtains an *encrypted message* which can be safely transmitted over an insecure channel, as it cannot be decrypted by anyone who is not privy to the secret key. Bob, on the other hand, can easily decrypt the message. To this end, he applies XOR to every bit of the encrypted message he receives and the corresponding bit of the secret key, thereby recovering the original message.

$$\begin{array}{r} \text{encrypted message } \texttt{11101001...} \\ \text{XOR} \\ \text{secret key } \texttt{10011010...} \\ \hline \text{recovered original message } \texttt{01110011...} \end{array}$$

This protocol, known as *private-key cryptography*, is very secure and simple; it has been known for hundreds of years. The trouble is, it is not easy for Alice and Bob to arrange sharing random data that would be secret to everyone else. As a rule, the only safe way to do this would be to send a courier carrying a briefcase loaded with random data. This is, of course, very expensive. For this reason, private-key cryptography is only used in the most sensitive government and commercial communications.

For other applications, such as e-commerce, a family of protocols known as *public-key cryptography* is used. Without going into details, these protocols rely on the existence of "one-way" functions that are easy to compute, but very difficult to invert. For example, multiplying two prime numbers containing a few dozen digits will take microseconds on a modern computer, but factoring a number of similar length will take months or years. Public-key cryptography protocols rely on one-way functions to enable secure communication between parties who have never had an opportunity to exchange a secret key.

While public-key protocols are convenient and inexpensive, they are not perfectly secure. The computational power available to us doubles every year or two, so a calculation that takes years at present may take only hours a few years in the future. Furthermore, *quantum computers* (Sec. 2.5) are potentially capable of cracking the security of public-key protocols almost instantly.

Known since ancient times, cryptography is now a major branch of the telecommunications industry, aimed at protecting the privacy and information security of individuals, businesses and government entities. Box 1.5 reviews classical approaches to cryptography. To sum it up, within the classical domain we are compelled to choose between private-key cryptography, which is secure but expensive, and public-key cryptography, which is cheap, but not perfectly secure.

Quantum mechanics offers us a solution that takes “the best from both worlds”. On the one hand, its security is guaranteed by fundamental laws of nature. On the other hand, it does not require random information to have been shared previously between the parties.

1.6.1 The BB84 protocol

Quantum cryptography, or, more precisely, *quantum key distribution*, relies on the property of measurements to alter the quantum state they are used on. The idea is that the sending party (Alice) sends secret data to the receiving party (Bob) by means of single photons, encoding the data in their quantum states. Anyone who tries to eavesdrop on this transmission will either destroy or alter these photons, thereby revealing themselves.

The best known quantum cryptography protocol is named “BB84” after its inventors C.H. Bennett and G. Brassard[15]. To implement it, Alice and Bob perform the following operations.

1. Alice tosses a coin to randomly choose the value of a bit, either 0 or 1, to be sent.
2. Alice tosses a coin again to choose the encoding basis, either canonical or diagonal.
3. Alice generates a photon and encodes the bit in that photon’s polarization:

$$\begin{cases} 0 \to |H\rangle \\ 1 \to |V\rangle \end{cases} \text{or} \begin{cases} 0 \to |+45^\circ\rangle \\ 1 \to |-45^\circ\rangle \end{cases}$$

   She then sends the photon to Bob.
4. Bob tosses a coin to choose the measurement basis, either canonical or diagonal.
5. Bob measures the arriving photon in the chosen basis:
   - if he chooses the same basis as Alice, he will detect the same bit value as the one Alice sent;
   - if he chooses the other basis, he will detect a random bit value.

This procedure is repeated many times. Of course, both Alice and Bob must keep record of the bases they used, states sent or detected, and the exact time when the

[15] C. H. Bennett, G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing”, Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

photons were sent or received. After many thousands of such records have been collected, Alice and Bob inform each other (via a classical, insecure channel) of their choice of bases for each photon, but *not* the bit values they sent or measured. Bob also informs Alice of those instances when he did not detect a photon, e.g., if it has been absorbed in the transmission line (this requires, of course, that the timing of Alice's transmissions be known to Bob, but this information need not be secret). Subsequently, Alice and Bob discard the data for those events in which different bases were used or the photon has been lost.

Alice and Bob now share a string of identical bits, which they can use as the one-time pad in a private-key protocol. To see why this string is guaranteed to be secret, let us suppose an eavesdropper (Eve) cuts the transmission line, intercepts Alice's photons, measures their polarization, and re-sends them to Bob (Fig. 1.4). Will she be able to obtain a copy of the secret key?

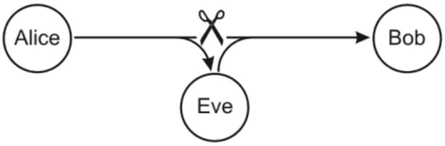


Fig. 1.4 Eavesdropping in quantum cryptography.

The answer is negative. Eve's problem is that, according to the Measurement Postulate, she must measure in a particular basis, and does not know which basis to choose. No matter how she chooses that basis, it will sometimes happen that Alice and Bob work in the same basis and Eve in a different one. But in this case Eve's measurement will alter the photon's state and Bob may not receive the same bit value as the one Alice sent him. The secret keys that Alice and Bob record will end up being different, and this will alert them to the eavesdropping.

Suppose, for example, that Alice and Bob both work in the canonical basis, but Eve in the diagonal basis. Alice sends a horizontally polarized photon, encoding bit value 0. But Eve uses the diagonal basis, so she will detect $|+\rangle$ or $|-\rangle$ with equal probabilities. If she detects and resends either of these states, Bob (who detects in the canonical basis) is equally likely to observe $|H\rangle$ or $|V\rangle$. Bob's observation of $|V\rangle$ will cause him to record a different bit value compared to the one Alice has sent.

In order to check whether the eavesdropper was present, Alice and Bob exchange, via an insecure channel, a part of the secret bit string they obtained. If there are no (or very few) errors, they can use the remainder of that string as the one-time pad.

Exercise 1.18. Suppose Eve intercepts Alice's photons and measures them in either the canonical or diagonal basis (she chooses at random). She then encodes the bit she measured in the same basis and re-sends it to Bob. What *error rate* will Alice and Bob register, i.e., what fraction of bits in the secret key they created will come out differently on average?

- frequency of dark events that are synchronized with Alice's photons[17] in each of Bob's detectors: $f_d = 10\ \mathrm{s}^{-1}$;

Answer: see Fig. 1.5.

The range of secure quantum communication can be improved by increasing Alice's photon emission rate or reducing the detector dark counts. However, this will not lead to dramatic results: the exponential nature of Beer's law prevents quantum communication at distances beyond a few hundred kilometers. In the setting of Ex. 1.21, increasing the emission rate by three orders of magnitude increases the communication distance by only a factor of 1.7 (Fig. 1.5).

To overcome this limit — and create the "quantum internet" that would cross oceans and eventually cover the entire planet — we need a fundamentally different technology. This technology, known as the *quantum repeater*, is discussed at the end of Chapter 2.

1.7 Operators in quantum mechanics

We now proceed to discussing linear operators, which are a key element of quantum physics[18]. They play a dual role. First, they describe evolution: as time passes, quantum states change, and this change is described mathematically by operators. A second, less obvious application of linear operators is the formal description of quantum measurements. We shall start with the first role in this section.

Exercise 1.22. Find the matrix of the operator $|+\rangle\langle-|$ in the canonical and the $(|R\rangle, |L\rangle)$ bases.

Exercise 1.23. Find, in the canonical basis, the matrix of the linear operator $\hat{A}$ that maps

a) $|H\rangle$ onto $|R\rangle$ and $|V\rangle$ onto $2|H\rangle$;
b) $|+\rangle$ onto $|R\rangle$ and $|-\rangle$ onto $|H\rangle$.

The waveplate, which transforms photon polarization states, is an example of a physical operation that can be associated with a quantum operator. In order to calculate this operator, we need to adopt a convention. As discussed in Sec. C.3, the waveplate changes the relative phase of the extraordinary (parallel to the optic axis) and ordinary (orthogonal to the optical axis) polarization states by an angle $\Delta\varphi$, which is equal to π for a half-wave plate and $\pi/2$ for a quarter-wave plate. In addition, it introduces a common phase shift for the entire wave.

These optical phase shifts transform into quantum phase shifts when applied to the single photon. The overall phase shift, common for all polarization components,

[17] The actual dark count rate can be higher. But because Bob knows the exact timing of Alice's transmission, the only dark count events that contribute to the error rate are those that occur synchronously with the clicks expected due to Alice's photons.

[18] A fuller introduction into linear operators and matrices can be found in Sections A.5 and A.6.