Quantum Information Processing and Quantum Computation

Draft version fall 2026

Nicolas Macris, EPFL

Contents

Introduction

Information processing and computation are, ultimately, physical processes. Indeed, information is stored and processed in biological systems (living systems), mechanical systems (Babbage's machine), electronic systems (modern computers), optical systems, etc.

Nevertheless, in classical information theory and classical computation, one can to a large extent abstract away from the physical laws governing the underlying systems. Thus it is generally sufficient to retain only the mathematical aspect of the concept of "information". This is makes the theory universal and, to a large extent, independent of the technology used. Only a few basic physical assumptions are retained. For example, the notion of a classical bit assumes stability and reproducibility of elementary signals, as well as the possibility of carrying out measurements without disturbing the state of the system. An electrical voltage or a magnetic domain is stable enough to be modeled by a well-defined digital signal $x \in \{0, 1\}$. Moreover, it is in principle possible to measure and observe the state $x \in \{0, 1\}$ without causing any significant disturbance.

However, the components of electronic and optical information-processing systems are approaching nanometer scales, and the limits of validity of classical physics are being reached. The processing of information stored on atomic, molecular, or nanometric length and time scales must take into account the laws of quantum physics that apply at those scales. The purely mathematical character of classical information theory is no longer sufficient there and must be reconsidered in the light of quantum laws of nature. In fact, radical conceptual changes with respect to classical concepts are required.

The notion of a classical bit, $x \in \{0, 1\}$, which is the basic unit of classical information, must be revised. We shall introduce the notion of a "quantum bit"—the qubit—which has a character that is somehow "both discrete and continuous". Quite surprisingly, we shall see that a quantum bit is a vector with two continuous complex components, yet it responds discretely when information is extracted from it! The qubit is the basic unit of quantum information. The notions of observation, measurement and stability of a qubit state must also be deeply revised.

The new discipline that correctly describes information processing and its implementation at atomic or molecular scales is called *Quantum Information and Computation*. While the technologies associated with this discipline are still emerging, the basic concepts and ideas of quantum information and computation first appeared in the pioneering work of Landauer, Benioff, Feynman, Bennett, Wiesner, Deutsch and others almost forty years ago (around 1980). These works were not necessarily motivated by

technological developments, but rather by deep scientific questions about the physical nature of information and computation, and in particular about the fundamental limits imposed by the laws of physics (notably thermodynamics and quantum physics). During the last 30 years the subject has grown spectacularly. On one hand the theory is well developed with quantum algorithms, quantum error correcting codes, new quantum simulation methods, communication protocols. On the other hand there are now many technological directions investigated (in academia and industry) for computing platforms and the so-called Noisy Intermediate Scale Quantum (NISQ) computing devices are a reality.

Part I is an elementary introduction to quantum physics. No prerequisites are required apart from some basic notions of linear algebra. Quantum physics arose from experimental discoveries that revolutionized physics at the turn of the twentieth century. The development of quantum theory was the result of a long process initiated, among others, in the work of M. Planck, A. Einstein, N. Bohr, L. de Broglie, E. Schrödinger, M. Born, E. Heisenberg and P. Dirac between 1900 and 1930. The modern formulation of the theory presented in Chapter 4 was developed by P. Dirac and J. von Neumann toward the end of that period and remains essentially unchanged today.

Chapter 1 gives a semi-historical description of the basic experiments (interference experiments and the photoelectric effect) that reveal wave-particle duality. This dual nature of matter lies at the origin of the notion of quantum state and also of the notion of quantum bit—the qubit—which has a continuous/discrete dual nature. The qubit generalizes the classical bit and forms the basic unit of quantum information theory and quantum computation.

Nature abounds in degrees of freedom that are exactly or approximately represented by qubits. Qubits are therefore a natural resource! Two fundamental examples of exact qubits are introduced in Chapter 2: photon polarization and the spin-$1/2$ degree of freedom of electrons. Several principles of quantum physics are illustrated with these examples.

Chapter 3 introduces the quantum laws and the mathematical formalism that we shall use in a more systematic way. In quantum information theory and quantum computation we mainly need quantum mechanics for discrete degrees of freedom, and we therefore restrict ourselves to this setting, which is in fact a major simplification. Quantum mechanics of continuous degrees of freedom will not be discussed in this course, although it is of course a very important subject. The situation is analogous to the classical case, where digital information processing requires little or none of the theory of continuous-signal processing.

Chapter 4 introduces the density matrix formalism which is necessary to describe non-isolated systems interacting with their environment, or subjected to noise. We come back to density matrices and notably reduced density matrices when we introduce von Neumann's entropy and also "entanglement entropy" which displays genuine quantum behaviors.

Part II is an introduction to the fundamental aspects of quantum information and computation.

Chapters 5 and 6 introduce protocols at the basis of quantum communication theory.

First, in Chapter 5, we present the celebrated Bennett–Brassard protocol (1984), which allows a secret key to be distributed between two distant parties, Alice and Bob. Studying this protocol provides a good illustration of the quantum-mechanical "measurement postulate" introduced in Chapters 2 and 3.

Chapter 6 discusses the protocols of "superdense coding" and "teleportation". These very important protocols reveal a new resource available in quantum information, with no classical counterpart. This resource comes from the possibility of "entangling" two systems (for example Alice's and Bob's qubits). As we shall see, entanglement is a form of correlation that has no classical analogue: in particular, this type of quantum correlation cannot be described by classical random variables. We shall see how this follows from J. Bell's inequalities (1964 - in the form of CHSH) and the experiments of Aspect–Grangier–Roger (1981).

Chapter 7 is an introduction to the formalism of quantum information. We introduce entropy, entanglement entropy, basic inequalities and discuss classical analogies and differences. We also discuss "accessible information" when a measurement is performed and Holevo's bound. Chapter 8 is a parenthesis introducing information theoretic protocols related to dilution and distillation of Bell pairs.

Quantum computation and quantum algorithms are introduced in Chapters 9 to 12. In Chapter 9 we introduce the popular model of computation due to D. Deutsch (1985)—the quantum-circuit model—which is a generalization of the classical circuit model. Quantum circuits are built from universal "quantum logic gates" that generalize classical AND, OR, XOR and TOFFOLI gates and make it possible to simulate a broad class of "computations". From this viewpoint a quantum algorithm is a circuit initialized in an appropriate state of several qubits and producing an output state. The measurement (observation) process applied to the output qubits produces the result of the computation. As we shall see, this measurement process gives a random result, and from this point of view quantum algorithms are randomized algorithms. The quantum circuit itself, however, is deterministic.

The most spectacular algorithm (in theory) is probably Shor's algorithm (1994), which factors integers in time polynomial in the number of bits (or decimal digits) of the integer. This algorithm is studied in detail in Chapter 11. The best classical algorithms known today require quasi-exponential time. Compared with these classical algorithms, Shor's algorithm offers a quasi-exponential speedup in computation time. This follows from the possibility of processing entangled qubits in parallel by means of quantum circuits. The complexity of factorization is at the basis of public-key cryptographic systems, and the advent of a quantum computer capable of implementing Shor's algorithm would be revolutionary.

As we will see many basic ideas are already present in Simon's algorithm in Chapter 10 which concerns the search of a hidden group in a larger group. Both Simon and Shor algorithms are based on an important primitive the "Quantum Fourier Transform" (QFT) which enters in other algorithms not treated here (such as Quantum Phase Estimation, HLL, ...).

Chapter 12 dwelves into Grover's algorithm, which is based on different ideas. Chap-

ter 13 is a brief parenthesis on distributed quantum computation. This is a good occasion to review computation and communication primitives put together.

Quantum bits are very fragile objects and constantly interacting with tehir environmental noise. Therefore in order to implement the algorithms in real devices one shall need erorr correcting methods. The first quantum error correcting codes where developped by Shor. This is introduced in Chapter 14. Fault tolerant computation is a whole subject by itself and we only scratch teh surface of it.

Part III addresses the *simplest* actual physical realizations of quantum information systems. For communication protocols such as key distribution, superdense coding or teleportation, there already exists an emerging technology based on the production, manipulation and transmission of quantum states of photons. For example, the feasibility of secret-key distribution protocols similar to Bennett and Brassard's has been demonstrated over distances of about one hundred kilometers. A detailed study of these experiments would require quantum optics, which lies well beyond the scope of this course. Here we concentrate on implementing logic gates and quantum circuits using nuclear magnetic resonance (NMR). In these physical realizations, the qubits are nuclear magnetic moments and are manipulated by electromagnetic pulses. The NMR framework allows us to discuss some existing experimental realizations, including the implementation of Shor's algorithm for a small number of qubits (of order ten). The major challenge today is to work with a large number of qubits (of order $10^4 - 10^7$). Technologies more suitable than NMR are being explored in laboratories for this purpose, but their discussion lies far beyond the scope of this course. Nevertheless, the principles of qubit manipulation are similar to those we shall study in the NMR setting.

Chapter 15 discusses the dynamics of spin $1/2$ in magnetic fields. This will allow us to describe the implementation of one-qubit logic gates such as NOT and Hadamard (the latter has no analogue in classical circuits).

Chapter 16 discusses two-qubit gates such as XOR or controlled-NOT. Their implementation is more difficult because one must control the interaction between two qubits. Fortunately, as we shall see, nature provides suitable interactions between magnetic moments (Heisenberg interactions).

Chapter 17 concludes the course with an overview of the realization of quantum circuits and algorithms with NMR technology. We briefly discuss experiments that successfully implement Shor's algorithm for about ten qubits (~ 2000). It is known that this NMR technology is not scalable, and is therefore not pursued in labs and industry, for what concerns quantum computing (of course NMR has other very important applications, e.g., in spectroscopy, biology, medicine with MRI, ect).

For quantum computing devices nowadays a host of other technologies are being pursued among which superconducting qubit platforms, trapped ions and atoms, spin-qubits, etc. Going into such subjects requires more advanced notions, but the dynamics of spin in magnetic fields in chapter 15 and 16 is still the underlying basis for all that.

As explained above, building a quantum computer capable of processing of order $10^4 - 10^7$ qubits is currently a major challenge. The reason is that, as the number of degrees of freedom of the system increases, the "coherence" of the quantum state is increasingly lost because of interactions between the system and its environment; the

system then behaves more and more like one obeying the laws of classical physics. This is the problem of decoherence, already discussed by Schrödinger in 1935 in the form of the paradox of "Schrödinger's cat". Decoherence will be discussed briefly at the end of the course. In a few words, the question is whether a macroscopic system—a cat or a quantum computer—can be kept in a coherent quantum state for sufficiently long (or, more precisely, for how long). Although the answer is not entirely settled, most physicists today agree that there is no fundamental obstacle in principle to maintaining the quantum coherence of a system provided that its degrees of freedom are sufficiently well isolated from their environment.

I would like to thank David Blanchet and Thomas Rubelli, who contributed to the preparation of these notes, as well as the many students whose questions, remarks and comments helped improve them.

Part I

Introduction to Quantum Theory

1 Wave–Particle Duality

Quantum mechanics emerged from a long experimental and conceptual development at the beginning of the twentieth century ($\sim$ 1900–1930). Around 1900, the framework of classical physics appeared essentially complete. On the one hand, Newtonian mechanics described the motion of material particles; on the other, Maxwell's theory described electromagnetic phenomena. The distinction between particles and waves seemed clear. An electron, for example, was regarded as a particle with a well-defined position $\vec{x} = (x, y, z) \in \mathbb{R}^3$, velocity, and momentum $\vec{p} = m\vec{v}$ ($\vec{v} = \frac{\mathrm{d}\vec{x}}{\mathrm{d}t}$).. Given initial conditions $\vec{x}(0)$ and $\vec{v}(0)$, Newton's differential equation determines the trajectory $\vec{x}(t)$, and hence also $\vec{v}(t)$. Any limitation in the precision of this description was viewed as merely technological, to be reduced by increasingly accurate instruments. By contrast, following Maxwell's work and Hertz's experiments, visible light was known to be an electromagnetic wave of the same nature as radio waves, differing only in wavelength and frequency. Electromagnetic waves are propagating oscillations of the electric and magnetic fields governed by Maxwell's partial differential equations. These equations are deterministic: once the initial conditions are specified, the electromagnetic field is determined at all later times.

The experiments that triggered the conceptual revolution leading to quantum mechanics concerned the interaction between matter and radiation.

First, in 1900, the spectral distribution of radiation in a "black body" led Planck to propose that light is absorbed and emitted by material walls in discrete amounts. Classical electromagnetic wave theory predicted a continuous exchange of energy and could not reproduce the observed black-body spectrum[1].

Next, the "photoelectric effect" (Section **1.2**), clearly demonstrated by Lénard in 1902 following earlier work by Hertz ($\approx$ 1885), led Einstein to postulate that light is made of particles, now called photons.

The observation of discrete emission and absorption lines for various chemical elements also indicated that energy exchange between atoms and radiation is quantized. Bohr (1910) incorporated the new photon concept into his model of the atom. His theory explained the known spectral lines and even predicted new ones that were observed much later (Section **1.6**).

Since light appeared to exhibit both particle-like and wave-like behavior, de Broglie proposed that the same duality might apply to electrons, and indeed to all forms of

[1] A "black body" may be idealized as a material cavity, such as an oven, whose walls are in thermal equilibrium with the radiation. We shall not discuss this topic further in this course.

matter. In 1924 he introduced a formula associating a wavelength, now called the de Broglie wavelength, with an electron. Using this relation, one can recover Bohr's results for the spectral lines of hydrogen. De Broglie's proposal was confirmed experimentally by Davisson and Germer through electron-diffraction experiments on crystals. Their 1927 experiments provided striking evidence that electrons can behave as waves.

Between 1925 and 1930, the modern theory of quantum mechanics, still in universal use today, was developed by Schrödinger, Heisenberg, Born, Jordan, Dirac, and others. Starting from de Broglie's ideas, Schrödinger (1926) derived the equation governing the time evolution of the wave associated with a particle (Section **1.7**). This equation provided a first-principles calculation of the spectrum of the hydrogen atom and ultimately became one of the foundations of modern chemistry. Heisenberg (1925–26) developed a different formulation, based more directly on the experimentally known properties of atom–radiation interactions, such as spectral lines. His abstract approach represented quantities such as the position and momentum of electrons by matrices and became known as matrix mechanics. Born, Jordan, and Dirac soon showed that Schrödinger's and Heisenberg's approaches were mathematically equivalent formulations of the same theory.

Today physicists rarely distinguish sharply between the wave and algebraic formulations. They were largely unified by Dirac and von Neumann ($\sim$ 1930–1932), who gave quantum mechanics a precise mathematical framework. This formalism, presented in Chapter **3**, remains essentially unchanged and provides the standard language for quantum phenomena. The present Chapter **1** and Chapter **2** introduce several basic ideas from the experimental phenomenology, so that the subsequent mathematical formulation of quantum theory will appear less arbitrary.

The historical development sketched above is too long and intricate to discuss in detail here. We therefore focus on two key experiments that illustrate essential features of quantum phenomena: Young's double-slit experiment (Section **1.1**) and the photoelectric effect (Section **1.2**).

1.1 Double-Slit Experiments

Young's Experiment – 1803

The wave nature of light was advocated early on by Hooke, Huygens, and Euler. Newton, however, favored a corpuscular description, and this view remained dominant until the nineteenth century. The debate was temporarily settled by Young's 1803 experiment, which demonstrated interference and established that light behaves as a wave. Young was also able to estimate the wavelengths of visible light.

The experimental setup is sketched in Figure **1.1**.

A monochromatic beam is sent toward a screen E_1 containing a narrow slit. The diffracted beam then reaches E_2. This first step simply produces an approximately point-like coherent source at the slit in E_1. The light is subsequently diffracted by the two slits

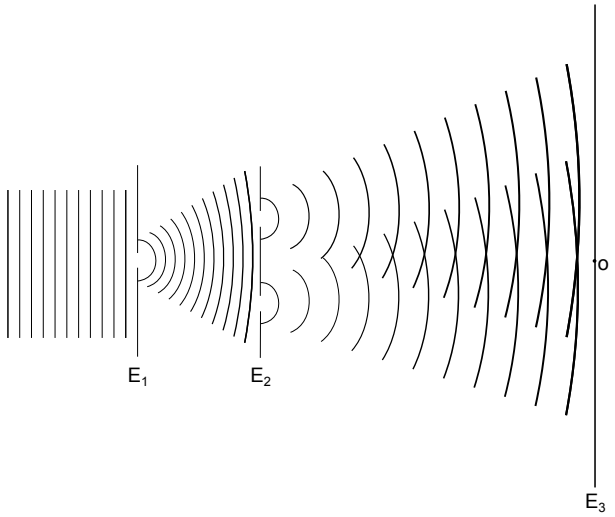


Figure 1.1 Young's double-slit experiment.

in E_2, which act as two point sources. If $\vec{r}_1$ and $\vec{r}_2$ denote the slit positions, the two outgoing spherical waves have the form

$$\psi_1(\vec{r}) = A\frac{e^{i(k|\vec{r}-\vec{r_1}|-\omega t)}}{|\vec{r}-\vec{r_1}|} \tag{1.1}$$

and

$$\psi_2(\vec{r}) = A\frac{e^{i(k|\vec{r}-\vec{r_2}|-\omega t)}}{|\vec{r}-\vec{r_2}|} \tag{1.2}$$

Here $\psi_1(\vec{r})$ and $\psi_2(\vec{r})$ are the amplitudes of the two waves at the point $\vec{r}$. The wave number k is related to the wavelength by $k = \frac{2\pi}{\lambda}$, and the angular frequency ω is related to the ordinary frequency by $\omega = 2\pi\nu$. For light, $\lambda\nu = \frac{\omega}{k} = c$, where $c \approx 2.997 \times 10^8$ m/s is the speed of light in vacuum. In the figure, the circles indicate successive maxima of the two wave amplitudes; the regions between them correspond to minima. The two waves superpose. According to the superposition principle, the total amplitude at $\vec{r}$ is

$$\psi(\vec{r}) = \psi_1(\vec{r}) + \psi_2(\vec{r}). \tag{1.3}$$

Where the two waves are in phase, their maxima reinforce one another. This produces the familiar interference pattern. A simple analogue can be observed by dropping two stones into still water. Young obtained a quantitative observation by measuring the light intensity on the screen E_3. The intensity is proportional to $|\psi(\vec{r})|^2$, with $\vec{r} \in E_3$. One can show that

$$|\psi(\vec{r})|^2 \simeq \frac{4A^2}{D^2}\cos^2\left(\frac{\pi d}{\lambda}\frac{\rho}{D}\right), \qquad D >> d \tag{1.4}$$

where D is the distance between E_2 and E_3, d is the separation of the two slits ($d = |\vec{r_1} - \vec{r_2}|$), and ρ is the radial coordinate measured from the center O of the screen. The interference fringes are circular. Figure **1.2** shows a radial cross-section of the intensity as a function of ρ.

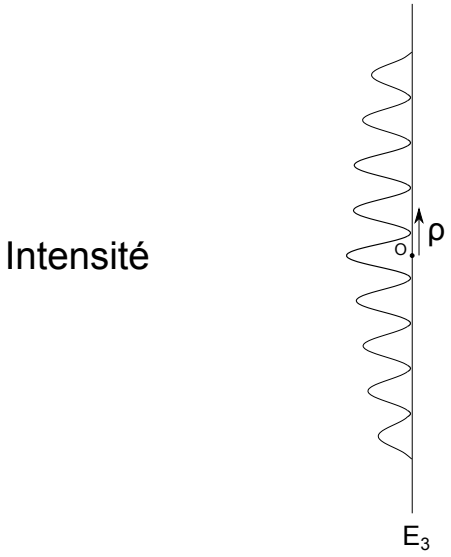


Figure 1.2 Intensity on E_3 for the interference pattern.

The intensity maxima lie on concentric circles of radii $\rho_n = n\lambda\frac{D}{d}$. The separation between successive maxima is $\rho_{n+1} - \rho_n = \lambda\frac{D}{d}$. Measuring this distance therefore gives access to λ. For visible light, λ is of order 400–600 nm (1 nm = 10^{-9} m).

What would happen if the incident beam consisted instead of classical projectiles, or "grains of light"? A naive classical picture predicts that the beam broadens as particles scatter from the edges of the slits. One would expect more particles near the center of each diffracted beam and fewer near the edges (Figure **1.3**). The intensity recorded on E_3 would show no interference fringes. The same qualitative result is obtained with tennis balls or ping-pong balls, whether they are sent through the slits one at a time or simultaneously (Figure **1.3**).

The intensity recorded on E_3, i.e. the number of particles as a function of position, has the form $N_1(\vec{r}) + N_2(\vec{r})$ (Figure **1.4**).

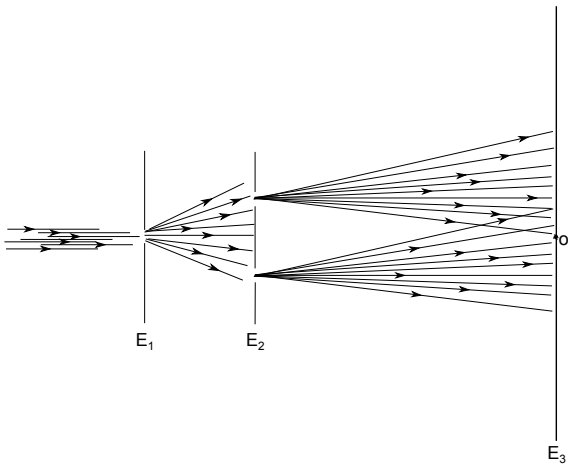


Figure 1.3 Double-slit experiment with classical projectiles.

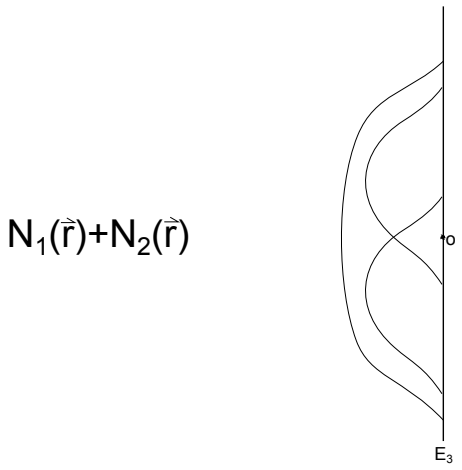


Figure 1.4 Intensity on E_3 for classical projectiles.

Nature, however, behaves in a much more surprising way. We now turn to modern versions of Young's experiment performed with electrons and even large molecules.

Modern Double-Slit Experiments – after 1960

In 1909, G. Taylor repeated Young's experiment using an extremely weak light source, corresponding roughly to a candle placed one kilometer from the screen. The interference pattern was still observed. At the time, the main conclusion was simply that the wave description of light remains valid at very low intensities. In hindsight, however, Taylor's experiment anticipated remarkable modern experiments with individual particles. As the photoelectric effect shows, a sufficiently weak light source can be viewed as a source of individual photons.

In 1961, C. Jönsson carried out a double-slit experiment with electrons. Interference fringes were observed, indicating wave-like behavior. An even more striking observation is obtained when the electrons are sent through the apparatus one at a time. Each electron produces a localized detection event at a seemingly random point on the screen E_3. After many electrons have been detected, the collection of individual impacts builds up an interference pattern. Thus an electron is detected as a localized particle, while the statistical distribution of detection events displays wave interference.

Similar experiments have been performed with neutrons and, in 1999, with carbon-60 molecules. A C60 molecule contains 60 carbon atoms arranged approximately on a sphere at the vertices of 12 pentagons and 20 hexagons, in a structure reminiscent of a football. Its diameter is about 0.7 nm, much larger than that of an elementary particle such as the electron, which is treated as point-like at present experimental resolution. More recent interference experiments have used artificial molecules containing several hundred to roughly a thousand atoms. Under suitable experimental conditions, interference fringes are again observed. The spacing of the fringes allows one to assign a wavelength λ to the molecules using the relation $\rho_{n+1} - \rho_n = \lambda \frac{D}{d}$ derived above. Remarkably, this wavelength can be hundreds of times smaller than the size of the molecule itself. Nevertheless, quantum mechanics predicts that a wave description remains meaningful.

These experiments provide striking evidence that material particles can exhibit wave-like behavior. Why, then, do we not observe interference fringes for tennis balls or footballs? Where is the boundary between electrons, C60 molecules, systems containing hundreds of atoms, and ordinary macroscopic objects? This is a deep question. There is no sharp, universally specified boundary between quantum wave–particle behavior and classical behavior. Modern interference experiments with increasingly large molecules are valuable precisely because they probe this quantum-to-classical transition.

Experiments show that if C60 molecules interact too strongly with their environment, for example by exchanging radiation with it, the interference fringes disappear. In other words, coherent wave behavior is preserved only when the molecules are sufficiently isolated. The loss of quantum coherence caused by interaction with the environment is called *decoherence*. Large molecules and macroscopic objects interact continually with their surroundings and therefore behave classically to an excellent approximation.

As we shall see near the end of this course, building a quantum computer is in some respects analogous to performing Young's experiment with macroscopic objects that are isolated so well that interference remains observable. The standard view is that quantum

mechanics applies to matter at all scales, provided the system is sufficiently isolated that decoherence does not destroy the relevant superpositions.

1.2 The Photoelectric Effect

The photoelectric effect concerns the interaction of light with matter. Above sufficiently high frequencies, typically in the ultraviolet but depending on the material also in the visible or infrared, the interaction reveals its discrete character. Several phenomena demonstrate this quantization, including Compton scattering and pair creation, but historically the photoelectric effect was the first to be understood in these terms.

In 1885, Hertz studied electrical sparks produced in an apparatus driven by radio waves. He noticed that the spark length changed when the apparatus was placed in darkness rather than daylight. The observation was not understood at the time. We now know that ultraviolet radiation present in daylight can eject electrons from nearby atoms and thereby influence the discharge. The effect was studied clearly by Lénard in 1902 using ultraviolet illumination. Above a material-dependent threshold frequency, electrons are ejected and an electric current can be measured. Lénard also showed that the kinetic energy of the emitted electrons increases with the frequency of the incident radiation. By contrast, this kinetic energy is essentially independent of the radiation intensity; the intensity controls mainly the number of emitted electrons per unit time, and hence the current.

Einstein interpreted these observations in one of his celebrated 1905 papers. He postulated that electromagnetic radiation consists of particles, now called photons, and associated with each photon an energy and momentum

$$E = h\nu \qquad \text{and} \qquad p = \frac{h}{\lambda}, \tag{1.5}$$

where λ and ν are the wavelength and frequency of the radiation. Here $h \simeq 6.63 \times 10^{-24}$ J·s is Planck's constant. Planck had already introduced a related quantization idea, together with the constant h, in his work on black-body radiation: energy exchange between matter and radiation occurs in multiples of $h\nu$. Planck, however, did not regard electromagnetic radiation itself as being made of particles. Einstein was the first to formulate explicitly this wave–particle duality for electromagnetic radiation.

According to Einstein, the kinetic energy of an electron ejected from a metal is (Figure **1.5**)

$$\frac{1}{2}mv^2 = \begin{cases} h\nu - W_0 & h\nu > W_0, \\ 0 & h\nu < W_0. \end{cases} \tag{1.6}$$

Here W_0 is the minimum energy required to remove an electron from the material. Setting $h\nu = W_0$ gives the threshold frequency $\nu_0 = \frac{W_0}{h}$ below which the photoelectric effect does not occur. The formula relies on three ingredients: (i) conservation of energy, (ii) the photon relation $h\nu$, and (iii) the assumption that W_0 is independent of frequency and

intensity in the regime considered. Energy conservation is a universal physical principle. Assumption (iii) is a material property valid in an appropriate regime rather than a fundamental law. By contrast, the photon-energy relation $h\nu$ is a fundamental law of quantum physics.

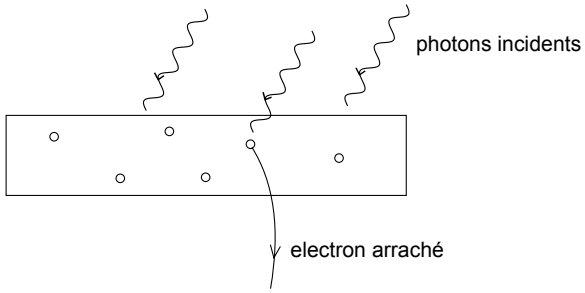


Figure 1.5 Photoelectric emission caused by incident photons.

Although simple, Einstein's formula was revolutionary in 1905. It states that radiation is composed of elementary quanta, photons, whose energy depends linearly on frequency rather than on light intensity. Classical Maxwell theory, by contrast, associates the energy carried by a wave with its intensity. The two descriptions are reconciled by recognizing that a classical electromagnetic wave corresponds to a large number of photons, each carrying energy $Nh\nu$; the photon number N is related to the wave intensity.

The linear dependence on frequency proposed by Einstein, building on Planck's work, was not obvious from Lénard's early data. Only later did carefully controlled experiments verify the relation accurately. Millikan's measurements, completed in the following decades, provided a precise linear test.

Millikan also used the slope of the straight line in Figure **1.6** to determine Planck's constant experimentally. Its numerical value is $h = 6.63 \times 10^{-24}$ J·s. Recall that 1 J = 6.2×10^{18} eV and that $13,6$ eV is the ionization energy of the hydrogen atom.

Young's experiment and the photoelectric effect reveal complementary aspects of light. Taken together, they establish its dual wave–particle behavior. This conclusion was so radical in the early twentieth century that Einstein's interpretation took considerable time to gain broad acceptance.

It is worth returning briefly to Taylor's 1909 experiment. The source intensity was so low that an exposure of several months was required before the interference fringes

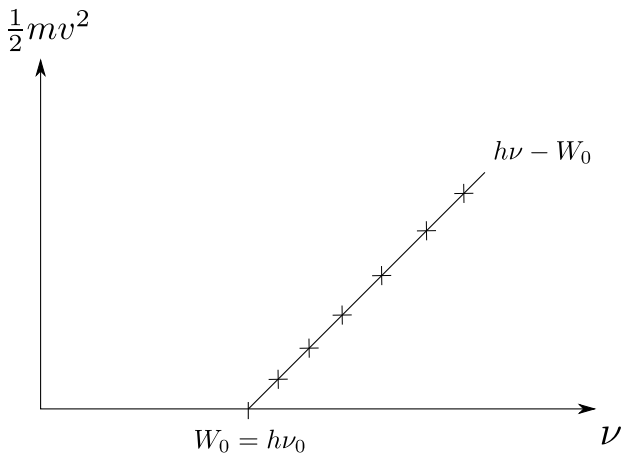


Figure 1.6 Linear dependence observed in the photoelectric effect.

became visible. In modern language, photons arrived only sparsely at the slits and detector. Today, sources that emit approximately one photon at a time can be controlled directly.

1.3 The "Wave Function": A Conceptual Revolution

The photoelectric effect and Young's experiment show that light exhibits both wave-like and particle-like behavior. In 1924 de Broglie conjectured that the same duality should apply to electrons and, more generally, to all matter. Modern interference experiments provide spectacular confirmation of this idea.

De Broglie associated a wavelength λ and a frequency ν with a particle through the relations

$$\lambda = \frac{h}{p}, \qquad \text{and} \qquad \nu = \frac{E}{h}. \tag{1.7}$$

These are essentially the same relations as for a photon. For a nonrelativistic particle of mass m, however, $p = mv$ and $E = \frac{1}{2}mv^2 = \frac{p^2}{2m}$, where v is the particle velocity.

More generally, one associates with the particle a wave amplitude $\psi(\vec{r}, t)$. We first consider two simple examples and then discuss the interpretation of this *wave function*.

For a free particle moving in the z direction, it is natural by analogy with electromagnetic waves to associate a plane wave,

$$\psi(\vec{r},t) = Ae^{2\pi i(\frac{z}{\lambda}-\nu t)} = Ae^{\frac{i}{\hbar}(pz-Et)} \tag{1.8}$$

where $\hbar = \dfrac{h}{2\pi}$.

For a particle passing through a double-slit apparatus, the wave emerging from each slit is approximately spherical,

$$\psi_{1,2}(\vec{r},t) = A\frac{e^{\frac{i}{\hbar}(p|\vec{r}-\vec{r_{1,2}}|-Et)}}{|\vec{r}-\vec{r_{1,2}}|} \tag{1.9}$$

and the total wave function or amplitude is obtained by superposition,

$$\psi(\vec{r},t) = \psi_1(\vec{r},t) + \psi_2(\vec{r},t) \tag{1.10}$$

The crucial difference from classical wave theory is that this wave function describes a *single particle*.

How should $\psi(\vec{r},t)$ be interpreted? Shortly after the introduction of the wave function, Max Born proposed that

$$|\psi(\vec{r},t)|^2 \tag{1.11}$$

represents the *probability density* for finding the particle at position $\vec{r}$ at time t. Equivalently,

$$\int_V \mathrm{d}^3\vec{r}\,|\psi(\vec{r},t)|^2 \tag{1.12}$$

is the probability of finding the particle in a region $V \subset \mathbb{R}^3$. For this probabilistic interpretation to be consistent, the wave function must satisfy the normalization condition

$$\int \mathrm{d}^3\vec{r}\,|\psi(\vec{r},t)|^2 = 1 \tag{1.13}$$

which can in general be enforced by choosing the normalization constant A appropriately.

This interpretation is fully consistent with double-slit experiments. When particles are sent through the apparatus one at a time, each produces a localized and apparently random detection event on the screen. After many events, however, the observed distribution forms interference fringes with intensity proportional to $|\psi(\vec{r},t)|^2$. Thus the probability distribution of individual detection events is given by Born's rule, $|\psi(\vec{r},t)|^2$.

1.4 A First Notion of a "Quantum State"

A quantum state may be viewed as an abstraction and generalization of the wave-function concept. A wave function describes continuous degrees of freedom, such as position. In Chapter **2** we shall introduce quantum states associated with discrete degrees of freedom. These are especially important in quantum information, where the elementary two-level system is the quantum bit, or qubit.

The wave-function concept and Born's probabilistic interpretation represented a radical departure from classical mechanics. In general, one gives up the notion of a definite particle trajectory. Position and momentum may each be sharply defined in appropriate states, but they cannot in general both be specified with arbitrary precision. For example, when a localized detection event is observed on a screen, the particle position is recorded, but a simultaneously well-defined propagation direction need not exist.

In quantum mechanics, the state of a particle is described by a wave function. More abstractly, this wave function can be regarded as a vector in a vector space of functions. The state vector is written

$$|\psi\rangle \quad \longleftrightarrow \quad \psi(\vec{r}). \tag{1.14}$$

This is Dirac's standard notation. One could use a conventional vector symbol instead, but $|\psi\rangle$ reminds us that state vectors do not live in ordinary three-dimensional physical space. The symbol $|\psi\rangle$ is called a *ket*. Its Hermitian conjugate, obtained by transposition and complex conjugation, is called a *bra* and is denoted

$$\langle\psi| \quad \longleftrightarrow \quad \psi^*(\vec{r}). \tag{1.15}$$

The inner product of a vector with itself gives its squared norm. In the present case,

$$\langle\psi|\psi\rangle = \int \mathrm{d}^3\vec{r}\; \psi^*(\vec{r})\,\psi(\vec{r}) = \int \mathrm{d}^3\vec{r}\; |\psi(\vec{r})|^2. \tag{1.16}$$

Born's interpretation requires $\int \mathrm{d}^3\vec{r}\; |\psi(\vec{r})|^2 = 1$, corresponding to total probability one. A physical state vector must therefore satisfy the normalization condition

$$\langle\psi|\psi\rangle = 1.$$

These observations suggest that, more generally, the inner product between two state vectors $|\psi\rangle$ and $|\phi\rangle$ will play a central role in quantum mechanics. For states represented by wave functions, the natural inner product is

$$\langle\phi|\psi\rangle = \int \mathrm{d}^3\vec{r}\; \phi^*(\vec{r})\,\psi(\vec{r}). \tag{1.17}$$

This inner product satisfies the usual properties of linearity, conjugate symmetry, and positivity.

If a particle is observed to be localized at $\vec{r_1}$, its state is denoted $|\vec{r_1}\rangle$. Formally, one may associate this state with a Dirac delta distribution,

$$|\vec{r_1}\rangle \quad \longleftrightarrow \quad \delta(\vec{r} - \vec{r_1}) \tag{1.18}$$

Using the inner product introduced above gives

$$\langle \vec{r}_1|\psi\rangle = \int \mathrm{d}^3\vec{r}\;\delta(\vec{r}-\vec{r}_1)\,\psi(\vec{r}) = \psi(\vec{r}_1). \tag{1.19}$$

which leads to the connection between bra–ket notation and the wave-function representation,

$$\langle \vec{r}|\psi\rangle = \psi(\vec{r}). \tag{1.20}$$

The derivation above is deliberately informal; more precisely, the last relation can be taken as the definition of the bra $\langle\vec{r}|$. Similarly, the ket $|\vec{r}\rangle$ is defined through

$$\langle \psi|\vec{r}\rangle = \psi^*(\vec{r}). \tag{1.21}$$

We can now state a more general version of Born's rule. Recall that the probability density for finding a particle at $\vec{r}$ when its state is $|\psi\rangle$ is

$$|\psi(\vec{r})|^2 = |\langle\vec{r}|\psi\rangle|^2 \tag{1.22}$$

The quantum-mechanical measurement postulate generalizes this statement. A precise formulation will be given in Chapter **3**. For the moment, we use the following form:

"If the state immediately before a measurement is $|\psi\rangle$, the probability of obtaining the final state $|\phi\rangle$ is $|\langle\phi|\psi\rangle|^2$."

The appropriate mathematical framework for quantum mechanics is the theory of Hilbert spaces. In particular, we shall see that

(i). Quantum states are vectors. Adding state vectors corresponds to the superposition principle.
(ii). Inner products determine the probabilities associated with measurement outcomes.

These statements will be made precise in Chapter **3**.

1.5 Heisenberg's Uncertainty Principle

A fundamental feature of quantum mechanics is that position and momentum cannot both be determined with arbitrarily small uncertainty. The uncertainty principle provides a quantitative expression of this fact.

For a particle in the state $|\psi\rangle$, we have seen that the probability density for finding the particle at x is $|\psi(x)|^2$; here we restrict ourselves to one spatial dimension $x \in \mathbb{R}$. The standard deviation obtained from repeated position measurements is

$$\sigma_x = \left\{ \int x^2 |\psi(x)|^2\,\mathrm{d}x - \left(\int x\,|\psi(x)|^2\,\mathrm{d}x \right)^2 \right\}^{\frac{1}{2}} \tag{1.23}$$

Physicists usually denote this uncertainty by δx rather than σ_x.

Now suppose that the particle momentum p is measured. What state $|p\rangle$ corresponds to a definite momentum p? The associated wave function is the plane wave $e^{\frac{i}{\hbar}px}$. Its

probability density is constant, $|e^{\frac{i}{\hbar}px}|^2 = 1$, so a state of perfectly definite momentum is completely delocalized in position. Since by definition $\langle \vec{r}|\psi\rangle = \psi(\vec{r})$, we have

$$\langle x|p\rangle = e^{\frac{i}{\hbar}px}. \tag{1.24}$$

If the initial state is $|\psi\rangle$, the probability density for measuring momentum p is, by the generalized Born rule,

$$|\langle p|\psi\rangle|^2 = \int \mathrm{d}x\, e^{-\frac{i}{\hbar}px}\psi(x) = |\hat{\psi}(p)|^2 \tag{1.25}$$

where $\hat{\psi}$ is essentially the Fourier transform of ψ. Thus $|\hat{\psi}(p)|^2$ is the momentum probability density. Its uncertainty can be defined by

$$\sigma_p = \left\{ \int p^2 |\hat{\psi}(p)|^2 \,\mathrm{d}p - \left(\int p\, |\hat{\psi}(p)|^2 \,\mathrm{d}p \right)^2 \right\}^{\frac{1}{2}} \tag{1.26}$$

Again, physicists usually write δp rather than σ_p.

For a square-integrable wave function, i.e. with finite $\int \mathrm{d}x\, |\psi(x)|^2$[2], a standard theorem of Fourier analysis implies

$$\sigma_x \sigma_p \geq \frac{\hbar}{2}. \tag{1.27}$$

This inequality, often written $\delta x\, \delta p \geqslant \frac{\hbar}{2}$, is Heisenberg's uncertainty relation. Physically, it states that the uncertainties in position x and momentum p cannot both be made arbitrarily small for the same quantum state. Improving the precision in x necessarily increases the minimum possible uncertainty in p, and vice versa. This is not a technological limitation of a particular measuring instrument; it is an intrinsic property of quantum states.

1.6 The Spectral-Line Problem

When visible light is passed through a prism, a continuous spectrum of colors is observed. More generally, electromagnetic waves form a continuous range of frequencies.

In 1885, Balmer showed that hydrogen, and atoms more generally, possess discrete emission spectra. For hydrogen he identified four lines in the visible range, at wavelengths $\lambda = 656.3$ nm, 481.1 nm, 434.1 nm, and 410 nm. They satisfy the empirical relation

$$\frac{1}{\lambda} = R_H \left(\frac{1}{4} - \frac{1}{m^2}\right), \qquad m = 3, 4, 5, 6 \tag{1.28}$$

[2] Parseval's theorem states that $\int \mathrm{d}x\, |\psi(x)|^2 = \int \mathrm{d}p\, |\hat{\psi}(p)|^2$

with $R_h = 10973731,57\ \mathrm{m}^{-1}$.

The challenge was to explain why only discrete wavelengths, indexed by the integer m, appear. The Balmer formula is in fact a special case of a more general formula proposed by Bohr, which predicted additional spectral series that were observed experimentally, in some cases only years later.

Rutherford's famous scattering experiments with α particles on gold foil established that atoms consist of a small positively charged nucleus, of charge Ze, surrounded by Z electrons of charge e. Classical physics, however, could not explain the stability of such a planetary model: an accelerating electric charge should radiate energy and eventually spiral into the nucleus.

The emerging quantum ideas did not initially provide a complete explanation of atomic stability, but they did account for the Balmer formula and its generalizations. Bohr postulated that (i) the electron may occupy only certain allowed orbits and (ii) classical mechanics applies along those allowed orbits. He then imposed a quantization rule selecting the permitted trajectories. This rule is discussed in the exercises. Here we follow de Broglie's later wave-based interpretation.

For an allowed circular orbit,

$$m\,\frac{v^2}{R} = k\,\frac{Ze^2}{R^2} \tag{1.29}$$

and

$$E = \frac{1}{2}mv^2 - k\,\frac{Ze^2}{R} \tag{1.30}$$

where v is the speed, m the electron mass, k Coulomb's constant, E the mechanical energy, and R the orbital radius. These relations imply that the energy of a circular orbit of radius R is

$$E = -\frac{k}{2}\frac{Ze^2}{R}. \tag{1.31}$$

It remains to determine which radii are allowed. In de Broglie's picture, the wave associated with the electron must form a standing wave along the orbit. For a circular orbit this requires

$$n\lambda = 2\pi R, \qquad n \geq 1 \tag{1.32}$$

where λ is the wavelength and n is an integer[3]. For λ, de Broglie's relation gives

[3] The situation is analogous to a violin string of length $2\pi R$: $n = 1$ gives the fundamental mode and $n = 2, 3, 4, \ldots$ the harmonics.

$$\lambda = \frac{h}{p} = \frac{h}{mv} \tag{1.33}$$

Using $v = \left(\frac{k}{m}\frac{Ze^2}{R}\right)^2$ gives $\lambda = \frac{hR^{\frac{1}{2}}}{(kmZe^2)^{\frac{1}{2}}}$ and hence the allowed radii

$$R = \frac{\hbar^2}{kmZe^2}\, n^2, \qquad n \geq 1 \tag{1.34}$$

which lead to

$$E_n = -\frac{k^2 Z^2 e^4 m}{2\hbar^2}\frac{1}{n^2} = -\mathrm{R_y}\,\frac{Z^2}{n^2}; \qquad n \geq 1. \tag{1.35}$$

Here $\mathrm{R_y} = \dfrac{k^2 e^4 m}{2\hbar^2} \simeq 13.6$ eV is the Rydberg energy. For hydrogen, $Z = 1$.

The discrete values E_n are called the atomic energy levels and form the spectrum of the hydrogen atom. Although the underlying notion of a classical electron orbit is not correct, the resulting energy formula is remarkably exact for hydrogen. Schrödinger later derived it within the full wave-mechanical theory, as briefly discussed in Section **1.7**.

Returning to spectral lines, Bohr further postulated that an electron can make a transition from an orbit labeled m to one labeled n by emitting a photon of energy $E_m - E_n$. The photon frequency is then determined by Einstein's relation

$$h\nu_{m\to n} = E_m - E_n \tag{1.36}$$

Since $E_n = -\frac{\mathrm{Ry}}{n^2}$, with $Z = 1$ for hydrogen, one obtains

$$h\nu_{m\to n} = -\left(\frac{\mathrm{Ry}}{m^2} - \frac{\mathrm{Ry}}{n^2}\right) \tag{1.37}$$

Using $\lambda\nu = c$ for the photon gives

$$\frac{1}{\lambda_{m\to n}} = \frac{\mathrm{Ry}}{hc}\left(\frac{1}{n^2} - \frac{1}{m^2}\right) \tag{1.38}$$

with $\dfrac{\mathrm{Ry}}{hc} = R_H$, the Rydberg constant. The Balmer lines correspond to transitions $m \to 2$ with $n = 2$. The transitions $m \to 1$ form the Lyman series in the ultraviolet, while the $m \to 3$ series is the Paschen series in the infrared. There are infinitely many such lines, but the crucial point is that the spectrum is discrete.

1.7 The Schrödinger Equation

The semiclassical treatment used in Section **1.6** is conceptually unsatisfactory because it still relies on classical particle trajectories.

In 1926, Schrödinger derived the equation that governs the dynamics of the wave function $\psi(\vec{r}, t)$. Solving this equation yields stationary states and their energy levels. The formula $E_n = -Ry\dfrac{Z^2}{n^2}$ remains valid, but the full quantum theory reveals additional structure: for a given quantum number n, several independent solutions, and hence several distinct wave functions or states, may correspond to the same energy. The energy level is then said to be degenerate. These different states correspond to different probability distributions for the electron around the nucleus. This richer structure is essential for understanding the periodic table and is one reason Schrödinger's equation lies at the foundation of quantum chemistry.

We give here a heuristic derivation of Schrödinger's equation. For a particle of momentum p and energy E, consider the plane-wave state

$$\psi(z, t) = A \exp\{\frac{i}{\hbar}(pz - Et)\}. \tag{1.39}$$

For a free particle, $E = \dfrac{p^2}{2m}$. If the particle is subject to a potential $V(z)$, classical mechanics gives $E = \dfrac{p^2}{2m} + V(z)$. It is tempting to substitute this expression for E directly into the phase of the plane wave. This is not generally justified, although it can be a useful approximation when $V(z)$ varies slowly on length scales larger than $\lambda = \dfrac{h}{p}$:

$$\psi(z, t) \simeq A \exp\{\frac{i}{\hbar}(pz - \frac{p^2}{2m} + V(z))\}. \tag{1.40}$$

One readily verifies that this function satisfies

$$i\hbar\frac{\partial\psi(z, t)}{\partial t} = -\frac{\hbar^2}{2m}\frac{d^2}{dz^2}\psi(z, t) + V(z)\psi(z, t) \tag{1.41}$$

The resulting equation is in fact exact for a nonrelativistic particle. It is the time-dependent Schrödinger equation. In three dimensions it becomes

$$i\hbar\frac{\partial\psi(\vec{r}, t)}{\partial t} = -\frac{\hbar^2}{2m}\Delta\psi(\vec{r}, t) + V(\vec{r})\psi(\vec{r}, t) \tag{1.42}$$

where $\Delta = \dfrac{\partial^2}{\partial x^2} + \dfrac{\partial^2}{\partial y^2} + \dfrac{\partial^2}{\partial z^2}$ is the Laplacian operator. For an electron bound to a nucleus of charge Ze, one uses the Coulomb potential $V(\vec{r}) = -k\dfrac{Ze^2}{r}$.

To determine the energy levels, one looks for stationary solutions of the form

$$\psi(\vec{r},t) = \phi(\vec{r})\exp\{-\frac{i}{\hbar}Et\} \tag{1.43}$$

The nodes of $\psi(\vec{r},t)$ are those of $\phi(\vec{r})$ and therefore do not move in time. Moreover, the probability density $|\psi(\vec{r},t)|^2 = |\phi(\vec{r})|^2$ is time-independent.

For a bound atomic electron, one seeks solutions for which $\phi(\vec{r}) \to 0$ as $|\vec{r}| \to +\infty$. The quantity $|\phi(\vec{r})|^2$ is often visualized as an electron probability cloud around the nucleus.

Substituting the stationary-state ansatz into Schrödinger's equation gives

$$\left(-\frac{\hbar^2}{2m}\Delta + V(\vec{r})\right)\phi(\vec{r}) = E\,\phi(\vec{r}). \tag{1.44}$$

This is an eigenvalue equation for the linear operator

$$H = -\frac{\hbar^2}{2m}\Delta + V(\vec{r}). \tag{1.45}$$

The stationary wave function $\phi(\vec{r})$ is an eigenvector and E the corresponding eigenvalue. Because the underlying function space is infinite-dimensional, the operator may be viewed formally as an infinite matrix. This operator is the quantum Hamiltonian, and its eigenvalues are the allowed energy levels. For hydrogen, $V(\vec{r}) = -k\frac{e^2}{r}$, Schrödinger's calculation gives $E_n = -\frac{R_y}{n^2}$.. The agreement with Bohr's formula is remarkable but special to the hydrogenic problem; for more general systems one must work with Schrödinger's equation itself.

1.8 The Correspondence Principle

Consider again a particle moving in a force field described by a potential $V(\vec{r})$. Classically, the energy is $E = \frac{\vec{p}^2}{2m} + V(\vec{r})$. Schrödinger's equation tells us that the quantum energy levels are the eigenvalues of $H = -\frac{\hbar^2}{2m}\Delta + V(\vec{r})$. The quantum Hamiltonian is obtained by replacing the classical quantities $V(\vec{r})$ and $\frac{\vec{p}^2}{m}$ by the corresponding operators $V(\vec{r})$ and $-\frac{\hbar^2}{2m}\Delta$. This is one manifestation of the *correspondence principle*.

More generally, the correspondence principle provides rules for constructing quantum observables from classical ones. A classical observable $A(\vec{r},\vec{p})$, i.e. a function of position and momentum, is replaced by an operator $\hat{A}$. The basic correspondence is

$$\begin{cases} \vec{r} & \longrightarrow & \vec{r} = (x, y, z) \\ \vec{p} & \longrightarrow & i\hbar\vec{\nabla} = \left(i\hbar\frac{\partial}{\partial x}, i\hbar\frac{\partial}{\partial y}, i\hbar\frac{\partial}{\partial z}\right). \end{cases} \tag{1.46}$$

For example, $\dfrac{\vec{p}^2}{2m} = \dfrac{p_x^2}{2m} + \dfrac{p_y^2}{2m} + \dfrac{p_z^2}{2m}$ becomes $-\dfrac{\hbar^2}{2m}\dfrac{\partial^2}{\partial x^2} - \dfrac{\hbar^2}{2m}\dfrac{\partial^2}{\partial y^2} - \dfrac{\hbar^2}{2m}\dfrac{\partial^2}{\partial z^2} = -\dfrac{\hbar^2}{2m}\Delta$, and applying the rule above yields

$$\frac{p^2}{2m} + V(\vec{r}) \to -\frac{\hbar^2}{2m}\Delta + V(\vec{r}). \tag{1.47}$$

An important subtlety is that operator ordering matters. Classically, $xp_x - p_x x = 0$ because ordinary numbers commute. Quantum mechanically, however,

$$-x\left(i\hbar\frac{\partial}{\partial x}\right) + \left(i\hbar\frac{\partial}{\partial x}\right)x = i\hbar \tag{1.48}$$

Indeed,

$$-x\left(i\hbar\frac{\partial}{\partial x}\phi(x)\right) + i\hbar\frac{\partial}{\partial x}\left(x\phi(x)\right) = -xi\hbar\phi'(x) + i\hbar x\phi'(x) + i\hbar\phi(x) \tag{1.49}$$

$$= i\hbar\phi(x). \tag{1.50}$$

Thus the position and momentum operators x and $p_x \equiv -i\hbar\dfrac{\partial}{\partial x}$ do not commute. Their difference

$$xp_x - p_x x \equiv [x, p_x] \tag{1.51}$$

is called the commutator of x and p_x. The relation

$$[x, p_x] = i\hbar, \qquad \text{(and similarly for } y, p_y \text{ and } z, p_z) \tag{1.52}$$

is the canonical commutation relation and is closely connected with the uncertainty relation $\delta x \delta p \geq \frac{\hbar}{2}$.

The correspondence principle does not, by itself, uniquely determine the ordering of noncommuting operators when a classical observable $A(x, p)$ contains mixed products of x and p. The appropriate ordering must be fixed using additional physical information about the system.

2 Discrete Degrees of Freedom: Polarization and Spin

2.1 Polarization of Electromagnetic Waves

Maxwell's equations in vacuum admit plane-wave solutions. For a plane wave propagating in the direction z, the electric field $\vec{E}$ and magnetic field $\vec{B}$ are perpendicular to the direction of propagation,

$$\vec{E} = \mathrm{Re}\left\{\vec{E}_0\, e^{i(kz-\omega t)}\right\} \qquad \text{and} \qquad \vec{B} = \frac{1}{c}\hat{z}\times\vec{E} \tag{2.1}$$

with $k = \dfrac{2\pi}{\lambda}$, $\omega = 2\pi\nu$, and $\lambda\nu = c$ the speed of light. It is sufficient to specify $\vec{E}$, since $\vec{B}$ is then automatically perpendicular to $\vec{E}$ and to the propagation direction.

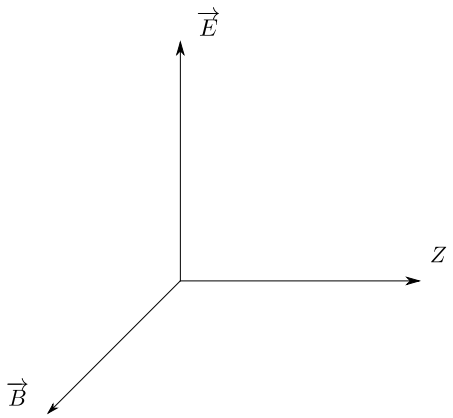


Figure 2.1 Directions of the electric and magnetic fields.

In general, $\vec{E}_0 = E_0\left((\cos\theta)e^{i\delta_x}; (\sin\theta)e^{i\delta_y}; 0\right)$. The orientation traced by $\vec{E}$ in the plane perpendicular to z defines the polarization of the wave. One may always set $\delta_x = 0$ and

retain δ_y as the relative phase; this simply amounts to choosing the origin of time. For fixed z, the electric-field vector $\vec{E} = (E_x, E_y, 0)$ traces an ellipse in the transverse plane $xy \perp z$ as time evolves. We shall focus on a few important special cases.

Example 2.1: Linear polarization

Let $\delta_x = 0$ and $\delta_y = 0$. For $z = 0$,

$$\vec{E} = \mathrm{Re}\left\{ E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} e^{-i\omega t} \right\} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \cdot \cos(\omega t) \tag{2.2}$$

Since $\dfrac{E_y}{E_x} = \tan\theta$, the electric field oscillates along a fixed axis at angle θ (equivalently $-\theta$). This is linear polarization along the direction θ (Figure **2.2**).

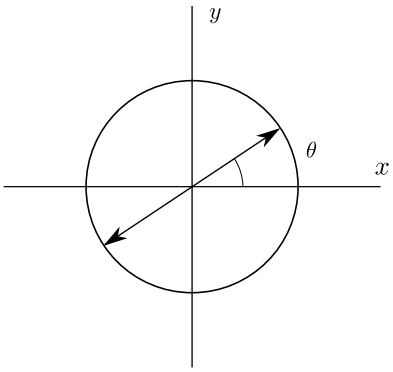


Figure 2.2 Linear polarization along the direction θ.

Example 2.2: Circular polarization

Consider $\theta = \frac{\pi}{4}$ and $\delta_x = 0$, with $\delta_y = \frac{\pi}{2}$ or $\delta_y = -\frac{\pi}{2}$. The electric field becomes

$$\vec{E} = \mathrm{Re}\left\{ E_0 \begin{pmatrix} \cos\frac{\pi}{4} \\ \sin\frac{\pi}{4} e^{\pm i\frac{\pi}{2}} \\ 0 \end{pmatrix} e^{-i\omega t} \right\} = E_0 \frac{1}{\sqrt{2}} \begin{pmatrix} \cos(\omega t) \\ \pm \sin(\omega t) \\ 0 \end{pmatrix} \tag{2.3}$$

Now $E_y^2 + E_x^2 = E_0^2$, so the electric-field vector rotates with constant magnitude, giving right- or left-circular polarization according to the sign of the phase (Figure 2.3).

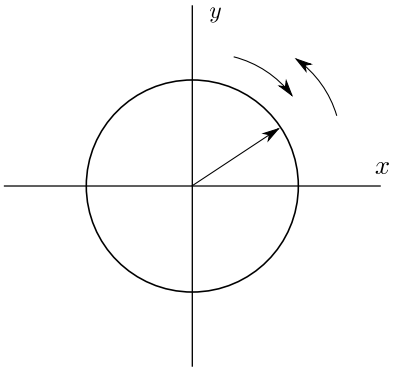


Figure 2.3 Circular polarization of the electric field.

The general case, with arbitrary θ, δ_y and with $\delta_x = 0$ chosen without loss of generality, is elliptic polarization: the electric field traces an ellipse in one of the two senses of rotation. Linear and circular polarization are limiting cases. Polarization can be selected experimentally with optical filters. A **linear polarizer**, for example, transmits only the component of the electric field along a chosen direction, say θ (Figure 2.4).

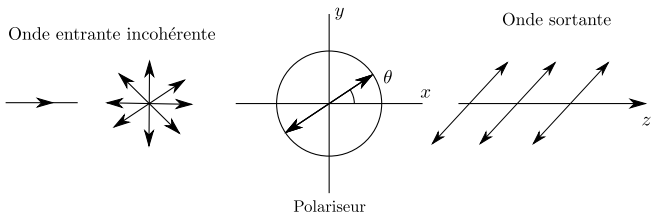


Figure 2.4 Linear polarizer.

The outgoing electric field is simply the projection of the incident field onto θ. Thus, at a fixed position such as $z = 0$, the transmitted field is

$$\vec{E} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \tag{2.4}$$

A second polarizing filter may be placed in series along a direction α. This second element is called an *analyzer* (Figure **2.5**) because it is used to analyze the polarization of the incoming wave.

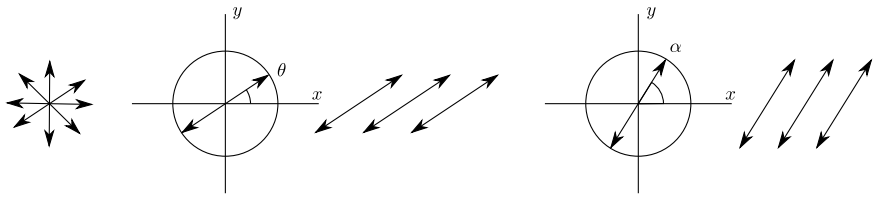


Figure 2.5 Polarization analyzer.

The field transmitted by the analyzer is polarized along α and is obtained by projecting the incident field onto that direction:

$$\vec{E} = E_0 \cos(\alpha - \theta) \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{pmatrix} \tag{2.5}$$

The corresponding amplitude is given by the scalar product

$$(\cos\alpha, \sin\alpha) \cdot \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \cos\alpha\cos\theta + \sin\alpha\sin\theta = \cos(\alpha - \theta) \tag{2.6}$$

The intensity before the analyzer (and after the first polarizer) is $\sim E_0^2$, while the intensity after the analyzer is $\sim E_0^2(\cos(\alpha-\theta))^2$. Therefore the ratio of transmitted to incident intensity is

$$\cos^2(\alpha-\theta) \tag{2.7}$$

This is **Malus's law**.

2.2 Photon Polarization

A photon possesses an internal degree of freedom closely related to the polarization of the electromagnetic field. This degree of freedom is called the *polarization of the photon*.

In Chapter **1** we introduced the wave-function concept. In particular, a free particle propagating in direction z may be associated with the plane wave $\psi(z,t) = A\,e^{i(kz-\omega t)}$.. For a photon, the corresponding wave function is vector-valued, just as the electric field is:

$$A\,e^{i(kz-\omega t)}\begin{pmatrix}\cos\theta\\(\sin\theta)e^{i\phi}\\0\end{pmatrix} \tag{2.8}$$

Here we have set $\delta_x = 0$ and $\delta_y = \phi$, as is customary for photons.

The choice $\phi = 0, \pi$ corresponds to linear polarization along θ or $\theta_\perp$. The choices $\theta = \dfrac{\pi}{4}$ together with $\phi = \dfrac{\pi}{2}$ or $-\dfrac{\pi}{2}$ correspond to right- and left-circular polarization, respectively.

In Dirac notation, a general free-photon state can be written

$$e^{-i\omega t}|k\rangle \otimes (\cos\theta|x\rangle + (\sin\theta)e^{i\phi}|y\rangle). \tag{2.9}$$

with the correspondence

$$|k\rangle \leftrightarrow e^{ikz}; \qquad |x\rangle \leftrightarrow \begin{pmatrix}1\\0\\0\end{pmatrix} \text{ and } \qquad |y\rangle \leftrightarrow \begin{pmatrix}0\\1\\0\end{pmatrix} \tag{2.10}$$

We use $|x\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|y\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ for the two transverse polarization basis states; the longitudinal z component is absent for a freely propagating electromagnetic wave.

In this chapter we focus exclusively on the photon's polarization degree of freedom,

$$|\theta,\phi\rangle = \cos\theta|x\rangle + (\sin\theta)e^{i\phi}|y\rangle = \begin{pmatrix}\cos\theta\\(\sin\theta)e^{i\phi}\end{pmatrix} \tag{2.11}$$

and suppress the orbital degree of freedom $|k\rangle$ as well as the explicit time dependence $e^{-i\omega t}$. The polarization vectors form the two-dimensional vector space $\mathbb{C}^2$ and satisfy $\langle\theta,\phi|\theta,\phi\rangle = 1$. To verify this, one uses

$$\langle\theta,\phi| = \cos\theta\langle x| + e^{-i\phi}\sin\theta\langle y| \tag{2.12}$$

and

$$\langle x|x\rangle = \langle y|y\rangle = 1, \qquad \langle x|y\rangle = \langle y|x\rangle = 0. \tag{2.13}$$

The same relation can also be checked directly in components:

$$\langle x| = (1,0) \qquad , \qquad \langle y| = (0,1) \tag{2.14}$$

and

$$\langle\theta,\phi| = (\cos\theta, e^{-i\phi}\sin\theta). \tag{2.15}$$

The linearly polarized states

$$\begin{cases} |\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle = \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix} \\ |\theta_\perp\rangle = \cos\theta_\perp|x\rangle + \sin\theta_\perp|y\rangle = \sin\theta|x\rangle - \cos\theta|y\rangle = \begin{pmatrix}\sin\theta\\ -\cos\theta\end{pmatrix} \end{cases} \tag{2.16}$$

form an orthonormal basis of $\mathbb{C}^2$. The two circularly polarized states

$$\begin{cases} |R\rangle = \frac{1}{\sqrt{2}}(|x\rangle + i|y\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix} \\ |L\rangle = \frac{1}{\sqrt{2}}(|x\rangle - i|y\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix} \end{cases} \tag{2.17}$$

form another orthonormal basis.

2.3 Experiments with Photon Polarization

We now consider a source that emits single photons prepared in the linearly polarized state $|\theta\rangle$. Experimentally, such a source can be approximated by a sufficiently weak light source followed by a polarizing filter oriented at angle θ.

Photodetection after an Analyzer

Single photons are sent through an analyzer oriented along α and are then recorded by a photodetector D (Figure **2.6**).

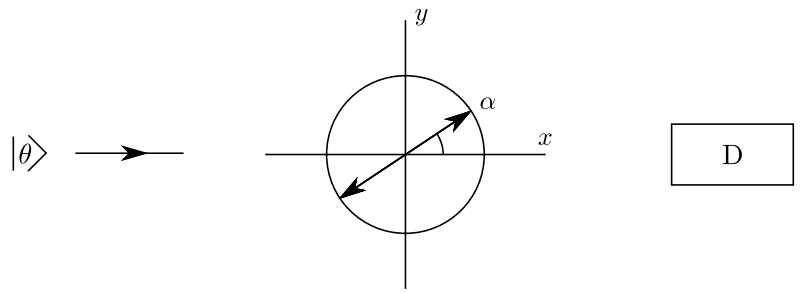


Figure 2.6 Analyzer followed by a photodetector.

Experimentally, the detector records either one photon or no photon: the photon is either transmitted by the analyzer α or absorbed and therefore never reaches D. Repeating the experiment produces a random binary sequence,

$$100101110010101 \tag{2.18}$$

and one cannot predict the outcome of an individual trial. What can be predicted is the statistical frequency of detections. The empirical probability of observing a photon at detector D is

$$\cos^2(\theta - \alpha). \tag{2.19}$$

These observations follow directly from Born's rule. Before the analyzer, the photon is in the state $|\theta\rangle$. The analyzer and detector together form a measurement apparatus. A click means that the photon has been projected onto the transmitted state $|\alpha\rangle$. Hence the transition probability is

$$\mathbb{P}\left[|\theta\rangle \to |\alpha\rangle\right] = |\langle\alpha|\theta\rangle|^2 \tag{2.20}$$

and Born's rule immediately gives

$$\begin{aligned}\langle\alpha|\theta\rangle &= (\cos\alpha\langle x| + \sin\alpha\langle y|)(\cos\theta|x\rangle + \sin\theta|y\rangle) \\ &= \cos\alpha\cdot\cos\theta + \sin\alpha\cdot\sin\theta \\ &= \cos(\alpha-\theta).\end{aligned} \tag{2.21}$$

Splitting with a Birefringent Plate

A birefringent element separates an incident beam into two components, one vertically polarized and one horizontally polarized (Figure **2.7**).

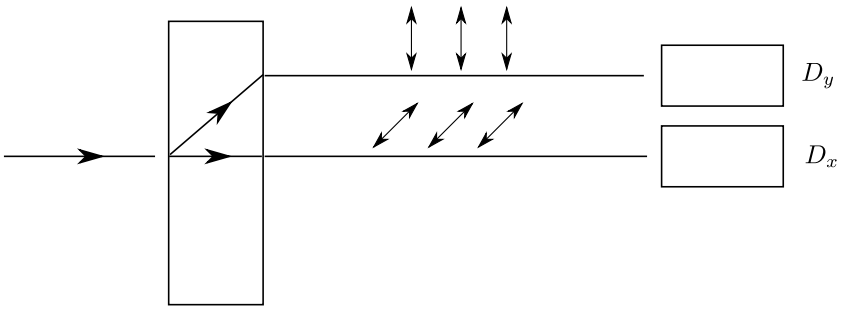


Figure 2.7 Birefringent plate.

For an electromagnetic wave with electric field

$$\vec{E} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \mathrm{Re}\left\{e^{i(kz-\omega t)}\right\} \tag{2.22}$$

the birefringent plate produces two outgoing waves,

$$E_y = E_0 \begin{pmatrix} 0 \\ \sin\theta \\ 0 \end{pmatrix} \mathrm{Re}\left\{e^{i(kz-\omega t)}\right\} \tag{2.23}$$

and

$$E_x = E_0 \begin{pmatrix} \cos\theta \\ 0 \\ 0 \end{pmatrix} \mathrm{Re}\left\{e^{i(kz-\omega t)}\right\} \tag{2.24}$$

The intensities measured at the two detectors, normalized by the incident intensity, are $D_y \sim \sin^2\theta$ and $D_x \sim \cos^2\theta$. Their sum equals the total incident intensity.

What happens for single photons? Exactly one of D_x or D_y registers a photon; the two events are mutually exclusive. If the detection sequence at D_x is

$$1010011010101, \tag{2.25}$$

then the sequence at D_y is its complement,

$$0101100101010. \tag{2.26}$$

The individual outcomes are random, but their statistics are predictable. The probability of a detection at D_x is $\cos^2\theta$, while the corresponding probability at D_y is $\sin^2\theta$.

The quantum interpretation is straightforward. Before the birefringent plate, the photon polarization is $|\theta\rangle$. After the plate, the orbital state contains two possible paths, while the polarization components associated with the two paths correspond to the decomposition of $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$. The probability of detecting the photon at D_x is the probability of observing polarization $|x\rangle$,

$$\mathbb{P}\left[|\theta\rangle \to |x\rangle\right] = |\langle x|\theta\rangle|^2 = \cos^2\theta \tag{2.27}$$

whereas the probability of detecting it at D_y is the probability of observing polarization $|y\rangle$,

$$\mathbb{P}\left[|\theta\rangle \to |y\rangle\right] = |\langle y|\theta\rangle|^2 = \sin^2\theta \tag{2.28}$$

Splitting and Recombination

Instead of detecting the photons immediately after the birefringent plate, one can recombine the two paths using a second, symmetric plate and then analyze the recombined beam with an analyzer oriented along α followed by a detector (Figure **2.8**).

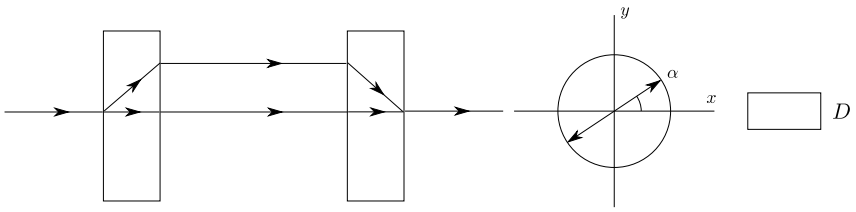


Figure 2.8 Splitting and recombination.

For a classical electromagnetic wave, the first plate separates the field into two components and the second plate recombines them. After the second plate, the electric field is the coherent superposition

$$E_x + E_y = \mathrm{Re}\left\{e^{i(kz-\omega t)}\right\} E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \tag{2.29}$$

After the analyzer, the detector therefore records an intensity $\cos^2(\theta - \alpha)$.

With single photons, the detector again produces a random sequence of clicks and no-clicks. Repeating the experiment yields an empirical click frequency $\cos^2(\theta - \alpha)$.

This result is immediate in the quantum description. After the second birefringent plate, the photon has returned to the state $|\theta\rangle$. Its probability of being detected by the apparatus $\alpha + D$ is therefore

$$\mathbb{P}\left[|\theta\rangle \to |\alpha\rangle\right] = |\langle\alpha|\theta\rangle|^2 = \cos^2(\alpha - \theta). \tag{2.30}$$

It is instructive to compare this with a purely classical particle picture in which each photon is assumed to follow a unique trajectory and to carry a definite polarization along that trajectory. That model gives the wrong prediction.

In such a classical picture, the particle follows the upper path with probability $\sin^2\theta$ and the lower path with probability $\cos^2\theta$. Along the upper path its polarization would be "y", giving a post-analyzer detection probability $\cos^2(\frac{\pi}{2} - \alpha) = \sin^2\alpha$; along the lower path it would be "x", giving probability $\cos^2(0 - \alpha) = \cos^2\alpha$. Thus

$$\begin{aligned}\mathbb{P}\left[\text{detection}\right] &= \mathbb{P}\left[\text{detection} \mid \text{upper path}\right] \cdot \mathbb{P}\left[\text{upper path}\right] \\ &\quad + \mathbb{P}\left[\text{detection} \mid \text{lower path}\right] \cdot \mathbb{P}\left[\text{lower path}\right] \\ &= \sin^2\theta \sin^2\alpha + \cos^2\theta \cos^2\alpha \\ &\neq \cos^2(\theta - \alpha).\end{aligned} \tag{2.31}$$

The difference between this classical prediction and the observed quantum result is $2\sin\theta\sin\alpha\cos\theta\cos\alpha$. Indeed,

$$\begin{aligned}\cos^2(\theta - \alpha) &= (\cos\theta\cos\alpha + \sin\theta\sin\alpha)^2 \\ &= \sin^2\theta\sin^2\alpha + \cos^2\theta\cos^2\alpha + 2\cos\theta\sin\theta\cos\alpha\sin\alpha.\end{aligned} \tag{2.32}$$

The situation is closely analogous to Young's double-slit experiment. The term missing from the classical calculation is an interference term between the two possible paths. Before detection, a photon cannot consistently be assigned both a unique path and one of the definite polarization states "x" or "y". Its state remains the coherent superposition $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$ until a measurement resolves the alternatives.

2.4 Observables Associated with Polarization

Consider again the photodetection experiment using an analyzer followed by a detector (Figure **2.9**).

If the incident photon is in state $|\theta\rangle$, the probability of a click is $\cos^2(\theta - \alpha) = |\langle\alpha|\theta\rangle|^2$ and the probability of no click is $\sin^2(\theta - \alpha) = |\langle\alpha_\perp|\theta\rangle|^2$. A click corresponds to the transition $|\theta\rangle \to |\alpha\rangle$, while no click corresponds to $|\theta\rangle \to |\alpha_\perp\rangle$. We may encode the two

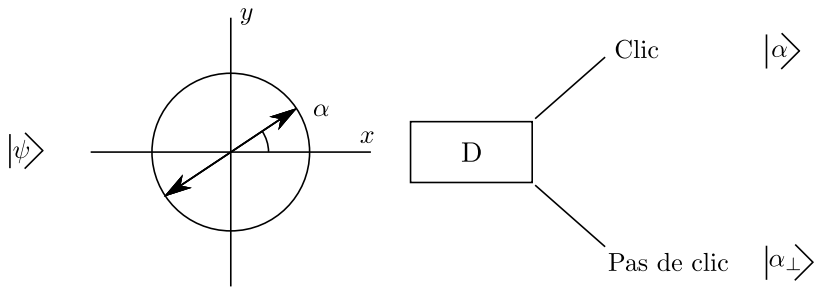


Figure 2.9 Photodetection experiment.

outcomes in a random variable taking the value $p_\alpha = +1$ for a click and $p_\alpha = -1$ for no click. Its expectation value is

$$\mathbb{E}\left[p_\alpha\right] = (+1)|\langle\alpha|\theta\rangle|^2 + (-1)|\langle\alpha_\perp|\theta\rangle|^2 \tag{2.33}$$

.

More generally, let the state entering the analyzer–detector system be $|\psi\rangle$, with $|\psi\rangle \in \mathbb{C}^2$ and unit norm. Then

$$\mathbb{E}\left[p_\alpha\right] = (+1)|\langle\alpha|\psi\rangle|^2 + (-1)|\langle\alpha_\perp|\psi\rangle|^2 \tag{2.34}$$

This can be rewritten as

$$\mathbb{E}\left[p_\alpha\right] = (+1)\,\langle\psi|\alpha\rangle\,\langle\alpha|\psi\rangle + (-1)\,\langle\psi|\alpha_\perp\rangle\,\langle\alpha_\perp|\psi\rangle \tag{2.35}$$

where we used $\overline{\langle\alpha|\psi\rangle} = \langle\psi|\alpha\rangle$, a standard property of the inner product. Equivalently,

$$\begin{aligned}\mathbb{E}\left[p_\alpha\right] &= \langle\psi|\,\left(|\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|\right)\,|\psi\rangle \\ &\equiv \langle\psi|P_\alpha|\psi\rangle\end{aligned} \tag{2.36}$$

where we have **defined** the polarization observable

$$P_\alpha = (+1)|\alpha\rangle\langle\alpha| + (-1)|\alpha_\perp\rangle\langle\alpha_\perp|. \tag{2.37}$$

Before discussing the physical meaning of P_α, let us examine its mathematical form. The object $|\alpha\rangle\langle\alpha|$ is a ket times a bra and is therefore the projector onto the vector $|\alpha\rangle$. Likewise, $|\alpha_\perp\rangle\langle\alpha_\perp|$ projects onto $|\alpha_\perp\rangle$. In matrix form these projectors give

$$|\alpha\rangle\langle\alpha| = \begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}\begin{pmatrix}\cos\alpha & \sin\alpha\end{pmatrix} = \begin{pmatrix}\cos^2\alpha & \cos\alpha\sin\alpha\\ \sin\alpha\cos\alpha & \sin^2\alpha\end{pmatrix} \tag{2.38}$$

$$|\alpha_\perp\rangle\langle\alpha_\perp| = \begin{pmatrix}-\sin\alpha\\ \cos\alpha\end{pmatrix}\begin{pmatrix}-\sin\alpha & \cos\alpha\end{pmatrix} = \begin{pmatrix}\sin^2\alpha & -\cos\alpha\sin\alpha\\ -\sin\alpha\cos\alpha & \cos^2\alpha\end{pmatrix} \tag{2.39}$$

and therefore

$$P_\alpha = \begin{pmatrix}\cos(2\alpha) & \sin(2\alpha)\\ \sin(2\alpha) & -\cos(2\alpha)\end{pmatrix} \tag{2.40}$$

The resulting matrix has eigenvalues ± 1 with eigenvectors $|\alpha\rangle = \begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}$ and $|\alpha_\perp\rangle = \begin{pmatrix}-\sin\alpha\\ \cos\alpha\end{pmatrix}$. Thus

$$P_\alpha|\alpha\rangle = (+1)|\alpha\rangle \tag{2.41}$$

$$P_\alpha|\alpha_\perp\rangle = (-1)|\alpha_\perp\rangle \tag{2.42}$$

It is useful to verify these relations directly in Dirac notation rather than by multiplying the matrix entries.

$$\begin{aligned} P_\alpha|\alpha\rangle &= \left(|\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|\right)|\alpha\rangle \\ &= |\alpha\rangle\underbrace{\langle\alpha|\alpha\rangle}_{1} - |\alpha_\perp\rangle\underbrace{\langle\alpha_\perp|\alpha\rangle}_{0} \\ &= |\alpha\rangle \end{aligned} \tag{2.43}$$

$$\begin{aligned} P_\alpha|\alpha_\perp\rangle &= \left(|\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|\right)|\alpha_\perp\rangle \\ &= |\alpha\rangle\underbrace{\langle\alpha|\alpha_\perp\rangle}_{0} - |\alpha_\perp\rangle\underbrace{\langle\alpha_\perp|\alpha_\perp\rangle}_{1} \\ &= -|\alpha_\perp\rangle \end{aligned} \tag{2.44}$$

What is the physical interpretation of the observable P_α? The matrix specifies the quantity being measured: here the photon's polarization in the pair of orthogonal directions $(\alpha, \alpha_\perp)$. The analyzer and detector implement that measurement. Its possible outcomes are the eigenvalues and associated eigenstates of the observable. In this case there are two outcomes, $(+1, |\alpha\rangle)$ and $(-1, |\alpha_\perp\rangle)$. Their probabilities are $|\langle\alpha|\psi\rangle|^2$ and $|\langle\alpha_\perp|\psi\rangle|^2$,

respectively, equivalently $\langle\psi|\alpha\rangle\langle\alpha|\psi\rangle$ and $\langle\psi|\alpha_\perp\rangle\langle\alpha_\perp|\psi\rangle$. The expectation value of the observable is $\langle\psi|P_\alpha|\psi\rangle$.

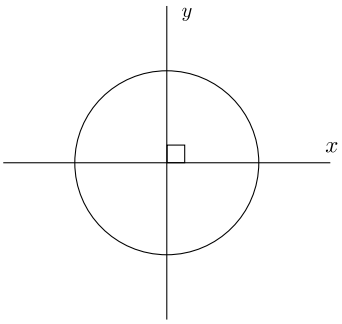
If the analyzer is rotated to an angle β rather than α, the measurement apparatus changes and so does the observable; it is then $P_\beta = |\beta\rangle\langle\beta| - |\beta_\perp\rangle\langle\beta_\perp|$.

Three observables will play a particularly important role throughout the course.

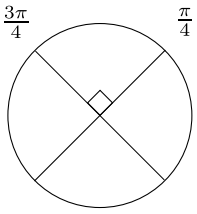
For $\alpha = 0$, the analyzer measures polarization in the directions x and y, and

$$P_{\alpha=0} = |x\rangle\langle x| - |y\rangle\langle y| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.45}$$

This analyzer, or measurement apparatus, is often represented by



For $\alpha = \dfrac{\pi}{4}$, the analyzer measures polarization along $\dfrac{\pi}{4}$ and $\dfrac{3\pi}{4}$ and is often represented by



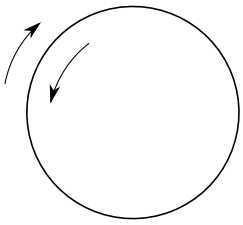
The corresponding observable is

$$P_{\alpha=\frac{\pi}{4}} = |\frac{\pi}{4}\rangle\langle\frac{\pi}{4}| - |\frac{3\pi}{4}\rangle\langle\frac{3\pi}{4}| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.46}$$

For an analyzer that measures circular polarization, the corresponding observable is

$$P_{\text{circ}} = |R\rangle\langle R| - |L\rangle\langle L| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{2.47}$$

and the analyzer is represented schematically by



It is instructive to verify this identity using

$$|R\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \qquad \langle R| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1, & -i \end{pmatrix} \tag{2.48}$$

$$|L\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} \qquad \langle L| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1, & i \end{pmatrix} \tag{2.49}$$

As we shall formalize in the postulates of quantum mechanics, every measurable quantity is represented by a Hermitian operator. The possible measurement outcomes are its eigenvalues, and the corresponding eigenvectors specify the associated post-measurement states. If λ_i is an eigenvalue with eigenvector $|v_i\rangle$, Born's rule gives

$$\mathbb{P}\left[\text{observer } \lambda_i \text{ and } |v_i\rangle\right] = |\langle v_i|\psi\rangle|^2 \tag{2.50}$$

when $|\psi\rangle$ is the state immediately before the measurement.

2.5 Classical Magnetic Moments

We now turn to another important internal degree of freedom, spin one-half. We first recall the classical notion of magnetic moment.

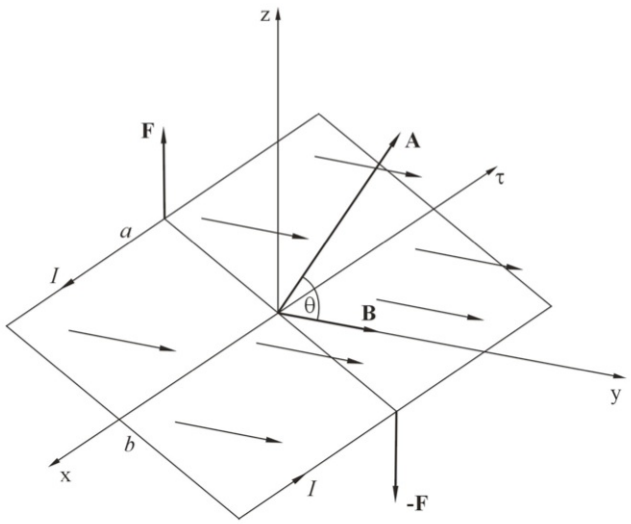


Figure 2.10 A rectangular current loop in a uniform magnetic field.

Consider a current loop placed in a uniform magnetic field (Figure **2.10**).

When a current flows through the loop, the Laplace forces on its different segments exert a torque that tends to align the loop with the magnetic field. Microscopically, the Laplace force originates from the Lorentz force. A particle of charge q and velocity $\vec{v}$ in a magnetic field $\vec{B}$ experiences the force $\vec{F} = q\vec{v}\times\vec{B}$. If a charge δq crosses a wire section during a time δt, the resulting force on a wire element of length $\delta\vec{l}$ is $\delta\vec{F} = \delta q\frac{\delta\vec{l}}{\delta t}\times\vec{B} = I\delta\vec{l}\times\vec{B}$, which is the Laplace-force expression. The work performed by these forces can be summarized by a magnetic potential energy

$$E = -\vec{M}\cdot\vec{B} \tag{2.51}$$

where $\vec{M}$ is the *magnetic moment* of the current loop, $\vec{M} = I\vec{S}$, and $\vec{S}$ is the unit normal to the loop. The energy is minimized when the magnetic moment is aligned with the field. A circulating charge q can likewise be assigned a magnetic moment

$$\vec{M} = \frac{q}{2}\vec{r}\times\vec{v} = \frac{q}{2m}\vec{L} \tag{2.52}$$

where $\vec{L} = \vec{r}\times\vec{p}$ is its orbital angular momentum. The energy is minimum when $\vec{L}$, equivalently $\vec{M}$, points along $\vec{B}$ and maximum when it points in the opposite direction.

Nature also contains *intrinsic* magnetic moments that are not generated by a classical orbital motion of charge. Electrons, protons, neutrons, and therefore atomic nuclei possess such intrinsic moments. One sometimes pictures these particles as tiny spinning tops, but this classical image is misleading and is not a useful foundation for the quantum formalism. The relations $E = -\vec{M}\cdot\vec{B}$ and $\vec{M} \sim \frac{q}{2m}\vec{L}$ retain analogous forms in quantum mechanics, but the components of $\vec{L}$ and $\vec{M}$ become operators. The corre-

sponding intrinsic angular-momentum operator $\vec{L}$ is called the *spin*; we use the notation $\vec{S}$ rather than $\vec{L}$.

2.6 The Stern–Gerlach Experiment

The celebrated Stern–Gerlach experiment revealed the quantization of the intrinsic magnetic moment associated with electron spin.

A beam of silver atoms emerging from an oven is sent through an inhomogeneous magnetic field with a gradient along the direction z (Figure **2.11**).

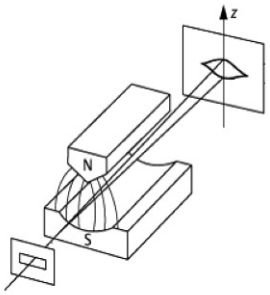


Figure 2.11 Stern–Gerlach experiment.

After passing through the magnet, the atomic beam splits into two components, producing two distinct spots on a detection screen.

This observation is surprising from a classical viewpoint. A silver atom is electrically neutral, so a simple Lorentz-force deflection of the whole atom is not expected. One may nevertheless suppose that the neutral atom carries a nonzero magnetic moment $\vec{M}$. In an inhomogeneous field, the force is then related to $\vec{\nabla}(\vec{M} \cdot B) = \vec{M} \cdot \vec{\nabla} B$, so a deflection is possible. Classically, however, atoms leaving the oven should have magnetic moments pointing in arbitrary directions. Since the component $\vec{M} \cdot \vec{\nabla} B = M_z (\vec{\nabla} B)_z$ would then vary continuously, one would expect a continuous spread of impacts on the screen. Instead, two narrow spots are observed along the z axis. *The experiment therefore shows that the measured component M_z takes only two possible values.*

This quantization of the magnetic moment has no classical explanation. The electrons in a silver atom, like all electrons, possess an intrinsic magnetic moment unrelated to their orbital motion. In silver, the electron configuration is such that the intrinsic moments of paired electrons cancel, leaving one unpaired outer electron. Its spin gives the atom an effective magnetic moment with two possible measured values.

We now describe the intrinsic magnetic moment and spin of a spin-one-half particle more explicitly.

2.7 Spin $\frac{1}{2}$ and Quantum Magnetic Moments

Elementary particles possess an intrinsic angular momentum called *spin*, together with an associated intrinsic magnetic moment. Spin is an angular-momentum degree of freedom, but it should not be interpreted as a tiny classical sphere literally rotating about its own axis. Quantum mechanics has already forced us to abandon such sharply defined classical trajectories and motions.

The spin operator is denoted $\vec{S}$. Like an ordinary angular momentum, it has three components (S_x, S_y, S_z). Its units are those of angular momentum, namely J·s, the same as $\hbar$. It is therefore convenient to write

$$\vec{S} = \frac{\hbar}{2}\vec{\sigma} \tag{2.53}$$

where the components $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are dimensionless. In quantum mechanics these components are matrices, since spin is an observable.

The magnetic moment associated with spin is

$$\vec{M} = \gamma\vec{S} \tag{2.54}$$

analogous to the orbital expression $\vec{M} = \frac{q}{2m}\vec{L}$ for a particle of charge q and mass m. The constant γ depends on the particle species; for an electron and a proton it takes the corresponding material-specific values indicated by $\gamma = g\frac{q}{2m}$ and $g \approx 5$.

The interaction energy between a magnetic moment and a magnetic field has the same formal structure as in classical physics,

$$-\vec{M}\cdot\vec{B} = -\gamma\frac{\hbar}{2}\vec{\sigma}\cdot\vec{B} \tag{2.55}$$

In quantum mechanics this is an operator, the Hamiltonian describing the spin in the magnetic field $\vec{B}$.

By blocking one of the two outgoing beams in a Stern–Gerlach apparatus, one obtains a **filter** analogous to an optical polarizer. It prepares one of the two spin states. Experiments analogous to the photon-polarization experiments can then be performed with spin-one-half particles.

For particles such as electrons, the spin components $\sigma_x, \sigma_y, \sigma_z$ are represented by 2×2 matrices closely related to the polarization observables:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.56}$$

A standard Stern–Gerlach apparatus measures the component z. The two possible results

are the eigenvalues of $M_z = \gamma\frac{\hbar}{2}\sigma_z$, namely ± 1 multiplied by $\gamma\frac{\hbar}{2}$. The corresponding eigenvectors are

$$\begin{pmatrix}1\\0\end{pmatrix} \equiv |\uparrow\rangle \qquad \text{and} \qquad \begin{pmatrix}0\\1\end{pmatrix} \equiv |\downarrow\rangle \tag{2.57}$$

and are precisely the two states obtained by measuring σ_z. In Dirac notation one may verify

$$\sigma_z = (+1)|\uparrow\rangle\langle\uparrow| + (-1)|\downarrow\rangle\langle\downarrow| \tag{2.58}$$

$$= \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} \tag{2.59}$$

If the apparatus is oriented along the x axis, it measures σ_x, or equivalently the magnetic-moment component $M_x = \gamma\frac{\hbar}{2}\sigma_x$. The eigenvalues are again ± 1 and the corresponding eigenstates are

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \equiv |+\rangle \tag{2.60}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle) \equiv |-\rangle \tag{2.61}$$

In Dirac notation,

$$\sigma_x = (+1)|+\rangle\langle+| + (-1)|-\rangle\langle-| \tag{2.62}$$

Similarly, for σ_y the eigenvalues are ± 1 with eigenstates

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle) \equiv |\circlearrowleft\rangle \tag{2.63}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle - i|\downarrow\rangle) \equiv |\circlearrowright\rangle \tag{2.64}$$

and

$$\sigma_y = (+1)|\circlearrowleft\rangle\langle\circlearrowleft| + (-1)|\circlearrowright\rangle\langle\circlearrowright| \tag{2.65}$$

2.8 The Hilbert Space of a Spin-$\frac{1}{2}$ Particle

The polarization degree of freedom of a photon is described by a two-dimensional Hilbert space. A normalized polarization state is a vector in $\mathbb{C}^2$, and in Dirac notation

a general state may be written $a|x\rangle + b|y\rangle$, with $|a|^2 + |b|^2 = 1$. Choosing $|x\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|y\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, a natural parameterization, directly analogous to the classical polarization of the electric field, is $a = \cos\theta$ and $b = e^{i\phi}\sin\theta$. Thus a general photon-polarization state can be written

$$|\theta, \phi\rangle = \cos\theta|x\rangle + e^{i\phi}\sin\theta|y\rangle \tag{2.66}$$

with $0 \le \theta \le \pi$ and $0 \le \phi \le 2\pi$.

Spin-one-half particles possess an analogous two-level internal degree of freedom. Electrons, protons, and neutrons are standard examples. Atomic nuclei carry a total spin obtained by combining the constituent nucleon spins; depending on the nuclear composition, the effective low-energy degree of freedom may again behave as a spin one-half. A Stern–Gerlach measurement of such a degree of freedom has two possible outcomes.

The spin-state space is therefore again two-dimensional. We conventionally write the basis vectors as $|\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|\downarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. A convenient parameterization of a general spin state is

$$|\theta, \phi\rangle = \cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle. \tag{2.67}$$

with $0 \le \theta \le \pi$ and $0 \le \phi \le 2\pi$. The half-angle $\frac{\theta}{2}$, rather than θ, reflects the characteristic geometry of spin one-half; in particular,

$$|\theta = 0, \phi = 0\rangle = |\uparrow\rangle \quad \text{and} \quad |\theta = \pi, \phi = 0\rangle = |\downarrow\rangle. \tag{2.68}$$

This parameterization is natural because reversing the magnetic-field direction in a Stern–Gerlach apparatus exchanges the two output beams. Field reversal corresponds to $\theta : 0 \to \pi$, while exchanging the two spots corresponds to $|\uparrow\rangle \to |\downarrow\rangle$.

For comparison, rotating a linear polarizer by π leaves its physical polarization axis unchanged. Likewise, for photons $|\theta = 0, \phi = 0\rangle = |x\rangle$ and $|\theta = \pi, \phi = 0\rangle = -|x\rangle$ represent the same physical state up to the overall phase $e^{i\pi}$.

2.9 The Quantum Bit

We have encountered the two-dimensional Hilbert space

$$\mathbb{C}^2 = \left\{\begin{pmatrix}a\\b\end{pmatrix};\ \ a \text{ and } b \in \mathbb{C}\right\} \tag{2.69}$$

equipped with the inner product

$$\begin{pmatrix} \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \bar{c}\, a + \bar{d}\, b \tag{2.70}$$

in two physical settings: photon polarization and spin one-half.

Degrees of freedom described by this Hilbert space are called *two-level systems*. Nature provides many examples. In some cases, such as ideal photon polarization or the spin of an elementary spin-one-half particle, the two-dimensional description is exact for the degree of freedom under consideration. In other situations it is an effective approximation obtained by retaining the two physically relevant levels of a more complicated system. A molecule such as benzene provides a useful illustration. Under ordinary conditions, the molecule can be described in terms of a low-energy superposition $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ of two resonance structures (Figure **2.12**). Absorption of ultraviolet light can promote it to a higher-energy state $\frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$. The drawings should not be interpreted as two static classical configurations; the physical molecular state is their quantum superposition.

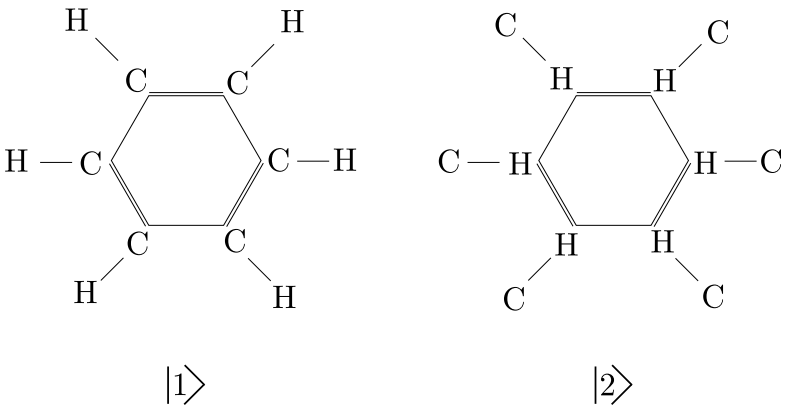


Figure 2.12 Benzene molecule. The bars represent chemical bonds involving electron pairs; double bars represent double bonds. The stable benzene state is the superposition $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$.

Many other effective two-level systems occur in chemistry, molecular and atomic physics, nuclear physics, and particle physics.

A *quantum bit*, or *qubit*, is the abstraction of a two-level quantum system from its specific physical realization. A general qubit state is

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{2.71}$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.

By convention, one often uses the spin-one-half identification $a = \cos\frac{\theta}{2}$ and $b = e^{i\phi}\sin\frac{\theta}{2}$, although the abstract qubit does not require any specific physical interpretation of the basis states.

The qubit combines discrete and continuous features. It is discrete in the sense that its Hilbert space $\mathbb{C}^2$ has dimension two and a projective measurement in a chosen basis has two possible outcomes. It is continuous in the sense that the complex amplitudes α and β vary continuously, subject to normalization. We shall return to this important distinction repeatedly.

2.10 The Bloch Sphere

The Hilbert space description of a normalized qubit state $\mathbb{C}^2$, satisfying $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|a|^2 + |b|^2 = 1$, is abstract. The Bloch sphere (Figure **2.13**) provides a very useful geometric representation based on the parameterization

$$|\psi\rangle = |\theta,\phi\rangle = (\cos\frac{\theta}{2})|0\rangle + e^{i\phi}(\sin\frac{\theta}{2})|1\rangle \tag{2.72}$$

ou

$$|\psi\rangle = |\theta,\phi\rangle = (\cos\frac{\theta}{2})|\uparrow\rangle + e^{i\phi}(\sin\frac{\theta}{2})|\downarrow\rangle \tag{2.73}$$

The state $|\theta,\phi\rangle$ is represented by a unit vector on a sphere. The angle θ is the polar angle measured from z, and ϕ is the azimuthal angle measured from x in the (x,y) plane. Thus θ and ϕ are ordinary spherical coordinates.

The states of the three orthonormal bases below,

$$\{|0\rangle \equiv |\uparrow\rangle \;\; ; \; |1\rangle \equiv |\downarrow\rangle\} \tag{2.74}$$

$$\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \equiv |+\rangle \;\; ; \;\; \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle) \;\equiv |-\rangle\} \tag{2.75}$$

$$\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle) \equiv |\circlearrowleft\rangle \; ; \;\; \frac{1}{\sqrt{2}}(|\uparrow\rangle - i|\downarrow\rangle) \equiv |\circlearrowright\rangle\} \tag{2.76}$$

are represented on the Bloch sphere in Figure **2.14**.

For obvious reasons, these are called the Z, X, and Y bases in quantum information. They are the eigenbases of the three Pauli spin matrices σ_z, σ_x and σ_y, which are themselves often denoted Z, X, and Y.

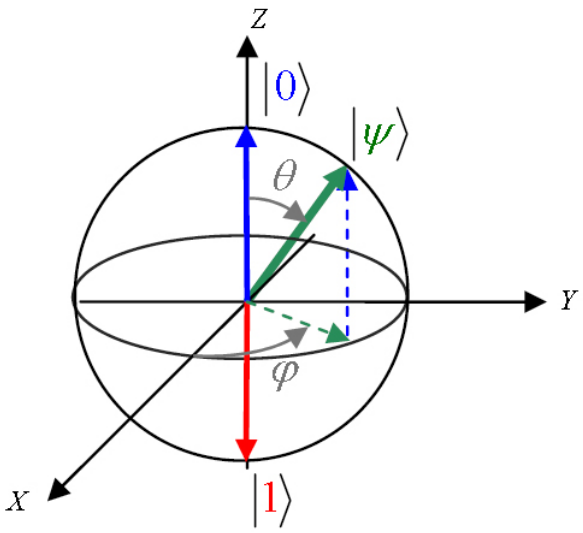


Figure 2.13 The Bloch sphere.

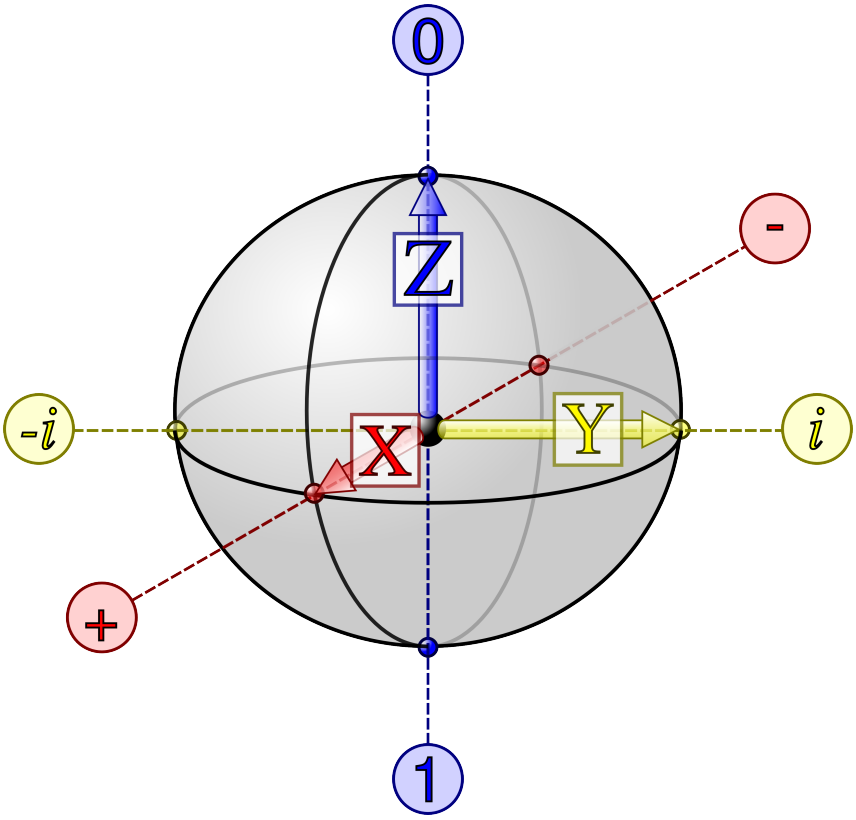


Figure 2.14 The three standard orthonormal bases on the Bloch sphere, with $|i\rangle = |\circlearrowleft\rangle$ and $|-i\rangle = |\circlearrowright\rangle$.

3 Principles of Quantum Mechanics

Modern physics is founded on quantum mechanics. The theory emerged from a sequence of decisive experiments—including atomic spectra, black-body radiation, the photoelectric and Compton effects, electron diffraction by crystals, atomic physics, and the Stern–Gerlach experiment—together with the work of the founders of the field. Among the major milestones were Planck's work on black-body radiation (1900), Einstein's photon hypothesis (1905), Bohr's atomic model (1913), de Broglie's matter waves (1924), Heisenberg's matrix formulation (1925), Schrödinger's wave equation (1926), Born's probabilistic interpretation of the wave function (1926), and Dirac's relativistic quantum mechanics (1930). A brief overview of several of these developments was given in Chapter **1**.

By about 1930, the main physical principles of quantum mechanics were essentially established. Dirac and von Neumann provided a precise mathematical formulation and a coherent framework. Their books *Principles of Quantum Mechanics* (Dirac, 1930) and *Mathematische Grundlagen der Quantenmechanik* (von Neumann, 1932) played a fundamental role. The basic principles remain unchanged today and, together with relativity, successfully describe an extraordinary range of phenomena in condensed-matter, atomic, molecular, nuclear, and subnuclear physics. A consistent quantum theory of gravity, however, remains an open problem, and direct experimental guidance in this regime is extremely limited because gravity is so weak.

The natural mathematical framework of quantum mechanics is Hilbert space: a vector space over the complex numbers equipped with an inner product. We therefore begin with a brief review of the relevant linear algebra and introduce Dirac's bra–ket notation more formally. We then state the postulates that form the basic principles of quantum mechanics.

3.1 Linear Algebra in Dirac Notation

A Hilbert space $\mathcal{H}$ is a vector space over the field $\mathbb{C}$, equipped with an inner product. For finite-dimensional spaces, this definition is sufficient. Infinite-dimensional spaces require additional conditions to control limiting processes; throughout this course, however, we shall work in finite dimension, as is usually the case in quantum information theory.

Vectors are denoted $|\psi\rangle$ (pronounced "ket psi). The Hermitian conjugate (transpose

and complex conjugate) is denoted $\langle\psi|$ (pronounced "bra psi). The inner product between $|\phi\rangle$ and $|\psi\rangle$ is written $\langle\phi|\psi\rangle$ and is also called a "braket. The inner product satisfies:

1. *Positivity*: $\langle\phi|\phi\rangle \geq 0$ with equality if and only if $|\phi\rangle = 0$.
2. *Linearity*: $\langle\phi|(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha\langle\phi|\psi_1\rangle + \beta\langle\phi|\psi_2\rangle$, $\alpha, \beta \in \mathbb{C}$
3. *Symmetry*: $\langle\phi|\psi\rangle = \overline{\langle\psi|\phi\rangle}$ where the bar denotes complex conjugation.

Example 3.1: Quantum bit or two-level system

$\mathcal{H} = \mathbb{C}^2 = \left\{\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \text{ with } \alpha, \beta \in \mathbb{C}\right\}$. The inner product is $(\overline{\gamma}, \overline{\delta})\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \overline{\gamma}\alpha + \overline{\delta}\beta$. In Dirac notation,

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

where $|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}$. Moreover,

$$(\bar{\gamma}, \bar{\delta}) = \bar{\gamma}\langle 0| + \bar{\delta}\langle 1|$$

and

$$(\bar{\gamma}\langle 0| + \bar{\delta}\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \overline{\gamma}\alpha\langle 0|0\rangle + \overline{\gamma}\beta\langle 0|1\rangle + \overline{\delta}\alpha\langle 1|0\rangle + \overline{\delta}\beta\langle 1|1\rangle = \overline{\gamma}\alpha + \overline{\delta}\beta$$

Example 3.2: Particle in three-dimensional space

$\mathcal{H} = L^2(\mathbb{R}^3) = \{f : \mathbb{R}^3 \to \mathbb{C},\ \int \mathrm{d}^3\vec{x}\,|f(\vec{x})|^2 < \infty\}$. The inner product is $\langle f|g\rangle = \int \mathrm{d}^3\vec{x}\,\overline{f(\vec{x})}g(\vec{x})$ and the induced norm is $\|f\|_2 = \langle f|f\rangle^{1/2} = \left(\int \mathrm{d}^3\vec{x}\,|f(\vec{x})|^2\right)^{1/2}$. This space plays a fundamental role in quantum mechanics, but we shall make little further use of it in this course, because we shall focus exclusively on discrete degrees of freedom.

Tensor product. We shall need the notion of the *tensor product*. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two finite-dimensional Hilbert spaces. Let $|i\rangle_1$, $i = 1, ..., n_1$, be an orthonormal basis of $\mathcal{H}_1$, with $\dim\mathcal{H}_1 = n_1$, and let $|j\rangle_2$, $j = 1, ..., n_2$, be an orthonormal basis of $\mathcal{H}_2$, with $\dim\mathcal{H}_2 = n_2$. We define the product space

$$\mathcal{H}_1 \otimes \mathcal{H}_2$$

which is the Hilbert space spanned by the basis vectors

$$|i\rangle_1 \otimes |j\rangle_2$$

(also denoted $|i, j\rangle$ or $|i\rangle_1|j\rangle_2$). This basis contains $n_1 \cdot n_2$ vectors, and therefore

$$\dim\mathcal{H}_1 \otimes \mathcal{H}_2 = n_1 n_2$$

A general vector in the product space has the form

$$|\psi\rangle = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} c_{ij}|i,j\rangle = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} c_{ij}|i\rangle_1 \otimes |j\rangle_2$$

The inner product on the product space is defined by

$$\langle i', j'|i, j\rangle = (\langle i'|_1 \otimes \langle j'|_2)(|i\rangle_1 \otimes |j\rangle_2) = \langle i'|i\rangle_1 \langle j'|j\rangle_2$$

.

Example 3.3: Tensor product of quantum bits

For a single quantum bit, the Hilbert space is $\mathbb{C}^2$. We shall see that the Hilbert space of two quantum bits is $\mathbb{C}^2 \otimes \mathbb{C}^2$. A basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$ is $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$, equivalently $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. A general state is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

We have $\dim \mathbb{C}^2 \otimes \mathbb{C}^2 = 4$, and of course $\mathbb{C}^2 \otimes \mathbb{C}^2$ is isomorphic to $\mathbb{C}^4$.
Here are a few examples of inner products:

- $\langle 00|00\rangle = \langle 0|0\rangle \langle 0|0\rangle = 1$
- $\langle 01|01\rangle = \langle 0|0\rangle \langle 1|1\rangle = 1$
- $\langle 01|11\rangle = \langle 0|1\rangle \langle 1|1\rangle = 0$

From these rules we can compute the inner product of $|\psi\rangle$ and $|\phi\rangle = \beta_{00}|00\rangle + \beta_{01}|01\rangle + \beta_{10}|10\rangle + \beta_{11}|11\rangle$. As expected, we obtain $\langle\phi|\psi\rangle = \overline{\beta}_{00}\alpha_{00} + \overline{\beta}_{01}\alpha_{01} + \overline{\beta}_{10}\alpha_{10} + \overline{\beta}_{11}\alpha_{11}$. It is often convenient to work in the canonical basis of $\mathbb{C}^4$:

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle\ ,\ \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle\ ,\ \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle\ ,\ \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle$$

Once this conventional correspondence has been fixed, the component form of the tensor product follows directly: the rules of the tensor product in components:

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \qquad \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$\begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \qquad \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

These rules generalize immediately to $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$, and more generally to arbitrary tensor products.

Cauchy–Schwarz inequality. As usual,

$$|\langle\phi|\psi\rangle| \leq \langle\phi|\phi\rangle^{1/2}\,\langle\psi|\psi\rangle^{1/2}$$

Completeness relation. Let $|i\rangle$, $i = 1, ..., n$, be an orthonormal basis of an n-dimensional Hilbert space. Any vector can be expanded as

$$|\phi\rangle = \sum_{i=1}^{n} c_i|i\rangle, \qquad c_i = \langle i|\phi\rangle$$

The coefficients c_i are obtained by projecting $|\phi\rangle$ onto the basis vectors. Hence

$$|\phi\rangle = \sum_{i=1}^{n}|i\rangle\,\langle i|\phi\rangle$$

Note that $|i\rangle\langle i|$ is the projector onto $|i\rangle$. Therefore $\sum_{i=1}^{n}|i\rangle\langle i|$ acts as the identity operator on $|\phi\rangle$. We thus obtain the *completeness relation*

$$\sum_{i=1}^{n}|i\rangle\langle i| = \mathbb{1}$$

Observables. In quantum mechanics, observables (measurable quantities) are represented by Hermitian operators acting on $\mathcal{H}$. We briefly recall some important properties.

The map $A : \mathcal{H} \to \mathcal{H}$, $|\psi\rangle \to A|\psi\rangle$ is linear if

$$A(\alpha|\phi_1\rangle + \beta|\phi_2\rangle) = \alpha(A|\phi_1\rangle) + \beta(A|\phi_2\rangle)$$

Any linear map can be represented by a matrix, which we also denote by A.

The matrix elements of A in the orthonormal basis $\{|i\rangle, i = 1, ..., n\}$ of $\mathcal{H}$ are denoted $\langle i|A|j\rangle$ or A_{ij}. Given A, its *adjoint*, denoted $A^\dagger$, is defined by

$$\langle\phi|A^\dagger|\psi\rangle = \overline{\langle\psi|A|\phi\rangle}$$

Thus the adjoint (or Hermitian conjugate) is represented by the transpose complex-conjugate matrix. For the matrix elements, transpose and complex conjugate. We have for the elements of matrix

$$\langle i|A^\dagger|j\rangle = \overline{\langle j|A|i\rangle}, \qquad (A^\dagger)_{ij} = \overline{A_{ij}}$$

We say that A is Hermitian if $A = A^\dagger$. One can verify that $(A + B)^\dagger = A^\dagger + B^\dagger$ and $(AB)^\dagger = B^\dagger A^\dagger$.

We also define the *commutator*

$$[A, B] = AB - BA$$

and the *anticommutator*

$$\{A, B\} = AB + BA$$

Projectors in Dirac notation. The linear operator

$$|i\rangle\langle i| = P_i$$

is the projector onto the basis vector $|i\rangle$. If P_i is a projector, then $P_i^\dagger = P_i$ and $P_i^2 = P_i$. In Dirac notation this follows immediately:

$$P_i^\dagger = (|i\rangle\langle i|)^\dagger = (\langle i|)^\dagger(|i\rangle)^\dagger = |i\rangle\langle i| = P_i$$

$$P_i^2 = (|i\rangle\langle i|)(|i\rangle\langle i|) = |i\rangle \underbrace{\langle i|i\rangle}_{=1}\langle i| = |i\rangle\langle i| = P_i$$

Since $|i\rangle$ and $|j\rangle$ are orthogonal for $i \neq j$ we have $P_iP_j = P_jP_i = 0$. Indeed,

$$P_iP_j = (|i\rangle\langle i|)(|j\rangle\langle j|) = |i\rangle \underbrace{\langle i|j\rangle}_{=0}\langle j|) = 0$$

$$P_jP_i = (|j\rangle\langle j|)(|i\rangle\langle i|) = |j\rangle \underbrace{\langle j|i\rangle}_{=0}\langle i|) = 0$$

If $|\phi\rangle$ is any normalized vector in the Hilbert space, then $P_\phi = |\phi\rangle\langle\phi|$ is the projector onto $|\phi\rangle$.

Spectral decomposition. Every Hermitian operator on a finite-dimensional Hilbert space admits a *spectral decomposition*, Hilbert have a *decomposition spectral*,

$$A = \sum_n a_n P_n$$

where $a_n \in \mathbb{R}$ are the eigenvalues and P_n the corresponding eigenprojectors. In the nondegenerate case, we have

$$P_n = |\phi_n\rangle\langle\phi_n|$$

where $|\phi_n\rangle$ is the eigenvector associated with eigenvalue a_n:

$$A|\phi_n\rangle = a_n|\phi_n\rangle$$

Eigenvectors (and eigenprojectors) associated with distinct eigenvalues are orthogonal. Moreover, they satisfy the completeness relation

$$\mathbb{1} = \sum_n P_n = \sum_n |\phi_n\rangle\langle\phi_n|$$

The spectral decomposition is therefore often written in the form

$$A = \sum_n a_n|\phi_n\rangle\langle\phi_n|$$

3.2 Principles of Quantum Mechanics

We now state five basic principles of quantum mechanics:

- an isolated system is described by a *state vector (ket) in a Hilbert space*;
- the state vector *evolves unitarily in time*;
- *observables* are represented by *Hermitian operators*;
- measurement is a process distinct from unitary time evolution and involves a *probabilistic projection*;
- composite systems are described by tensor-product Hilbert spaces.

Principle 1: State vectors. The state of a system isolated from the rest of the universe is *completely* specified by a vector in its Hilbert space. The state vector $|\psi\rangle \in \mathcal{H}$ is normalized so that $\langle\psi|\psi\rangle = 1$.

Example 3.4: Examples of state vectors

- The polarization of a photon (Section 2.2) is described by $\mathcal{H} = \mathbb{C}^2$. A general state vector is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. A linearly polarized state may be written $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, while a circular or elliptic polarization can be represented by $|\tilde{\theta}\rangle = \cos\theta|0\rangle + i\sin\theta|1\rangle$, or more generally by
$$\cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$$
- A spin-$\frac{1}{2}$ degree of freedom (for example that of an electron; see Section 2.7) is described by the same Hilbert space. A natural parameterization is
$$\cos\frac{\theta}{2}|0\rangle + e^{i\delta}\sin\frac{\theta}{2}|1\rangle$$
The Bloch sphere (Section 2.10) provides a natural geometric representation of these states.
- For a particle in $\mathbb{R}^3$, one has $\mathcal{H} = L^2(\mathbb{R}^3)$. The state vectors are normalized wave functions satisfying $\int \mathrm{d}^3\vec{x}\,|\psi(\vec{x})|^2 = 1$.

Principle 2: Time evolution. An isolated system evolves unitarily in time. Thus, if $|\psi\rangle$ is the state at time 0, then at time t the state has the form $U_t|\psi\rangle$, where U_t is a unitary operator on $\mathcal{H}$. Unitarity means $U_t^\dagger U_t = U_t U_t^\dagger = \mathbb{1}$, equivalently $U_t^{-1} = U_t^\dagger$.

The family of time-evolution operators forms a group (more precisely, a representation of the group of time translations):

$$U_{t=0} = \mathbb{1}, \qquad U_{t_1}U_{t_2} = U_{t_1+t_2}$$

Quantum mechanics tells us how to determine U_t for a given system by solving the *Schrödinger equation* (Section 1.7). In quantum information we often take a more operational viewpoint: we assume that an engineer or experimental physicist can build

a device (a quantum circuit) implementing the desired unitary operation U_t, which is specified by the quantum algorithm. We shall return to this viewpoint later in the course.

Example 3.5: Hadamard gate

A semitransparent beam splitter divides an incident beam into reflected and transmitted components. Let $\mathcal{H} = \mathbb{C}^2$ be the Hilbert space with basis $|T\rangle$, $|R\rangle$. The beam splitter acts unitarily:

$$|T\rangle \rightarrow \boxed{\text{H}} \rightarrow H|T\rangle = \frac{1}{\sqrt{2}}(|T\rangle + |R\rangle)$$

$$|R\rangle \rightarrow \boxed{\text{H}} \rightarrow H|R\rangle = \frac{1}{\sqrt{2}}(|T\rangle - |R\rangle)$$

The unitary matrix H is called the Hadamard matrix, or Hadamard gate:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Principle 3: Observables. In quantum mechanics, an observable quantity (energy, magnetic moment, angular momentum, position, momentum, velocity, etc.) is represented by a Hermitian operator.

It is not always obvious how to choose the operator corresponding to a given physical quantity. A correspondence principle (Section **1.8**) provides a practical rule for constructing quantum operators from classical quantities. This rule can be ambiguous because operators need not commute. Moreover, some observables, such as spin, have no direct classical analogue.

Example 3.6: Some observables

- Position x, momentum $p = \frac{\hbar}{i}\frac{\partial}{\partial x}$, energy or Hamiltonian $\frac{p^2}{2m} + V(x)$. We shall not need these observables explicitly in this course.
- Photon polarization. A photon is sent through a birefringent analyzer (Section 2.3). If detector D_y clicks we record -1, whereas if D_x clicks we record $+1$. These outcomes are described by the observable

$$\mathcal{P} = (+1)|x\rangle\langle x| + (-1)|y\rangle\langle y|$$

  This observable is represented by the Hermitian matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (expressed in the basis $\{|x\rangle, |y\rangle\}$).
- Every observable (Hermitian operator) on $\mathcal{H} = \mathbb{C}^2$ can be represented by a 2×2 matrix 2×2

$$A = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \gamma \end{pmatrix}$$

  or, in Dirac notation,

$$A = \alpha|0\rangle\langle 0| + \beta|0\rangle\langle 1| + \overline{\beta}|1\rangle\langle 0| + \gamma|1\rangle\langle 1|$$

  Every 2×2 Hermitian matrix can be written as a linear combination of the matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

  The Hermitian matrices X, Y, and Z are called the Pauli matrices.

  The Pauli matrices are used, among other things, to describe a spin-$\frac{1}{2}$ degree of freedom: the spin operator is represented by the three-component vector $\Sigma = (X, Y, Z)$. In the physics literature one usually writes $\Sigma = (\sigma_x, \sigma_y, \sigma_z)$. Important properties of these matrices include

$$X^2 = Y^2 = Z^2 = I, \; XY = -YX, \; XZ = -ZX, \; YZ = -ZY$$

  and

$$[X, Y] = 2iZ, \; [Y, Z] = 2iX, \; [Z, X] = 2iY$$

Principle 4: Measurement postulate. Let a system be prepared in the state $|\psi\rangle$. We wish to measure an observable of the system using a measurement apparatus. The apparatus is modeled by a set of orthogonal projectors $\{P_n\}$ satisfying $\sum_n P_n = \mathbb{1}$. A measurement *projects*[1] the state $|\psi\rangle$ onto one of the subspaces associated with the projectors. Immediately after the measurement the state is

$$|\phi_n\rangle = \frac{P_n|\psi\rangle}{\| P_n|\psi\rangle\|} = \frac{P_n|\psi\rangle}{\langle\psi|P_n|\psi\rangle^{1/2}}$$

[1] Physicists often say that the state, or wave function, is "collapsed.

For a single measurement, the outcome n cannot in general be predicted with certainty: it is random. If the measurement is repeated many times on identically prepared systems, the probability of obtaining outcome n is

$$\mathbb{P}\left[\text{result } n\right] = |\langle \phi_n|\psi\rangle|^2 = \langle \psi|P_n|\psi\rangle$$

Remark 1. Since $\sum_j P_j = \mathbb{1}$ and $|\psi\rangle$ is normalized, we have

$$\sum_j \mathbb{P}\left[\text{result } j\right] = 1$$

Remark 2. If $P_j = |j\rangle\langle j|$, the probability of obtaining outcome j is

$$\mathbb{P}\left[\text{result } j\right] = \langle \psi|P_j|\psi\rangle = |\langle j|\psi\rangle|^2$$

and the post-measurement state is $|j\rangle$.

An important consequence for the measurement of observables. This point is fundamental because experiments directly access observables. A measurement apparatus modeled by a set of projectors $\{P_n\}$ can measure any observable of the form $A = \sum_j a_j P_j$. A measurement projects $|\psi\rangle$ onto $|\phi_n\rangle$ for some outcome n. Since $A|\phi_n\rangle = a_n|\phi_n\rangle$, the measured value of A is precisely a_n.

The expectation value of repeated measurements of A on systems prepared in the state $|\psi\rangle$ is

$$\sum_j a_j \langle \psi|P_j|\psi\rangle = \langle \psi|A|\psi\rangle$$

and the variance is

$$\sum_j a_j^2 \langle \psi|P_j|\psi\rangle - \left(\sum_j a_j \langle \psi|P_j|\psi\rangle\right)^2 = \langle \psi|A^2|\psi\rangle - \langle \psi|A|\psi\rangle^2$$

In practice, the right-hand sides of these expressions are used to compute expectation values and variances.

After a measurement, the state vector has collapsed according to $|\psi\rangle \to |\phi_n\rangle$. In the resulting eigenstate $|\phi_n\rangle$, the expectation value of A is a_n and the variance is zero.

Moreover, a single measurement apparatus can simultaneously measure only observables that share an eigenbasis. In particular, simultaneous measurement with the same apparatus is meaningful only when the observables have compatible eigenprojectors. They may have different eigenvalues, but the corresponding operators must commute.

Example 3.7: Measurement of the polarization of the photon

To measure the observable

$$\mathcal{P} = |x\rangle\langle x| - |y\rangle\langle y|$$

we use an apparatus consisting of an analyzer oriented along x followed by a detector. This apparatus realizes the measurement basis $\{|x\rangle, |y\rangle\}$. If the photon passes through the analyzer, the post-measurement state is $|x\rangle$; if it is absorbed, the post-measurement state is $|y\rangle$. The corresponding probabilities are after the measurement is $|y\rangle$. The probabilities associated are

$$\mathbb{P}\,[\text{result } +1)] = |\langle x|\psi\rangle|^2, \quad \mathbb{P}\,[\text{result } -1] = |\langle y|\psi\rangle|^2$$

If the initial polarization state is $|\psi\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$, these probabilities are simply $\cos^2\theta$ and $\sin^2\theta$. Now suppose that the analyzer is rotated by an angle γ. This corresponds to measuring the observable

$$\mathcal{P} = |\gamma\rangle\langle\gamma| - |\gamma_\perp\rangle\langle\gamma_\perp|$$

The associated probabilities are

$$\mathbb{P}\,[\text{result } +1] = |\langle\gamma|\psi\rangle|^2 = \cos^2(\theta-\gamma)$$

$$\mathbb{P}\,[\text{result } -1] = |\langle\gamma_\perp|\psi\rangle|^2 = \sin^2(\theta-\gamma)$$

Finally, note that in the first case the measured observable is represented by the matrix

$$\mathcal{P} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and in the second case

$$\mathcal{P} = \begin{pmatrix} \cos 2\gamma & \sin 2\gamma \\ \sin 2\gamma & -\cos 2\gamma \end{pmatrix} = (\cos 2\gamma)Z + (\sin 2\gamma)X$$

.

Heisenberg uncertainty principle. Consider a system in the state $|\psi\rangle$ and two observables A and B, with spectral decompositions

$$A = \sum_j a_j P_j, \quad B = \sum_j b_j Q_j$$

As explained above, in the state $|\psi\rangle$ the observables have expectation values $\langle\psi|A|\psi\rangle$ and $\langle\psi|B|\psi\rangle$, and standard deviations $\Delta A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$ and $\Delta B = \sqrt{\langle\psi|B^2|\psi\rangle - \langle\psi|B|\psi\rangle^2}$.

The Heisenberg uncertainty relation states that

$$\Delta A \cdot \Delta B \geq \frac{1}{2}\langle\psi|[A,B]|\psi\rangle$$

The interpretation of this inequality is as follows. If $[A,B] \neq 0$, the two observables

cannot in general be determined simultaneously with arbitrarily small uncertainty. The familiar example is $A = x$ (position) and $B = p = \frac{\hbar}{i}\frac{\partial}{\partial x}$ (momentum). In this case $\Delta x \Delta p \geq \frac{h}{4\pi}$: position and momentum cannot both be measured with arbitrary precision. This is not a technological limitation, but a fundamental consequence of the laws of quantum mechanics.

If $[A, B] = 0$, there exists a common basis of the Hilbert space in which both A and B are diagonal. Measuring in this basis allows the two observables to be determined simultaneously. There is no contradiction with the uncertainty principle, because the right-hand side of the Heisenberg inequality vanishes when $[A, B] = 0$.

Principle 5: Composite quantum systems. Consider two systems $\mathcal{A}$ and $\mathcal{B}$ with Hilbert spaces $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$. The Hilbert space of the composite system $\mathcal{AB}$ is the tensor product

$$\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$$

The states of $\mathcal{AB}$ are vectors $|\psi\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. The preceding postulates apply unchanged to composite systems.

This postulate is far from trivial, and we shall explore several of its consequences. Einstein, Podolsky, Rosen, and Schrödinger were among the first to analyze its implications. Their work ultimately led to Bell inequalities and, much later, to protocols such as quantum teleportation and superdense coding, which play central roles in quantum information.

Example 3.8: Composite system

N quantum bits have Hilbert space

$$\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{N \text{ copies}}$$

If $\{|0\rangle, |1\rangle\}$ is a basis of $\mathbb{C}^2$, then a basis of the composite system is

$$|b_1\rangle \otimes |b_2\rangle \ldots \otimes |b_N\rangle = |b_1 \ldots b_N\rangle$$

where $b_i \in \{0, 1\}$. There are 2^N basis states, in one-to-one correspondence with the 2^N classical bit strings of length N. A general state of N quantum bits is a superposition of these basis states:

$$|\psi\rangle = \sum_{b_1 \ldots b_N} c_{b_1 \ldots b_N} |b_1 \ldots b_N\rangle$$

where the coefficients $c_{b_1 \ldots b_N}$ satisfy

$$\sum_{b_1 \ldots b_N} |c_{b_1 \ldots b_N}|^2 = 1$$

3.3 Product States and Entangled States

The states of a composite system $\mathcal{AB}$ belong to $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. A state is a *product state* if it can be written as it can be represented as

$$|\psi\rangle = |\phi\rangle_\mathcal{A} \otimes |\gamma\rangle_\mathcal{B}$$

Such a state is also said to be *separable*.
An *entangled state* $|\psi\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ is a state for which no vectors $|\phi\rangle_\mathcal{A} \in \mathcal{H}_\mathcal{A}$ and $|\gamma\rangle_\mathcal{B} \in \mathcal{H}_\mathcal{B}$ exist such that $|\psi\rangle = |\phi\rangle_\mathcal{A} \otimes |\gamma\rangle_\mathcal{B}$.

Entangled states generate correlations between subsystems $\mathcal{A}$ and $\mathcal{B}$ that have no classical counterpart. These correlations are a key resource in quantum-information protocols such as teleportation.

Example 3.9: Examples of product and entangled states

Consider two quantum bits with $\mathcal{A} \otimes \mathcal{B} = \mathbb{C}^2 \otimes \mathbb{C}^2$.

- Some simple product states:

$$|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} = |00\rangle$$
$$|0\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B} = |01\rangle$$
$$|1\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} = |10\rangle$$
$$|1\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B} = |11\rangle$$

- Some less obvious product states:

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} + |1\rangle_\mathcal{B}) \otimes |0\rangle_\mathcal{B} = \frac{1}{2}(|00\rangle + |10\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} + |1\rangle_\mathcal{B}) \otimes \frac{1}{\sqrt{2}}(|0\rangle_\mathcal{B} - |1\rangle_\mathcal{B}) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

- Examples of entangled states that cannot be written as product states:

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} + |1\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} - |1\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$\frac{1}{\sqrt{2}}(|1\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} + |0\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} - |1\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

These four states play a special role and are called the Bell states.

Generation of entangled states. Consider a composite system initially in the product state $|\phi\rangle_{\mathcal{A}} \otimes |\chi\rangle_{\mathcal{B}}$. For example, the two subsystems might be electrons in the spin state $|\uparrow\rangle \otimes |\downarrow\rangle$. If they evolve independently without interaction, the unitary time-evolution operator has the form $U_{\mathcal{A}} \otimes U_{\mathcal{B}}$ and

$$U_{\mathcal{A}} \otimes U_{\mathcal{B}}(|\uparrow\rangle \otimes |\downarrow\rangle) = U_{\mathcal{A}}|\uparrow\rangle \otimes U_{\mathcal{B}}|\downarrow\rangle$$

so the state remains a product state.

To generate entanglement, $\mathcal{A}$ and $\mathcal{B}$ must interact, so that the joint time-evolution operator satisfies $U_{\mathcal{AB}} \neq U_{\mathcal{A}} \otimes U_{\mathcal{B}}$. Known physical interactions are local in space and time; two systems that are entangled must therefore have interacted directly or through a common mediator in their past.

3.4 Impossibility of Cloning an Unknown Quantum State

Classical information can be copied freely. A text, for example, can be duplicated by a universal photocopier: the same machine can copy any document. to photocopier "universal": the same machine can copy all the textes.

Now consider a set of quantum states $|\psi\rangle \in \mathcal{H}$ and suppose we wish to construct a universal quantum machine that copies an arbitrary state $|\psi\rangle \in \mathcal{H}$. Such a physical process, if deterministic and reversible, would have to be described by a unitary operator U. The Hilbert space is $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, where $\mathcal{A}$ contains the states to be copied and $\mathcal{B}$ is the copy register. We begin with the initial state

$$|\psi\rangle \otimes |\text{blank}\rangle$$

The desired machine would produce

$$|\psi\rangle \otimes |\text{blank}\rangle \rightarrow \boxed{\text{U}} \rightarrow |\psi\rangle \otimes |\psi\rangle$$

Mathematically, the question is whether there exists a unitary operator such that, for every state in a sufficiently large set, $|\psi\rangle$ satisfies

$$U(|\psi\rangle \otimes |\text{blank}\rangle) = |\psi\rangle \otimes |\psi\rangle$$

The answer is no. This statement is known as the *no-cloning theorem*. It is nevertheless possible to clone a set of mutually orthogonal states using an appropriate unitary U that depends on the chosen set.

Proof of the no-cloning theorem. Suppose that there exists U such that $U^\dagger U = UU^\dagger = 1$ with

$$U(|\phi_1\rangle \otimes |\text{blank}\rangle) = |\phi_1\rangle \otimes |\phi_1\rangle$$

$$U(|\phi_2\rangle \otimes |\text{blank}\rangle) = |\phi_2\rangle \otimes |\phi_2\rangle$$

Taking the Hermitian conjugate of the second equation gives

$$(\langle\phi_2| \otimes \langle\text{blank}|)U^\dagger = \langle\phi_2| \otimes \langle\phi_2|$$

Taking the inner product with the first equation then yields

$$\langle\phi_2| \otimes \langle \text{blank}|U^\dagger U|\phi_1\rangle \otimes |\text{blank}\rangle = (\langle\phi_2| \otimes \langle\phi_2|)(|\phi_1\rangle \otimes |\phi_1\rangle)$$

which implies

$$\langle\phi_2|\phi_1\rangle \langle \text{blank}|\text{blank}\rangle = \langle\phi_2|\phi_1\rangle^2$$

and therefore

$$\langle\phi_2|\phi_1\rangle = 0 \text{ or } \langle\phi_2|\phi_1\rangle = 1$$

We conclude that the same unitary U cannot clone two distinct nonorthogonal states $|\phi_1\rangle$ and $|\phi_2\rangle$. It can clone a prescribed orthogonal basis, or any specified set of mutually orthogonal states.

Nonorthogonal states cannot be perfectly distinguished.

There are several variants and refinements of the no-cloning theorem. Consider two states $|\psi\rangle$ and $|\phi\rangle$ and suppose we try to construct a unitary device that distinguishes them. We introduce an ancillary state $|a\rangle$ and ask whether there exists a unitary matrix U such that

Mathematically, we seek a unitary operator satisfying

$$U|\psi\rangle \otimes |a\rangle = |\psi\rangle \otimes |v\rangle$$

$$U|\phi\rangle \otimes |a\rangle = |\phi\rangle \otimes |v'\rangle$$

where the output states $|v\rangle$ and $|v'\rangle$ would have to be distinguishable. Taking the inner product of these two relations gives

$$\langle\phi| \otimes \langle a|U^\dagger U|\psi\rangle \otimes |a\rangle = (\langle\phi| \otimes \langle v'|)(|\psi\rangle) \otimes |v\rangle)$$

which implies

$$\langle\phi|\psi\rangle \langle a|a\rangle = \langle\phi|\psi\rangle \langle v'|v\rangle$$

If $|\phi\rangle$ is not orthogonal to $|\psi\rangle$, then $\langle\phi|\psi\rangle \neq 0$, and therefore

$$\langle v'|v\rangle = \langle a|a\rangle = 1$$

Hence $|v\rangle = |v'\rangle$. The output register contains no information that can distinguish $|\psi\rangle$ from $|\phi\rangle$.

4 The Density Matrix

We have formulated the postulates of quantum mechanics for isolated systems. In particular, the state of an isolated system is described by a normalized Hilbert-space vector $|\psi\rangle \in \mathcal{H}$. In practice, however, this description is often insufficient. No physical system is perfectly isolated, and when coupling to the environment becomes relevant we must use the more general density-matrix formalism. A second important application concerns statistical ensembles. Consider, for example, a box containing photons of which 30% are in polarization state $|H\rangle$, 20% in $|V\rangle$, and 50% in $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. If a small aperture is opened so that photons leave the box one at a time at random, the box acts as a source emitting the states $\left\{|H\rangle, |V\rangle, \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)\right\}$ with probabilities $\left\{\frac{3}{10}, \frac{1}{5}, \frac{1}{2}\right\}$. This is a statistical ensemble, and the density matrix is the natural tool for describing it.

4.1 Mixed States and the Density Matrix

Let $\mathcal{H}$ be a Hilbert space. Normalized vectors $|\psi\rangle \in \mathcal{H}$, or equivalently rank-one projectors $|\psi\rangle\langle\psi|$, are called *pure states*. If A is an observable, i.e. a Hermitian operator $A : \mathcal{H} \to \mathcal{H}$, a pure state defines a positive linear functional on the algebra of observables $\mathcal{B}(\mathcal{H})$[1]:

$$\mathrm{Av}_\psi : \begin{array}{ccc} \mathcal{B}(\mathcal{H}) & \longrightarrow & \mathbb{C} \\ A & \mapsto & \mathrm{Av}_\psi(A) = \langle\psi|A|\psi\rangle \end{array}$$

which gives the expectation value of A in repeated measurements on systems prepared in the state $|\psi\rangle$. Note that

$$\mathrm{Av}_\psi(A) = \langle\psi|A|\psi\rangle = \mathrm{Tr}\,(A|\psi\rangle\langle\psi|) \tag{4.1}$$

This functional has three important properties:

1. $\mathrm{Av}_\psi(\lambda A + \mu B) = \lambda \mathrm{Av}_\psi(A) + \mu \mathrm{Av}_\psi(B) \qquad \forall \lambda, \mu \in \mathbb{C},\ \forall A, B \in \mathcal{B}(\mathcal{H})$
2. $\mathrm{Av}_\psi(\mathbb{1}) = 1$
3. If $A \geq 0$[2], then $\mathrm{Av}_\psi(A) \in \mathbb{R}_+$.

[1] $\mathcal{B}(\mathcal{H})$ denotes the bounded linear operators on $\mathcal{H}$. In quantum information the Hilbert spaces considered are usually finite-dimensional, so every linear operator is bounded. In infinite-dimensional quantum mechanics, unbounded operators also arise and require the tools of functional analysis.

[2] A Hermitian matrix A is positive semidefinite if $\vec{x}^\dagger A \vec{x} \geq 0$ for every $\vec{x}$. Equivalently, all eigenvalues of A are nonnegative.

We now generalize the notion of a quantum state.

Definition 1: quantum state

Given a Hilbert space $\mathcal{H}$, a general quantum state can be defined as a normalized positive linear functional on the observables:

$$\begin{array}{rccc} \mathrm{Av}: & \mathcal{B}(\mathcal{H}) & \longrightarrow & \mathbb{C} \\ & A & \mapsto & \mathrm{Av}(A) \end{array}$$

that is, $\mathrm{Av}(\lambda A + \mu B) = \lambda \mathrm{Av}(A) + \mu \mathrm{Av}(B)$, $\mathrm{Av}(\mathbb{1}) = 1$, and $\mathrm{Av}(A) \in \mathbb{R}_+$ whenever $A \geq 0$.

This definition may appear abstract, but a standard theorem of linear algebra states that every such positive linear functional can be represented by a matrix ρ satisfying

$$\mathrm{Av}(A) = \mathrm{Tr}(A\rho)$$

with $\rho = \rho^\dagger$, $\rho \geq 0$, and $\mathrm{Tr}(\rho) = 1$. The matrix ρ is called the *density matrix*. The set of density matrices is convex.

Example 4.1: Pure state

If a system is described by a normalized state vector $|\psi\rangle$, then $\rho = |\psi\rangle\langle\psi|$. In this case ρ is a rank-one projector onto $|\psi\rangle$. It satisfies $\rho = \rho^\dagger$ and $\rho \geq 0$, and the normalization condition $\langle\psi|\psi\rangle = 1$ is equivalent to $\mathrm{Tr}(\rho) = 1$. Such a density matrix represents a pure state.

Example 4.2: Gas of photons

For the photon gas described in the introduction, suppose that we measure an observable A on each photon leaving the box. Averaging over many photons gives

$$\frac{3}{10}\langle H|A|H\rangle + \frac{1}{5}\langle V|A|V\rangle + \frac{1}{2}\left(\frac{\langle H| + \langle V|}{\sqrt{2}}\right)A\left(\frac{|H\rangle + |V\rangle}{\sqrt{2}}\right)$$
$$= \mathrm{Tr}\left(A\left\{\frac{3}{10}|H\rangle\langle H| + \frac{1}{5}|V\rangle\langle V| + \frac{1}{2}\left(\frac{|H\rangle + |V\rangle}{\sqrt{2}}\right)\left(\frac{\langle H| + \langle V|}{\sqrt{2}}\right)\right\}\right)$$

In other words, this photon source is described by the density matrix

$$\rho = \frac{3}{10}|H\rangle\langle H| + \frac{1}{5}|V\rangle\langle V| + \frac{1}{2}\left(\frac{|H\rangle + |V\rangle}{\sqrt{2}}\right)\left(\frac{\langle H| + \langle V|}{\sqrt{2}}\right)$$

Definition 2: quantum state

A mixed state is a density matrix of the form

$$\rho = \sum_{i=1}^{k} p_i|\varphi_i\rangle\langle\varphi_i|$$

where $\{|\varphi_1\rangle, \ldots, |\varphi_k\rangle\}$ is a set of normalized, not necessarily orthogonal, states and $\{p_1, \ldots, p_k\}$ is a probability distribution with $p_i \geq 0$ and $\sum_i p_i = 1$.

The state is pure when $k = 1$. Pure states are the extreme points of the convex set of density matrices. A state with a nontrivial statistical mixture of distinct states is called mixed.

The two definitions of a quantum state are equivalent. Starting from Definition 2, $\rho = \rho^\dagger$ because each term is Hermitian, $\rho \geq 0$ because it is a convex combination of positive projectors, and $\mathrm{Tr}(\rho) = \sum_i p_i = 1$. Conversely, every positive Hermitian matrix with unit trace admits a spectral decomposition

$$\rho = \sum_{i=1}^{d} \lambda_i|\chi_i\rangle\langle\chi_i|$$

where $\rho|\chi_i\rangle = \lambda_i|\chi_i\rangle$ and $\{|\chi_i\rangle\}$ is an orthonormal basis. Since $\rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$, the eigenvalues satisfy $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$, so they form a probability distribution.

Remark 1. The spectral decomposition used in this argument need not coincide with the physical preparation of a statistical ensemble. More generally, knowing only a density matrix ρ does not necessarily determine the underlying physical preparation that produced it.

Remark 2. In a decomposition $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$, the states $|\varphi_i\rangle$ need not be orthogonal, and the decomposition is not unique. It may or may not correspond directly to a physical preparation procedure.

Remark 3. We shall see below that density matrices also describe subsystems that are entangled with an environment. This situation is physically distinct from an ordinary statistical mixture.

Measurement on a Density Matrix

It remains to explain how the measurement postulate is expressed in the density-matrix formalism. For pure states the predictions must, of course, agree with those obtained from the state-vector description.

Let $A \in \mathcal{B}(\mathcal{H})$ be an observable with spectral decomposition $A = \sum_i \alpha_i |\varphi_i\rangle\langle\varphi_i| = \sum_i \alpha_i P_i$, where $\{|\varphi_i\rangle\}$ is an orthonormal basis of $\mathcal{H}$. Consider a pure state represented either by the ket $|\psi\rangle$ or equivalently by the density matrix $\rho = |\psi\rangle\langle\psi|$. From Chapter **3**, the expectation value of A in repeated measurements is

$$\langle\psi|A|\psi\rangle$$

On the other hand, the density matrix was defined so that

$$\mathrm{Av}(A) = \mathrm{Tr}(A\rho) \tag{4.2}$$

Equation (4.1) shows that the two expressions are indeed identical.

For a single measurement of A on the state $|\psi\rangle$, the outcome is one of the eigenvalues α_i of A, with probability

$$\mathbb{P}\,[\alpha_i] = |\langle\varphi_i|\psi\rangle|^2$$

Now $|\langle\varphi_i|\psi\rangle|^2 = \langle\psi|P_i|\psi\rangle$ is precisely the expectation value of the projector P_i. It is therefore natural to define

$$\mathbb{P}\,[\alpha_i] = \mathrm{Tr}(P_i\rho) \tag{4.3}$$

in the density-matrix formalism.

Finally, if the outcome α_i is obtained, the state $|\psi\rangle$ is projected onto the corresponding eigenspace. In state-vector notation the post-measurement state is[3]

$$|\psi'\rangle = \frac{P_i|\psi\rangle}{\sqrt{\mathbb{P}\,[\alpha_i]}}$$

The corresponding density matrix is

$$\rho' = |\psi'\rangle\langle\psi'| = \frac{P_i|\psi\rangle\langle\psi|P_i^\dagger}{\sqrt{\mathbb{P}\,[\alpha_i]^2}} = \frac{P_i\rho P_i}{\mathbb{P}\,[\alpha_i]} \tag{4.4}$$

[3] $P_i|\psi\rangle$ projects $|\psi\rangle$ onto the eigenspace associated with α_i, and the factor $\sqrt{\mathbb{P}\,[\alpha_i]}$ provides the required normalization.

Equations (4.2), (4.3), and (4.4) provide the measurement rules in density-matrix form. Importantly, the same formulas remain valid for mixed states.

4.2 Density Matrix for One Qubit

The states of a single qubit are completely characterized by 2×2 density matrices. The Pauli matrices

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

form a basis for the real vector space of 2×2 Hermitian matrices. Hence

$$\rho = \frac{a_0}{2}\mathbb{1} + \frac{a_1}{2}X + \frac{a_2}{2}Y + \frac{a_3}{2}Z$$

Because ρ is Hermitian, the coefficients a_0, a_1, a_2, a_3 are real. The condition $\mathrm{Tr}(\rho) = 1$ implies $a_0 = 1$, so

$$\rho = \frac{1}{2}\left(\mathbb{1} + \vec{a} \cdot \vec{\Sigma}\right) = \frac{1}{2}\begin{pmatrix} 1 + a_3 & a_1 - ia_2 \\ a_1 + ia_2 & 1 - a_3 \end{pmatrix}$$

where $\vec{a} = (a_1, a_2, a_3)$ and $\vec{\Sigma} = (X, Y, Z)$. Positivity of ρ is equivalent, in the 2×2 case with unit trace, to $\det(\rho) \geq 0$. Thus

$$\det(\rho) = 1 - \|\vec{a}\|^2 \geq 0$$

i.e. $\|\vec{a}\|^2 \leq 1$. Therefore the set of one-qubit density matrices is $\left\{\rho = \frac{1}{2}(\mathbb{1} + \vec{a} \cdot \vec{\Sigma}) \mid \|\vec{a}\|^2 \leq 1\right\}$.

The ball $\|\vec{a}\|^2 \leq 1$ is convex, and its extreme points lie on the sphere $\|\vec{a}\|^2 = 1$. These extreme points are precisely the pure states. Indeed,

$$\begin{aligned}
\rho^2 &= \frac{1}{4}\left(\mathbb{1} + \vec{a} \cdot \vec{\Sigma}\right)^2 \\
&= \frac{1}{4}\left(\mathbb{1} + a_1^2X^2 + a_2^2Y^2 + a_3^2Z^2\right) + \frac{1}{4}2\vec{a} \cdot \vec{\Sigma} \\
&+ \frac{1}{4}a_1a_2\underbrace{(XY + YX)}_{0} + \frac{1}{4}a_1a_3\underbrace{(XZ + ZX)}_{0} + \frac{1}{4}a_2a_3\underbrace{(YZ + ZY)}_{0} \\
&= \frac{\mathbb{1}}{4}\underbrace{(1 + \|\vec{a}\|^2)}_{2} + \frac{1}{2}\vec{a} \cdot \vec{\Sigma} \\
&= \frac{1}{2}\left(\mathbb{1} + \vec{a} \cdot \vec{\Sigma}\right) \\
&= \rho
\end{aligned}$$

thus ρ is a projector if and only if $\|\vec{a}\|^2 = 1$.

The ball $\|\vec{a}\|^2 \leq 1$ is called the *Bloch ball*. It generalizes the Bloch sphere, which

is simply its surface and represents the pure states. Pure qubit states require only two angular parameters, whereas mixed states additionally require the radial coordinate inside the ball. The center $\vec{a} = (0,0,0)$ corresponds to the maximally mixed state $\frac{1}{2}\mathbb{1}$. The vectors $\vec{a} = (0,0,\pm 1)$ represent the orthogonal pure states $\{|\uparrow\rangle, |\downarrow\rangle\}$, while $\vec{a} = (\pm 1,0,0)$ represent $\{|+\rangle, |-\rangle\}$.

4.3 Reduced Density Matrix

A very common and important situation is a system S interacting with an environment $\mathcal{E}$. If S is not sufficiently isolated, the interaction generally entangles the joint state of $S \cup \mathcal{E}$. The subsystem S can then no longer be described by a pure state vector; instead one uses its *reduced density matrix*. To introduce this object we first define the *partial trace*.

Partial Trace

Consider the Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_\mathcal{E}$. Let $\{|a_1\rangle, \ldots, |a_N\rangle\}$ and $\{|b_1\rangle, \ldots, |b_M\rangle\}$ be orthonormal bases of $\mathcal{H}_S$ and $\mathcal{H}_\mathcal{E}$, respectively. Any state $|\psi\rangle \in \mathcal{H}_S \otimes \mathcal{H}_\mathcal{E}$ can be expanded as

$$|\psi\rangle = \sum_{i=1}^{N}\sum_{j=1}^{M} c_{ij}|a_i\rangle \otimes |b_j\rangle$$

and any operator $A \in \mathcal{B}(\mathcal{H}_S \otimes \mathcal{H}_\mathcal{E})$ can be written as

$$A = \sum_{i,j,k,l} A_{ij;kl}\left(|a_i\rangle \otimes |b_j\rangle\right)\left(\langle a_k| \otimes \langle b_l|\right) = \sum_{i,j,k,l} A_{ij;kl}\left(|a_i\rangle\langle a_k|\right) \otimes \left(|b_j\rangle\langle b_l|\right)$$

The state $|\psi\rangle$ has NM components c_{ij}, while A is an $NM \times NM$ matrix with entries $A_{ij;kl}$.

The *partial trace over the environment* $\mathcal{E}$ is defined by

$$\begin{aligned} \mathrm{Tr}_\mathcal{E}(A) &\equiv \sum_{i,j,k,l} A_{ij;kl}\,|a_i\rangle\langle a_k|\,\mathrm{Tr}_\mathcal{E}\left(|b_j\rangle\langle b_l|\right) \\ &= \sum_{i,j,k,l} A_{ij;kl}\,|a_i\rangle\langle a_k|\,\underbrace{\langle b_l|b_j\rangle}_{\delta_{jl}} \\ &= \sum_{i,k}\Big(\sum_j A_{ij;kj}\Big)|a_i\rangle\langle a_k| \end{aligned} \tag{4.5}$$

Thus $\mathrm{Tr}_\mathcal{E}(A)$ is an $N \times N$ matrix with entries $\sum_j A_{ij;kj}$ and acts on $\mathcal{H}_S$.

The partial trace over the system S is similarly defined by

$$\begin{aligned} \mathrm{Tr}_S(A) &\equiv \sum_{i,j,k,l} A_{ij;kl}\ \mathrm{Tr}_S\Big(|a_i\rangle\langle a_k|\Big)|b_j\rangle\langle b_l| \\ &= \sum_{i,j,k,l} A_{ij;kl}\ \underbrace{\langle a_i|a_k\rangle}_{\delta_{ik}}|b_j\rangle\langle b_l| \\ &= \sum_{j,l}\Big(\sum_i A_{ij;il}\Big)|b_j\rangle\langle b_l| \end{aligned} \tag{4.6}$$

Thus $\mathrm{Tr}_S(A)$ is an $M \times M$ matrix with entries $\sum_i A_{ij;il}$ and acts on $\mathcal{H}_\mathcal{E}$.

Example 4.3: Partial trace

Let $\mathcal{H}_S = \mathbb{C}^2$ and $\mathcal{H}_\mathcal{E} = \mathbb{C}^2$ be two one-qubit Hilbert spaces. The total system is described by $\mathcal{H}_S \otimes \mathcal{H}_\mathcal{E} = (\mathbb{C}^2)^{\otimes 2}$, with computational basis

$$\Big\{|0\rangle_S \otimes |0\rangle_\mathcal{E}, \quad |0\rangle_S \otimes |1\rangle_\mathcal{E}, \quad |1\rangle_S \otimes |0\rangle_\mathcal{E}, \quad |1\rangle_S \otimes |1\rangle_\mathcal{E}\Big\}$$

Consider the entangled pure state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle_S \otimes |0\rangle_\mathcal{E} + |1\rangle_S \otimes |1\rangle_\mathcal{E}\Big)$$

The associated density matrix is

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{\sqrt{2}}\Big\{|0\rangle\langle 0|_S \otimes |0\rangle\langle 0|_\mathcal{E} + |0\rangle\langle 1|_S \otimes |0\rangle\langle 1|_\mathcal{E} + |1\rangle\langle 0|_S \otimes |1\rangle\langle 0|_\mathcal{E} + |1\rangle\langle 1|_S \otimes |1\rangle\langle 1|_\mathcal{E}\Big\}$$

Applying the formulas above for the two partial traces gives

$$\mathrm{Tr}_S(\rho) = \frac{1}{2}|0\rangle\langle 0|_S + \frac{1}{2}|1\rangle\langle 1|_S$$
$$\mathrm{Tr}_\mathcal{E}(\rho) = \frac{1}{2}|0\rangle\langle 0|_\mathcal{E} + \frac{1}{2}|1\rangle\langle 1|_\mathcal{E}$$

In matrix notation, using the basis

$$|0\rangle \otimes |0\rangle \equiv \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |0\rangle \otimes |1\rangle \equiv \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad |1\rangle \otimes |0\rangle \equiv \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |1\rangle \otimes |1\rangle \equiv \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

we have

$$\rho = \frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} = \begin{pmatrix}A_{0000}&A_{0001}&A_{0010}&A_{0011}\\A_{0100}&A_{0101}&A_{0110}&A_{0111}\\A_{1000}&A_{1001}&A_{1010}&A_{1011}\\A_{1100}&A_{1101}&A_{1110}&A_{1111}\end{pmatrix}$$

and the partial traces are obtained through

$$\mathrm{Tr}_S(\rho) = \begin{pmatrix}A_{0000}+A_{1010}&A_{0001}+A_{1011}\\A_{0100}+A_{1110}&A_{0101}+A_{1111}\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$$
$$\mathrm{Tr}_\mathcal{E}(\rho) = \begin{pmatrix}A_{0000}+A_{0101}&A_{0010}+A_{0111}\\A_{1000}+A_{1101}&A_{1010}+A_{1111}\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

This example illustrates why Dirac notation is often more convenient than component notation.

Reduced Density Matrix and Its Physical Interpretation

The preceding example illustrates the notion of a reduced density matrix. If $\mathcal{H}_{\text{tot}} = \mathcal{H}_S \otimes \mathcal{H}_\mathcal{E}$ and the total state is pure, $|\psi\rangle \in \mathcal{H}_{\text{tot}}$, then the reduced density matrix of S is obtained by tracing over the environment:

$$\rho_S = \text{Tr}_\mathcal{E}(|\psi\rangle\langle\psi|)$$

Similarly, the reduced density matrix of the environment is obtained by tracing over the system:

$$\rho_\mathcal{E} = \text{Tr}_S(|\psi\rangle\langle\psi|)$$

What is the physical meaning of ρ_S? Suppose we measure an observable acting only on S, namely $A = A_S \otimes \mathbb{1}_\mathcal{E}$. The expectation value in repeated measurements on the joint state $|\psi\rangle$ is

$$\begin{aligned} \text{Av}_\psi(A) &= \langle\psi|A_S \otimes \mathbb{1}_\mathcal{E}|\psi\rangle = \text{Tr}_{\mathcal{H}_S\otimes\mathcal{H}_\mathcal{E}}\Big(A_S \otimes \mathbb{1}_\mathcal{E}|\psi\rangle\langle\psi|\Big) \\ &= \text{Tr}_{\mathcal{H}_S}\Big(A_S\Big\{\text{Tr}_{\mathcal{H}_\mathcal{E}}\Big(|\psi\rangle\langle\psi|\Big)\Big\}\Big) = \text{Tr}_{\mathcal{H}_S}\Big(A_S\rho_S\Big) \end{aligned} \tag{4.7}$$

Thus $\text{Av}_\psi(A) = \text{Tr}_{\mathcal{H}_S}(A_S\rho_S)$. All measurement statistics for observables acting only on S are therefore completely determined by the reduced density matrix ρ_S.

We can go further. Suppose $A_S = \sum_n \alpha_n P_n$, where $P_n = |n\rangle\langle n|$ are the eigenprojectors of A_S. The spectral decomposition of $A = A_S \otimes \mathbb{1}_\mathcal{E}$ is

$$A = A_S \otimes \mathbb{1}_\mathcal{E} = \sum_n \alpha_n\Big(P_n \otimes \mathbb{1}_\mathcal{E}\Big)$$

where $P_n \otimes \mathbb{1}_\mathcal{E}$ are the eigenprojectors of A. By the measurement postulate, if the pre-measurement state is $|\psi\rangle$, then outcome n occurs with probability $\mathbb{P}[n] = \langle\psi|(P_n \otimes \mathbb{1}_\mathcal{E})|\psi\rangle$, which can be written as

$$\begin{aligned} \mathbb{P}[n] &= \langle\psi|P_n \otimes \mathbb{1}_\mathcal{E}|n\rangle = \text{Tr}_{\mathcal{H}_S\otimes\mathcal{H}_\mathcal{E}}\Big(P_n \otimes \mathbb{1}_\mathcal{E}|\psi\rangle\langle\psi|\Big) \\ &= \text{Tr}_{\mathcal{H}_S}\Big(P_n\Big\{\text{Tr}_{\mathcal{H}_\mathcal{E}}(|\psi\rangle\langle\psi|\Big\}\Big) \\ &= \text{Tr}_{\mathcal{H}_S}\Big(P_n\,\rho_S\Big) \end{aligned}$$

The total post-measurement density matrix on $\mathcal{H}_S \otimes \mathcal{H}_\mathcal{E}$ is proportional to

$$\rho_{\text{after}} \propto P_n \otimes \mathbb{1}_\mathcal{E}(|\psi\rangle\langle\psi|)P_n \otimes \mathbb{1}_\mathcal{E}$$

and the corresponding reduced density matrix is proportional to

$$\begin{aligned} \rho_{S,\text{after}} &\propto \text{Tr}_\mathcal{E}\Big(\rho_{\text{after}}\Big) = \text{Tr}_\mathcal{E}\Big(P_n \otimes \mathbb{1}_\mathcal{E}(|\psi\rangle\langle\psi|)P_n \otimes \mathbb{1}_\mathcal{E}\Big) \\ &= P_n\Big(\text{Tr}_\mathcal{E}(|\psi\rangle\langle\psi|)\Big)P_n \\ &= P_n\,\rho_S\,P_n \end{aligned}$$

Normalizing this expression gives

$$\rho_{S,\text{after}} = \frac{P_n \rho_S P_n}{\mathrm{Tr}\big(P_n \rho_S P_n\big)}$$

Example 4.4: Reduced density matrix of a pure state

Consider a bipartite pure state. If it is a product state, each reduced density matrix is pure. If the total pure state is entangled, the reduced states are generally mixed. We illustrate this distinction with an explicit maximally entangled example.

Consider again two qubits, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^2 \otimes \mathbb{C}^2$. For a product state $|\varphi_1\rangle \otimes |\varphi_2\rangle$,

$$\rho = \big(|\varphi_1\rangle \otimes |\varphi_2\rangle\big)\big(\langle\varphi_1| \otimes \langle\varphi_2|\big) = |\varphi_1\rangle\langle\varphi_1| \otimes |\varphi_2\rangle\langle\varphi_2|$$

and the reduced density matrices obtained by partial trace are

$$\rho_1 = |\varphi_1\rangle\langle\varphi_1| \quad \text{and} \quad \rho_2 = |\varphi_2\rangle\langle\varphi_2|$$

Thus each qubit is itself in a pure state, as is already clear from the product structure.

Now consider an entangled state, for example $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. The reduced density matrices are

$$\rho_1 = \frac{1}{2}\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big) = \frac{1}{2}\mathbb{1} \quad \text{and} \quad \rho_2 = \frac{1}{2}\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big) = \frac{1}{2}\mathbb{1}$$

Both are maximally mixed states, corresponding to the center $\vec{a} = (0, 0, 0)$ of the Bloch ball. The density matrix $\frac{1}{2}\mathbb{1}$ can be represented as an equal mixture of any two orthonormal states $\{|e_1\rangle, |e_2\rangle\}$. In other words, each subsystem separately is completely random and carries no information about the global pure state.

4.4 Schmidt Decomposition and Purification

We now introduce two mathematical tools that are particularly useful in quantum information.

Schmidt Decomposition

For a bipartite pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, the reduced density matrices $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$ and $\rho_B = \mathrm{Tr}_A(|\psi\rangle\langle\psi|)$ have remarkable related properties.

Theorem

Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a pure state. Then ρ_A and ρ_B have the same nonzero eigenvalues, with the same multiplicities. Consequently, the reduced density matrices admit spectral decompositions

$$\rho_A = \sum_i \lambda_i |\varphi_i\rangle_A \langle\varphi_i|_A \quad \text{and} \quad \rho_B = \sum_i \lambda_i |\chi_i\rangle_B \langle\chi_i|_B$$

with the same positive eigenvalues λ_i satisfying $\sum_i \lambda_i = 1$. Zero eigenvalues may occur with different multiplicities in ρ_A and ρ_B. The vectors $|\varphi_i\rangle_A$ and $|\chi_i\rangle_B$ form orthonormal sets in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and satisfy $\rho_A|\varphi_i\rangle_A = \lambda_i|\varphi_i\rangle_A$ and $\rho_B|\chi_i\rangle_B = \lambda_i|\chi_i\rangle_B$.

Moreover, the pure state can be written as

$$|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |\varphi_i\rangle_A \otimes |\chi_i\rangle_B$$

This representation is called the *Schmidt decomposition*.

Remark. If the nonzero eigenvalues λ_i are nondegenerate, the corresponding eigenvectors $|\varphi_i\rangle_A$ and $|\chi_i\rangle_B$ are unique up to phase. In degenerate eigenspaces they are not unique, because arbitrary unitary rotations may be performed within the eigenspace. These vectors form complete bases only after adding eigenvectors associated with zero eigenvalues of ρ_A and ρ_B.

Proof of the theorem

Let $\{|n\rangle_A\}$ and $\{|n\prime\rangle_B\}$ be orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$. Expand the pure state as

$$|\psi\rangle = \sum_{n,\, n'} a_{nn'} |n\rangle_A \otimes |n'\rangle_B$$

For each n, define $|\tilde{n}\rangle_B = \sum_{n\prime} a_{nn\prime} |n\prime\rangle_B$, so that

$$|\psi\rangle = \sum_n |n\rangle_A \otimes |\tilde{n}\rangle_B$$

Note that the vectors $\{|\tilde{n}\rangle_B\}$ need not be orthonormal. The reduced density matrix of A is

$$\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \sum_{n_1,\, n_2} \langle\tilde{n}_2|\tilde{n}_1\rangle_B \; |n_1\rangle_A\langle n_2|_A$$

Choose $\{|n\rangle_A\}$ to be the eigenbasis $\{|\varphi_i\rangle_A\}$ of ρ_A, with $\rho_A|\varphi_i\rangle_A = \lambda_i|\varphi_i\rangle_A$. Then

$$\rho_A = \sum_{i_1,i_2} \langle\tilde{\varphi}_{i_2}|\tilde{\varphi}_{i_1}\rangle_B \, |\varphi_{i_1}\rangle_A\langle\varphi_{i_2}|_A = \sum_{i_1} \lambda_{i_1} |\varphi_{i_1}\rangle_A\langle\varphi_{i_2}|_A$$

where the second equality is the spectral decomposition. Therefore, for every nonzero eigenvalue λ_{i_1},

$$\langle\tilde{\varphi}_{i_2}|\tilde{\varphi}_{i_1}\rangle_B = \lambda_{i_1}\delta_{i_1 i_2}$$

and the states $|\tilde{\varphi}_i\rangle_B$ are mutually orthogonal. Defining the normalized vectors $|\chi_i\rangle_B = \lambda_i^{-1/2}|\tilde{\varphi}_i\rangle_B$, we obtain

$$|\psi\rangle = \sum_i |\varphi_i\rangle_A \otimes |\tilde{\varphi}_i\rangle_B = \sum_i \lambda_i^{-\frac{1}{2}} |\varphi_i\rangle_A \otimes |\chi_i\rangle_B$$

which is the Schmidt decomposition. Taking the partial traces also gives

$$\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \sum_i \lambda_i |\varphi_i\rangle_A\langle\varphi_i|_A$$

$$\rho_B = \mathrm{Tr}_A(|\psi\rangle\langle\psi|) = \sum_i \lambda_i |\chi_i\rangle_B\langle\chi_i|_B$$

Definition. The *Schmidt rank* of a pure state $|\psi\rangle$ is the number of nonzero Schmidt coefficients λ_i.

For a product state $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$, the Schmidt rank is one. If the Schmidt rank is at least two, the state is entangled. The Schmidt rank is therefore our first quantitative measure of bipartite entanglement.

The Schmidt rank is invariant under local unitary transformations $U = U_A \otimes U_B$.

Indeed,

$$U|\psi\rangle = \sum_i \sqrt{\lambda_i} U_A|\varphi_i\rangle_A \otimes U_B|\chi_i\rangle_B$$

and the sets $\{U_A|\varphi_i\rangle_A\}$ and $\{U_B|\chi_i\rangle_B\}$ remain orthonormal. Hence the Schmidt rank can change only through an interaction between A and B, for which the evolution is not of the form $U_A \otimes U_B$.

Purification of a Density Matrix

We have seen that if the total system $S \cup \mathcal{E}$ is in a pure state $|\psi\rangle \in \mathcal{H}_S \otimes \mathcal{H}_\mathcal{E}$, then the reduced state of S is described by the density matrix

$$\rho_S = \mathrm{Tr}_{H_\mathcal{E}}(|\psi\rangle\langle\psi|)$$

Conversely, given any density matrix ρ_S, one can enlarge the Hilbert space to $\mathcal{H}_S \otimes \mathcal{H}_\mathcal{E}$ and construct a pure state $|\psi\rangle$ such that $\rho_S = \mathrm{Tr}_\mathcal{E}(|\psi\rangle\langle\psi|)$. This construction, called a purification, is not unique and need not correspond to the actual physical preparation of S.

An explicit construction follows directly from the spectral decomposition. Write

$$\rho_S = \sum_i \lambda_i |\varphi_i\rangle_S \langle\varphi_i|_S$$

and choose the environment to contain an isomorphic copy of $\mathcal{H}_S$. For each $|\varphi_i\rangle_S$, let $|\varphi_i\rangle_\mathcal{E}$ denote the corresponding vector in the environmental copy, and define

$$|\psi\rangle = \sum_i \sqrt{\lambda_i} |\varphi_i\rangle_S \otimes |\varphi_i\rangle_\mathcal{E}$$

4.5 Density Matrix for Two Qubits

We have seen how to represent the density matrix of a single qubit in Section **4.2**. A similar representation exists for two qubits. Since $\{\mathbb{1}, X, Y, Z\}$ is a basis of the real vector space of 2×2 Hermitian matrices, tensor products of two such basis elements form a basis of the real vector space of 4×4 Hermitian matrices. Therefore every two-qubit density matrix can be written as

$$\rho = \frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} + \vec{a} \cdot \vec{\Sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \vec{b} \cdot \vec{\Sigma} + \sum_{n,m=1}^{3} t_{nm}\, \sigma_n \otimes \sigma_m\right) \tag{4.8}$$

where $\vec{\Sigma} = (\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$, $\vec{a}, \vec{b} \in \mathbb{R}^3$, and (t_{nm}) is a real 3×3 matrix.

The conditions $\rho = \rho^\dagger$ and $\mathrm{Tr}\,\rho = 1$ are automatically satisfied because the Pauli matrices are Hermitian and traceless. Thus a two-qubit state is described by 15 real parameters, subject to the additional positivity constraint $\rho \geq 0$. This positivity condition

is not as simple to express analytically as in the one-qubit case. The set of two-qubit density matrices is nevertheless a bounded convex subset of $\mathbb{R}^{15}$, with a much richer geometry than the Bloch ball.

It is also useful to note that

$$\mathrm{Tr}_B\,\rho = \frac{1}{2}\left(\mathbb{1} + \vec{a}\cdot\vec{\Sigma}\right) \quad \text{and} \quad \mathrm{Tr}_A\,\rho = \frac{1}{2}\left(\mathbb{1} + \vec{b}\cdot\vec{\Sigma}\right)$$

The special case $\vec{a} = \vec{b} = \vec{0}$ corresponds to states whose one-qubit reduced density matrices are maximally mixed. This subset has a particularly useful geometric representation.

Remark. Although the entries of ρ can be complex because Y is imaginary, Hermiticity implies that the coefficients $\vec{a}$, $\vec{b}$, and t_{nm} are real. The representation generalizes immediately to n qubits:

$$\rho = \frac{1}{2^n}\sum_{\substack{(i_1,i_2,\ldots,i_n)\\ \in(0,1,2,3)^n}} t_{i_1 i_2 \ldots i_n}\,\sigma_{i_1}\otimes\sigma_{i_2}\otimes\ldots\otimes\sigma_{i_n} \tag{4.9}$$

where $(\sigma_0,\sigma_1,\sigma_2,\sigma_3) = (\mathbb{1}, X, Y, Z)$ and $t_{i_1\ldots i_n} \in \mathbb{R}$. The unit-trace condition imposes $t_{00\ldots0} = 1$, leaving $4^n - 1$ real parameters. Positivity restricts these parameters to a bounded convex subset of $\mathbb{R}^{4^n-1}$.

Separable and Entangled States

For mixed states, the distinction between product and entangled states is subtler than for pure states. One might first define a product state as $\rho = \rho_A \otimes \rho_B$, but a statistical source can emit different product states $\rho_A^i \otimes \rho_B^i$ with probabilities p_i. The resulting mixed state is the convex combination

$$\rho = \sum_i p_i\,\rho_A^i \otimes \rho_B^i \tag{4.10}$$

with $0 \le p_i \le 1$ and $\sum_i p_i = 1$. States of the form (4.10) need not factorize as $\rho_A \otimes \rho_B$, even though every term in the sum is a product state. This distinction is important for mixed states. States of the form (4.10) are therefore called *separable*.

Definition: States separable and entangled

A state is called separable if it can be written in the form (4.10). If a state cannot be written in the form (4.10), it is called entangled.

This definition applies to any bipartite system and, in particular, to two-qubit density matrices. In that case $\rho_A^i = \frac{1}{2}(\mathbb{1} + \vec{a}^i\cdot\vec{\Sigma})$ and $\rho_B^i = \frac{1}{2}(\mathbb{1} + \vec{b}^i\cdot\vec{\Sigma})$. Comparing (4.8) with (4.10) gives $\vec{a} = \sum_i p_i\vec{a}^i$, $\vec{b} = \sum_i p_i\vec{b}^i$, and $t_{nm} = \sum_i p_i a_n^i b_m^i$. In particular, it is possible to have $\vec{a} = \vec{b} = \vec{0}$ while $t_{nm} \neq 0$.

Given a density matrix ρ, deciding whether it is separable or entangled is generally nontrivial. For two qubits, however, a criterion due to Peres and the Horodeckis gives a necessary and sufficient condition that is easy to check: the *positive partial transpose* (PPT) criterion. Let ρ^{T_B} denote the partial transpose with respect to subsystem B. If ρ is separable, then

$$\rho^{T_B} = \sum_i p_i \, \rho_A^i \otimes {\rho_B^i}^T$$

where ${\rho_B^i}^T$ is the transpose of ρ_B^i. Since transposition preserves the eigenvalues of a Hermitian matrix, ${\rho_B^i}^T \geq 0$ whenever $\rho_B^i \geq 0$. Hence a separable state must satisfy $\rho^{T_B} \geq 0$. Consequently, if ρ^{T_B} has at least one negative eigenvalue, then ρ is necessarily entangled.

Peres–Horodecki criterion

Let ρ be a density matrix of a general bipartite system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. If the partial transpose ρ^{T_B} has a negative eigenvalue, then ρ is entangled. In particular, it cannot be written in the separable form (4.10).

The PPT condition is necessary in every dimension but is not sufficient in general. Remarkably, it is both necessary and sufficient for $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$. Thus, for two-qubit density matrices, the Peres–Horodecki criterion completely characterizes separability.

Bell-Diagonal States and Their Geometry

The subset of density matrices in (4.8) with $\vec{a} = \vec{b} = \vec{0}$ has a particularly simple geometry. These states have maximally mixed one-qubit reduced density matrices and include the Bell states.

Let ρ belong to this set. One can always find a local unitary transformation $U_A \otimes U_B$ such that $(U_A \otimes U_B)\rho(U_A^\dagger \otimes U_B^\dagger)$ has the form[4]

$$\tilde{\rho} = \frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} t_i \, \sigma_i \otimes \sigma_i\right)$$

with $(t_1, t_2, t_3) \in \mathbb{R}^3$. These density matrices therefore form a convex subset of $\mathbb{R}^3$. To determine the allowed region, we impose the positivity condition $\rho \geq 0$.

The Bell states are eigenvectors of $\tilde{\rho}$, with eigenvalues p_{ij}:

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad \text{with} \quad p_{00} = \frac{1 + t_1 - t_2 + t_3}{4}$$
$$|B_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad \text{with} \quad p_{01} = \frac{1 + t_1 + t_2 - t_3}{4}$$

[4] The purpose of this transformation is to diagonalize the 3×3 correlation matrix so that the state is described by only three real parameters (t_1, t_2, t_3) rather than nine correlated coefficients t_{nm}. Finding the required local unitaries need not be trivial.

$$|B_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad \text{with} \quad p_{10} = \frac{1 - t_1 + t_2 + t_3}{4}$$
$$|B_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad \text{with} \quad p_{11} = \frac{1 - t_1 - t_2 - t_3}{4}$$

We may therefore express $\tilde{\rho}$ in the Bell basis as

$$\tilde{\rho} = \sum_{i,j=0}^{1} p_{ij} |B_{ij}\rangle\langle B_{ij}|$$

In this orthonormal basis the density matrix is diagonal, with eigenvalues p_{ij}. The original matrix ρ is diagonal with the same eigenvalues in the orthonormal entangled basis $(U_A \otimes U_B)|B_{ij}\rangle$. Since $\sum_{i,j} p_{ij} = 1$, the allowed convex region in (t_1, t_2, t_3) is obtained by imposing $p_{ij} \geq 0$. Using the expressions above gives

$$t_1 - t_2 + t_3 \geq -1$$
$$t_1 + t_2 - t_3 \geq -1$$
$$t_1 - t_2 - t_3 \leq 1$$
$$t_1 + t_2 + t_3 \leq 1$$

These four inequalities define a tetrahedron bounded by four planes, shown in Figure 4.1.

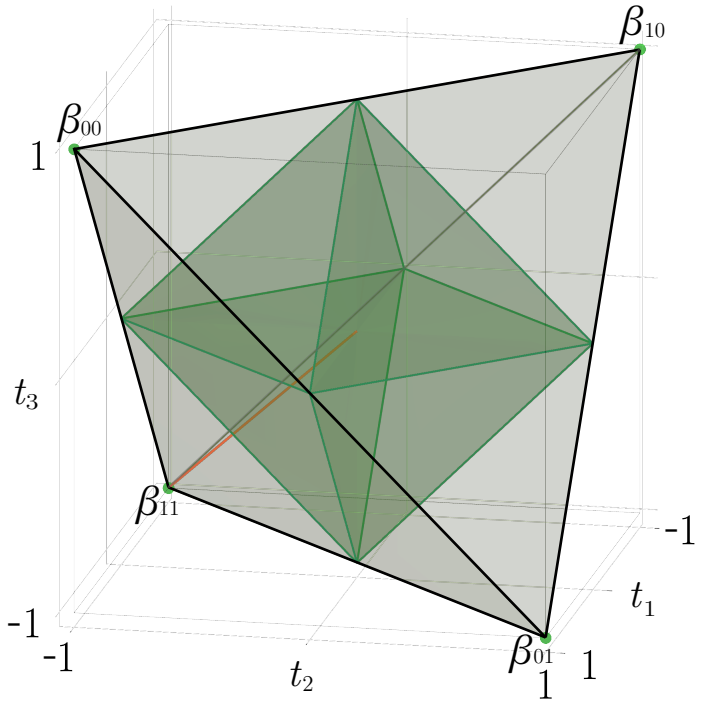


Figure 4.1 Geometric representation of Bell-diagonal states (BDS) as a tetrahedron. The inner octahedron is the subset of separable BDS. The red line represents the Werner states.

The allowed region is a tetrahedron, as expected for a convex set. Every point in the tetrahedron represents a Bell-diagonal state (BDS). The four vertices are the four pure Bell states $|B_{ij}\rangle$; points on edges are mixtures of two Bell states, points on faces are mixtures of three, and interior points are mixtures of all four.

The tetrahedron contains both separable and entangled states. Intuitively, separable states lie near the origin, whereas strongly entangled states lie near the Bell-state vertices. The Peres criterion identifies the boundary exactly. The partial transpose of a BDS is

$$\begin{aligned}\rho^{T_B} &= \frac{1}{4}\left(\mathbb{1}\otimes\mathbb{1}^T + t_1\,\sigma_1\otimes\sigma_1^T + t_2\,\sigma_2\otimes\sigma_2^T + t_3\,\sigma_3\otimes\sigma_3^T\right)\\ &= \frac{1}{4}\left(\mathbb{1}\otimes\mathbb{1} + t_1\,\sigma_1\otimes\sigma_1 - t_2\,\sigma_2\otimes\sigma_2 + t_3\,\sigma_3\otimes\sigma_3\right)\end{aligned}$$

If (t_1, t_2, t_3) lies in the original tetrahedron, then partial transposition sends it to $(t_1, -t_2, t_3)$, corresponding geometrically to reflection through the (t_1, t_3) plane. A state is PPT precisely when both the original point and its reflected point lie inside the tetrahedron. Their intersection is the octahedron shown in Figure **4.1**:

$$\text{SEP} = \left\{(t_1, t_2, t_3) \mid |t_1| + |t_2| + |t_3| \le 1\right\}$$

The complement of this octahedron inside the tetrahedron consists of four disjoint pyramidal regions, each containing one Bell-state vertex; these are the entangled Bell-diagonal states.

Finally, the one-parameter family $w = -t_1 = -t_2 = -t_3$, known as the *Werner states*, is especially useful because of its simple form. These states are convex mixtures of the maximally mixed state and the Bell state $|B_{11}\rangle$:

$$\tilde{\rho} = \frac{1-w}{4}\mathbb{1}\otimes\mathbb{1} + w\,|B_{11}\rangle\langle B_{11}|$$

It is straightforward to compute $\tilde{\rho}^{T_B}$. The Peres criterion shows that the states are separable for $0 \le w \le \frac{1}{3}$ and entangled for $\frac{1}{3} < w \le 1$. The point $w = \frac{1}{3}$ lies on a face of the separable octahedron.

Part II

Quantum Information and Computation

5 Quantum Cryptography

One of the earliest applications of quantum mechanics to quantum information is the protocol introduced by Bennett and Brassard in 1984 for distributing a secret key between two distant parties, traditionally called Alice and Bob. Since then many related protocols have been developed, giving rise to the field of quantum cryptography. Strictly speaking, the protocol discussed here is a method for *quantum key distribution* (QKD): it establishes a shared secret key that can subsequently be used with a classical cryptographic scheme.

The central idea of BB84 is simple. Alice encodes classical information in nonorthogonal quantum states and sends the corresponding qubits to Bob. Any eavesdropper, Eve, who attempts to extract information must interact with or measure these qubits. Because measurement generally disturbs a quantum state, Eve's intervention produces detectable errors. By publicly comparing a suitable subset of their data, Alice and Bob can estimate the disturbance and decide whether the key should be accepted or discarded.

A complete security analysis is considerably more subtle than the simplified treatment given here. Real communication channels are noisy, practical sources and detectors are imperfect, and one must distinguish ordinary experimental errors from those caused by an eavesdropper. Nevertheless, rigorous security proofs exist, and quantum key distribution has also become an experimental technology. Implementations over optical fibers and free-space links have been demonstrated over substantial distances. In this chapter we focus on the physical ideas behind BB84 and on simple eavesdropping strategies.

5.1 Key Generation with BB84

The protocol has four essential stages: Aliceś encoding procedure, Bobś decoding procedure, public communication between the two parties, and finally the generation of a shared secret key. The general setup is shown in Figure **5.1**.

Aliceś encoding procedure. Alice generates a random binary sequence $x_1, ..., x_N$, $x_i \in \{0, 1\}$, which she keeps secret. The shared key will ultimately be formed from a subset of these bits. She also generates a second random binary sequence $e_1, ..., e_N$, $e_i \in \{0, 1\}$, which she initially keeps secret. Alice encodes the classical bit x_i into a qubit as follows:

- If $e_i = 0$, she prepares a qubit in the state $|x_i\rangle$. Concretely, the photon is prepared

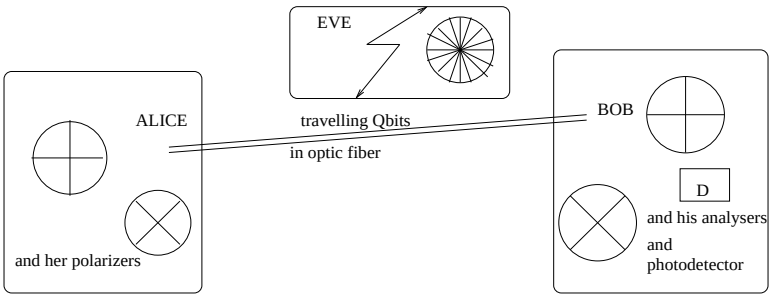


Figure 5.1 Alice and Bob generate a secret key over an optical-fiber channel.

with a polarizer in the basis Z (Figure **5.2**).

$$\Big\{|0\rangle, |1\rangle\Big\}$$

For $x_i = 0$ (respectively $x_i = 1$), the polarizer is oriented horizontally (respectively vertically), so the photon is prepared in polarization state $|0\rangle$ (respectively $|1\rangle$). Ideally, a single photon is then selected from the output beam.

Figure 5.2 Polarizer orientations used to prepare photons in the Z basis.

- If $e_i = 1$, Alice prepares the qubit in the state $H|x_i\rangle$[1]. Experimentally, this can be achieved by sending photons through a polarizer aligned with the X basis (Figure **5.3**)

$$\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$$

  which prepares the photon in polarization state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ (respectively $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$).

Figure 5.3 Polarizer orientations used to prepare photons in the X basis.

[1] Here H is the Hadamard matrix $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$.

In summary, Alice sends the sequence of qubits $|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$, $i = 1, ..., N$, through a quantum channel (in practice, for example, an optical fiber).

Bobś decoding procedure. Bob generates an independent random binary sequence $d_1, ..., d_N$, $d_i \in \{0, 1\}$, which he initially keeps secret. He measures the qubits received from Alice as follows:

- If $d_i = 0$, he measures the received qubit $|A_{e_i,x_i}\rangle$ in the Z basis

$$\Big\{|0\rangle, |1\rangle\Big\}.$$

After the measurement, the photon is projected onto a state

$$|y_i\rangle \in \Big\{|0\rangle, |1\rangle\Big\}.$$

Bob records the corresponding classical bit y_i. Experimentally, he may use the analyzer–detector apparatus described in Chapter **2**. The analyzer is oriented horizontally. If the detector clicks, the photon is projected onto $|0\rangle$; if the detector does not click, the photon is projected onto $|1\rangle$. According to the measurement postulate, these outcomes are intrinsically random when the incoming state is not a Z-basis eigenstate. Only Bob knows the recorded result.

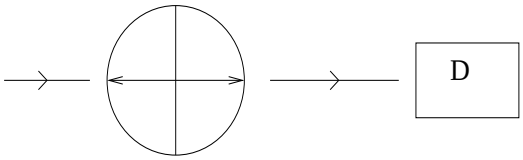


Figure 5.4 Analyzer–detector apparatus for measuring polarization in the Z basis.

- If $d_i = 1$, Bob measures the received qubit $|A_{e_i,x_i}\rangle$ in the X basis

$$\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}.$$

After the measurement, the photon state belongs to belongs to

$$H|y_i\rangle \in \left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$$

For a post-measurement state $H|y_i\rangle$, Bob records the classical bit y_i.

Experimentally, Bob again uses the analyzer–detector apparatus described in Chapter **2**, now with the analyzer rotated by 45° (Figure **5.5**). If the detector clicks, the photon is projected onto $H|0\rangle$; if it does not click, the photon is projected onto $H|1\rangle$. Again, the measurement outcome is intrinsically random unless the incoming photon is already an X-basis eigenstate. Only Bob knows the recorded result.

In summary, Bob has converted the qubits sent by Alice into a classical binary sequence $y_1, ..., y_N$. This sequence consists of his measurement outcomes and cannot in general be predicted in advance. is the result of the measurements of Bob and not can be predicted.

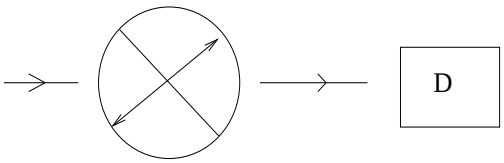


Figure 5.5 Analyzer–detector apparatus for measuring polarization in the X basis.

Public communication. Alice holds two binary sequences: two sequences binary: $e_1, ..., e_N$, which specify the encoding basis, and $x_1, ..., x_N$, which specify the encoded bit values. Bob likewise holds $d_1, ..., d_N$, which specify his measurement bases, and $y_1, ..., y_N$, which are his measurement outcomes.

Alice and Bob publicly reveal the basis choices $e_1, ..., e_N$ and $d_1, ..., d_N$ over an authenticated classical channel, while keeping the data sequences $x_1, ..., x_N$ and $y_1, ..., y_N$ secret. *Crucially, this public discussion begins only after Bob has completed all measurements.* From the announced basis choices, Alice and Bob—and indeed anyone listening to the public channel—can infer the following:

- If $d_i = e_i$, so that Alice and Bob used the same basis, then ideally $y_i = x_i$ with certainty. This follows directly from the fact that Bob measures a basis state in the same basis in which it was prepared. In this case no genuinely quantum ambiguity is introduced by the measurement.
- If $d_i \neq e_i$, the qubit is measured in a basis different from the preparation basis, and the measurement outcome is genuinely random. By the measurement postulate, $y_i \neq x_i$ with probability $\frac{1}{2}$ and $y_i = x_i$ with probability $\frac{1}{2}$. To see this, Bob receives the qubit

  $$|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$$

  and measures it in the basis

  $$\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}.$$

  The outcome is one of the two basis vectors:

  $$H^{d_i}|0\rangle, \qquad \text{with probability } |\langle 0|H^{d_i}H^{e_i}|x_i\rangle|^2$$

  or

  $$H^{d_i}|1\rangle, \qquad \text{with probability } |\langle 1|H^{d_i}H^{e_i}|x_i\rangle|^2.$$

  If $e_i \neq d_i$, both probabilities are $\frac{1}{2}$; if $e_i = d_i$, one probability is 1 and the other is 0. (and if $e_i = d_i$ they valent 0 or 1).

Generation of the shared key. Alice and Bob discard all positions i for which $e_i \neq d_i$. They retain the remaining bits, for which $e_i = d_i$. In the ideal protocol these retained subsequences satisfy $x_i = y_i$, and can therefore be used to construct a shared secret key. Since the basis choices are independent and random, the retained subsequence has expected length approximately $\frac{N}{2}$, because $\mathbb{P}[e_i \neq d_i] = \frac{1}{2}$. Finally, Alice and Bob

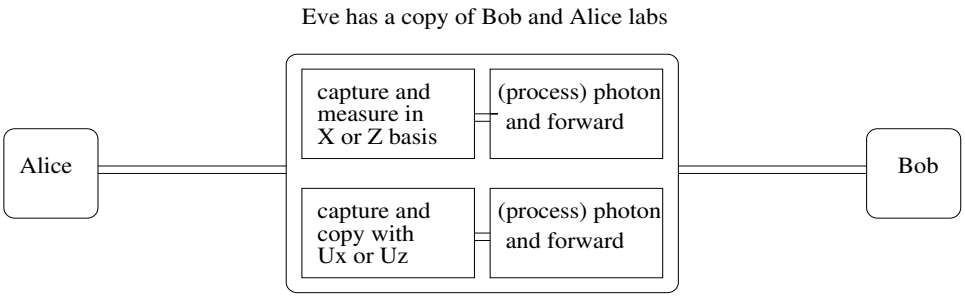


Figure 5.6 Eveś interception apparatus placed along the optical-fiber channel.

perform a security test. In the absence of noise and eavesdropping, quantum mechanics predicts [2]

$$\mathbb{P}\left[x_i = y_i | e_i = d_i\right] = 1$$

Alice and Bob test this condition by publicly comparing a small fraction, say $\epsilon\frac{N}{2}$, of their retained bits. If the observed error rate is acceptable, they discard the test bits and keep the remainder as a shared secret key of length approximately $(1-\epsilon)\frac{N}{2}$.

5.2 Eveś Attacks – Simplified Discussion

We assume ideal single-photon sources, perfect state preparation, no channel noise, and perfect measurement apparatuses for Bob. Under these ideal conditions, when Eve is absent the security criterion are parfaits. In these conditions, when Eve is absente, the criterion of security absolue $\mathbb{P}\left[x_i = y_i | e_i = d_i\right] = 1$ is satisfied.

We further assume that Eve attacks one qubit at a time, acting only on photons intercepted along the optical fiber, and that she has no access to Aliceś or Bobś laboratories. She is nevertheless assumed to know perfectly the definitions of the X and Z bases used by Alice and Bob, though not their random basis choices on any particular transmission. X and Z of the polariseurs and analyzers of Alice and Bob (but not of the choice random successifs).

We consider two simple attacks: an intercept–measure–resend attack and an attack based on unitary operations. Both involve two stages. First, Eve intercepts a photon and either measures it or applies a unitary operation; she then forwards a photon to Bob (Figure **5.6**). We shall see that the basic postulates of quantum mechanics imply that either strategy produces detectable errors. When Alice and Bob observe such a violation, they infer the presence of an eavesdropper and abort the protocol.

Intercept–measure–resend attack. Suppose Eve intercepts a photon in the optical fiber. Its state is one of

$$|A_{e_i,x_i}\rangle \in \{|0\rangle, |1\rangle, H|0\rangle, H|1\rangle\}$$

[2] Here we assume an ideal noiseless implementation and no eavesdropper.

Eve performs a measurement. If she uses the Z basis, the outcome belongs to $\{|0\rangle, |1\rangle\}$ and she records a bit $y_i^E \in \{0, 1\}$. If she uses the X basis, the outcome belongs to $\{H|0\rangle, H|1\rangle\}$ and she again records the corresponding bit y_i^E. After the measurement, she sends the photon on to Bob in the post-measurement state[3]. Two cases arise:

- Eve used the same basis as Alice. Then $y_i^E = x_i$, and Bob receives the photon in the correct state.
- Eve used a basis different from Aliceś. Then her outcome agrees with x_i only half the time, and the state she forwards to Bob is compatible with Aliceś preparation only probabilistically.

We now determine what Alice and Bob observe in their security test. Let EA denote the event "Eve uses the same basis as Alice".

$$\begin{aligned}\mathbb{P}\left[x_i = y_i | e_i = d_i\right] &= \mathbb{P}\left[x_i = y_i | e_i = d_i, EA\right]\mathbb{P}\left[EA\right] \\ &\quad + \mathbb{P}\left[x_i = y_i | e_i = d_i, \text{not } EA\right]\mathbb{P}\left[\text{not } EA\right] \\ &= 1 \cdot \mathbb{P}\left[EA\right] + \frac{1}{2} \cdot (1 - \mathbb{P}\left[EA\right]) \\ &= \frac{1}{2}(1 + \mathbb{P}\left[EA\right])\end{aligned}$$

where we have used

$$\mathbb{P}\left[x_i = y_i | e_i = d_i, EA\right] = 1, \qquad \mathbb{P}\left[x_i = y_i | e_i = d_i, \text{not EA}\right] = \frac{1}{2} \tag{5.1}$$

Assuming Eve has no information about Aliceś random basis choice, $\mathbb{P}\left[EA\right] = \frac{1}{2}$. Hence

$$\mathbb{P}\left[x_i = y_i | e_i = d_i\right] = \frac{3}{4}.$$

Alice and Bob therefore observe an error rate of $\frac{1}{4}$ even among positions where they used the same basis. Such an excess error rate reveals the presence of an eavesdropper.

Unitary attack. In the previous attack, Eve gains no advance knowledge of Aliceś basis choice. One might imagine that she could instead copy the qubit $|A_{e_i,x_i}\rangle$ while leaving the original photon undisturbed and forwarding it to Bob. Eve could then keep the copy until after the public basis announcement and measure it in the correct basis. If this were possible, she would obtain the same retained-key bit as Bob whenever $e_i = d_i$. She would then share Alice and Bobś secret key without introducing errors.

The flaw in this reasoning is the *no-cloning theorem* (Section **3.4**), a consequence of unitary quantum evolution. It guarantees that there is no universal unitary machine satisfying

$$U(|A_{e_i,x_i}\rangle \otimes |\text{blank}\rangle) = |A_{e_i,x_i}\rangle \otimes |A_{e_i,x_i}\rangle$$

The crucial point is that $|A_{e_i,x_i}\rangle$ belongs to the set

$$\left\{|0\rangle,\ |1\rangle,\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$$

[3] She could instead prepare another photon in the same state, but this does not improve the attack.

which contains nonorthogonal states.

Eve could try to use two separate copying machines, one designed for the two Z-basis states and one for the two X-basis states. But she does not know which machine to apply to a given intercepted photon. She therefore chooses the wrong machine half the time. An analysis analogous to the previous one again gives

$$\mathbb{P}\left[x_i = y_i | e_i = d_i\right] = \frac{3}{4}.$$

The security criterion is violated: one quarter of the retained bits are corrupted.

5.3 Bennett's 1992 Protocol

In BB84, Alice prepares photons in four possible states. The essential property is not the number four, but the use of nonorthogonal states. In 1992, Bennett proposed a protocol using only two nonorthogonal states, $|0\rangle$ and $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. A detailed analysis of this protocol and its security is left as an exercise.

6 Quantum Entanglement

In this chapter we study the correlations present in entangled quantum states. These correlations are intrinsically quantum: they have no classical counterpart and, in general, cannot be described by an ordinary classical probability distribution. We use the term *entanglement* for this special form of correlation in composite quantum systems.

We begin with the canonical two-qubit examples, the Bell states (Section **6.1**). We then discuss Bell inequalities—more precisely the Clauser–Horne–Shimony–Holt (CHSH) form—which provide experimentally testable constraints on local hidden-variable theories. Experiments beginning with those of Aspect and collaborators, and many increasingly stringent tests since then, agree with the predictions of quantum mechanics and violate the corresponding Bell inequalities.

Entanglement is also a central resource in quantum information processing and quantum communication. We shall illustrate this role with two fundamental protocols: quantum teleportation (Section **6.3**) and superdense coding (Section **6.4**).

6.1 Bell States

The Bell states are the canonical examples of two-qubit entangled states. They form an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$, a four-dimensional Hilbert space. The four Bell states are

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = U|00\rangle$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) = U|01\rangle$$

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) = U|10\rangle$$

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) = U|11\rangle$$

Here U is a 4×4 unitary matrix that maps the computational basis to the Bell basis. In these states the two qubits are strongly correlated. For example, in $|B_{00}\rangle$ the two polarization or spin degrees of freedom are aligned. It would nevertheless be incorrect

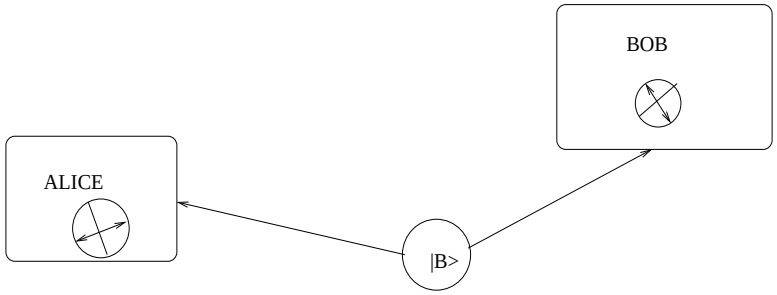


Figure 6.1 Alice and Bob share an entangled pair.

to say that the pair simply has a definite "up–up or "down–down direction, because one can verify that

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle\Big) \tag{6.1}$$

where $|\gamma\rangle = \cos\gamma|0\rangle + \sin\gamma|1\rangle$. Thus neither subsystem has a definite direction by itself; what is definite is the correlation between the two directions.

A pair of photons or spin-$\frac{1}{2}$ particles can be prepared in a Bell state by bringing the two systems into interaction. If the interaction is chosen appropriately, entanglement is generated. The two particles may then be spatially separated. Provided decoherence from the environment remains negligible, the polarization or spin correlations are preserved.

As we shall see, these correlations have no classical analogue. The term *entanglement* refers precisely to this special type of quantum correlation. Bell pairs are also often called EPR pairs, after Einstein, Podolsky, and Rosen, while Schrödinger was among the first to emphasize the apparently paradoxical properties of such states.

To develop some intuition, we now examine several possible measurement scenarios. Suppose a source produces EPR photon pairs, with Alice receiving one photon and Bob the other (Figure **6.1**). Regardless of the distance between the laboratories, the two-photon polarization state remains entangled in $|B_{00}\rangle$ as long as environmental disturbances are negligible. We consider several simple measurements that Alice and Bob can perform locally. In this discussion, assume that they do not communicate their measurement outcomes. We examine three cases: Alice measures first and Bob later; Bob measures first and Alice later; and Alice and Bob measure simultaneously.

- *Alice measures first, Bob later.* Alicеś measurement is described by the projectors $\{|\alpha\rangle\langle\alpha| \otimes \mathbb{1}, |\alpha_\perp\rangle\langle\alpha_\perp| \otimes \mathbb{1}\}$. According to the measurement postulate, the Bell state is projected onto one of the states

$$|\alpha\rangle\langle\alpha| \otimes \mathbb{1}|B_{00}\rangle = \frac{1}{\sqrt{2}}|\alpha\alpha\rangle \to |\alpha\rangle \otimes |\alpha\rangle \qquad \text{with proba } \frac{1}{2}$$

$$|\alpha_\perp\rangle\langle\alpha_\perp| \otimes \mathbb{1}|B_{00}\rangle = \frac{1}{\sqrt{2}}|\alpha_\perp\alpha_\perp\rangle \to |\alpha_\perp\rangle \otimes |\alpha_\perp\rangle \qquad \text{with proba } \frac{1}{2}$$

Consequently, Alice observes her photon in state $|\alpha\rangle$ or $|\alpha_\perp\rangle$ with probability $1/2$. Bob, on his side, does not know Alicés outcome and may not even know that she has measured. To perform his measurement, Bob chooses a basis $\{|\beta\rangle, |\beta_\perp\rangle\}$. perform its measurement, Bob chosen a basis $\{|\beta\rangle, |\beta_\perp\rangle\}$. If his photon is in state $|\alpha\rangle$ before the measurement, it is projected onto $|\beta\rangle$ with probability $\cos^2(\alpha - \beta)$ or onto $|\beta_\perp\rangle$ with probability $\sin^2(\alpha - \beta)$. If instead the photon is in $|\alpha_\perp\rangle$, the two probabilities are interchanged. Bob does not know the pre-measurement state of his photon, nor whether Alice has already measured, but this has no effect on his local statistics. He performs a definite experiment—measurement in the basis $\{|\beta\rangle, |\beta_\perp\rangle\}$—and obtains a definite outcome. Averaged over Aliceś unknown result, Bob finds $|\beta\rangle$ with probability $\frac{1}{2}$ and $|\beta_\perp\rangle$ with probability $\frac{1}{2}$. the state $|\beta\rangle$ with probability $\frac{1}{2}$ or $|\beta_\perp\rangle$ with probability $\frac{1}{2}$.

- *Bob measures first, Alice later.* By symmetry, if Bob measures first in the basis $\{|\beta\rangle, |\beta_\perp\rangle\}$ while Alice has not yet measured, and Alice later measures in $\{|\alpha\rangle, |\alpha_\perp\rangle\}$, the local statistics observed by each party are exactly the same as before. of each of the parts is the same that previously.
- *Alice and Bob measure simultaneously.* One might wonder whether simultaneous measurements change the conclusions. Suppose Alice and Bob perform simultaneous measurements in the product basis

$$\{|\alpha\beta\rangle; |\alpha\beta_\perp\rangle; |\alpha_\perp\beta\rangle; |\alpha_\perp\beta_\perp\rangle\}.$$

The state of Bell

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle)$$

The Bell state is projected onto one of these four basis states. Alice therefore obtains either $|\alpha\rangle$ or $|\alpha_\perp\rangle$, while Bob obtains either $|\beta\rangle$ or $|\beta_\perp\rangle$. The local situation is again the same as before. It is instructive to compute the corresponding probabilities explicitly. Alice finds $|\alpha\rangle$ (respectively $|\alpha_\perp\rangle$) with probability Alice constate that the probability of its results $|\alpha\rangle$ (resp. $|\alpha_\perp\rangle$) valent

$$\frac{1}{2}\cos^2(\alpha - \beta) + \frac{1}{2}\sin^2(\alpha - \beta) = \frac{1}{2}$$

The same result holds for Bob. Thus the local statistics of simultaneous measurements are identical to those of sequential measurements; the order of the local measurements is irrelevant.

Let us summarize. Whenever Alice and Bob perform local measurements, sequentially or simultaneously, and whatever bases they choose, each party obtains either basis state with probability $\frac{1}{2}$. In other words, the local outcome distribution has maximal entropy. Each photon taken separately is therefore maximally mixed, even though the joint two-photon state is pure and strongly correlated. Without access to one anotherś results, Alice and Bob cannot infer locally that the source produced an entangled pair. Each party sees only a maximally mixed local state. If neither party is told that the photons are entangled and no classical communication is allowed, entanglement cannot be established from local measurements alone. The situation changes once Alice

and Bob are allowed to compare their data. By exchanging classical messages, they can test the correlations between their measurement outcomes and thereby reveal entanglement. Here "communication" means ordinary classical exchange of measurement records. Thus entanglement is not directly observable through operations restricted to a single subsystem; it is the joint correlations between the separated subsystems that carry the relevant information.

6.2 Bell inequalities

Without communication, Alice and Bob cannot determine from their local data alone that the photons are entangled. Each observes a maximally mixed local state.

Once they compare their measurement records, however, they can test whether the joint correlations are compatible with a classical local description.

This idea originates in Bellś 1964 theorem, motivated by the celebrated 1935 paper of Einstein, Podolsky, and Rosen (EPR). EPR argued that the quantum state might not provide a complete description of a physical system and considered the possibility of a more classical underlying theory involving additional variables.

Bell provided an experimentally testable criterion for deciding whether the correlations of an EPR pair can be reproduced by a broad class of local classical theories. If the correlations admit such a description, suitable combinations of Aliceś and Bobś correlation functions must satisfy specific inequalities. Quantum mechanics predicts violations of these inequalities for entangled states. Bellś result therefore makes it possible to distinguish experimentally between local classical models and quantum mechanics. The landmark experiments of Aspect, Grangier, and Roger, followed by many later experiments, agree with the quantum-mechanical predictions and violate Bell inequalities.

Experimental protocol. At each trial n, a source S produces a pair of photons. One photon travels to Aliceś laboratory and the other to Bobś. The two laboratories are spatially separated and operate independently during the measurements: Alice and Bob do not communicate their settings or outcomes while a trial is in progress. Each laboratory can choose between two measurement bases (Figure **6.2**).

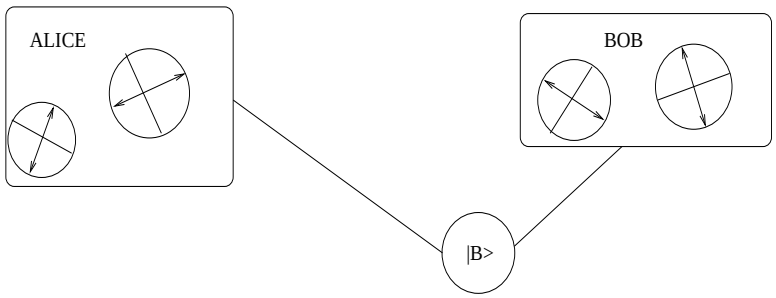


Figure 6.2 Experimental protocol used to test a Bell inequality.

- At each trial n, Alice randomly chooses one of the two analyzer settings

$$\{|\alpha\rangle, |\alpha_\perp\rangle\} \qquad \text{or} \qquad \{|\alpha'\rangle, |\alpha'_\perp\rangle\}$$

  to measure the polarization of her photon. If the detector clicks, she records $a_n = +1$ or $a'_n = +1$; otherwise she records $a_n = -1$ or $a'_n = -1$, according to the chosen setting.
- At each trial n, Bob independently chooses one of the two analyzer settings

$$\{|\beta\rangle, |\beta_\perp\rangle\} \qquad \text{or} \qquad \{|\beta'\rangle, |\beta'_\perp\rangle\}$$

  to measure the polarization of his photon. If the detector clicks, he records $b_n = +1$ or $b'_n = +1$; otherwise he records $b_n = -1$ or $b'_n = -1$. it records $b_n = -1$ or $b'_n = -1$.
- After all measurements have been completed, Alice and Bob use an ordinary classical channel to compare their records.

  They group the outcomes according to the measurement settings used in each trial. There are four possible experimental configurations:

$$1 = (\alpha, \beta);\ 2 = (\alpha, \beta');\ 3 = (\alpha'\beta);\ 4 = (\alpha'\beta')$$

  For each configuration they compute the corresponding empirical correlation

$$\frac{1}{N_1}\sum_{n_1} a_{n_1} b_{n_1},\ \frac{1}{N_2}\sum_{n_2} a_{n_2} b'_{n_2},\ \frac{1}{N_3}\sum_{n_1} a'_{n_3} b_{n_3},\ \frac{1}{N_4}\sum_{n_4} a'_{n_4} b'_{n_4}$$

  and combine the four correlations into the CHSH quantity

$$X_{exp} = \frac{1}{N_1}\sum_{n_1} a_{n_1} b_{n_1} + \frac{1}{N_2}\sum_{n_2} a_{n_2} b'_{n_2} - \frac{1}{N_3}\sum_{n_1} a'_{n_3} b_{n_3} + \frac{1}{N_4}\sum_{n_4} a'_{n_4} b'_{n_4}$$

  Evaluating this correlation therefore requires Alice and Bob to exchange their recorded values a and b.

Prediction of local classical theories. Suppose that the quantities measured by Alice and Bob are represented by observables A, A', B, and B' that possess definite values a, a', b, and b' in $\{+1, -1\}$, independently of which measurements are actually performed. This is analogous to the classical assumption that a particle has a definite position and velocity whether or not either quantity is measured. We further assume that Alicés and Bobś results can be described by a joint probability distribution[1]

$$\mathbb{P}\,[a, a', b, b']$$

The theoretical predictions corresponding to the four empirical averages above are

$$\mathbb{E}\,[ab], \mathbb{E}\,[ab'], \mathbb{E}\,[a'b], \mathbb{E}\,[a'b']$$

[1] Below we show how such a joint distribution follows from the standard locality assumption for a broad class of classical models, deterministic or stochastic.

By linearity of expectation,

$$\begin{aligned} X_{\text{theorique}} &= \mathbb{E}\,[ab] + \mathbb{E}\,[ab'] - \mathbb{E}\,[a'b] + \mathbb{E}\,[a'b'] \\ &= \mathbb{E}\,[ab + ab' - a'b + a'b'] \end{aligned}$$

Now observe that

$$ab + ab' - a'b + a'b' = a(b + b') + a'(b' - b)$$

and that

$$a(b + b') + a'(b' - b) = \pm 2$$

Indeed, if $b = b'$, only the first term contributes and its value is ± 2; if $b \neq b'$, only the second term contributes and its value is again ± 2. Therefore the expectation value must lie in $[-2, 2]$, and any local classical model of this type predicts

$$-2 \leq X_{\text{theorique}} \leq 2$$

This is the Clauser–Horne–Shimony–Holt (CHSH) inequality, one of the most widely used Bell inequalities.

The derivation assumes that the four variables A, A', B, and B' admit a common joint distribution $\mathbb{P}\,[a, a', b, b']$. This assumption is what allows $X_{\text{theorique}}$ to be written as the expectation value of a quantity that always lies in $[-2, 2]$. Experimentally, however, Alice and Bob never measure all four observables in a single trial. After comparing their records, they construct four histograms corresponding to the four possible pairs of analyzer settings. These histograms define four probability distributions:

$$\mathbb{P}_1\,[a, b],\ \mathbb{P}_2\,[a', b],\ \mathbb{P}_3\,[a, b'],\ \mathbb{P}_4\,[a', b']$$

It is not obvious a priori that these four distributions must be marginals of a single common distribution $\mathbb{P}\,[a, a', b, b']$. For a local classical theory, however, this is precisely what follows.

Assume that the laws governing the experiment are local. By this we mean that, once the physical state of the emitted pair is specified, Aliceś outcome depends only on her local analyzer setting, and Bobś outcome only on his. Let λ denote any additional classical variables (often called hidden variables) that characterize the state of the pair. Conditioned on λ, locality requires that Aliceś and Bobś response probabilities depend only on their respective local settings.

They can therefore be represented by distributions

$$p_{\mathcal{A}}(a|\alpha, \lambda),\ p_{\mathcal{A}}(a'|\alpha', \lambda),\ p_{\mathcal{B}}(b|\beta, \lambda),\ p_{\mathcal{B}}(b'|\beta', \lambda)$$

For fixed choices of α, α', β, and β', the four observed distributions are obtained by averaging over the hidden variable λ:

$$\mathbb{P}_1\,[a, b] = \int \mathrm{d}\lambda\ h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{B}}(b|\beta, \lambda)$$

$$\mathbb{P}_2\,[a', b] = \int \mathrm{d}\lambda\ h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{B}}(b'|\beta'; \lambda)$$

$$\mathbb{P}_3\,[a, b'] = \int \mathrm{d}\lambda\; h(\lambda) p_{\mathcal{A}}(a'|\alpha'; \lambda) p_{\mathcal{B}}(b|\beta, \lambda)$$

$$\mathbb{P}_4\,[a', b'] = \int \mathrm{d}\lambda\; h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{B}}(b|\beta, \lambda)$$

These distributions are the marginals of the joint probability distribution

$$\mathbb{P}_{\text{classical}}\,[a, a', b, b'] = \int \mathrm{d}\lambda\; h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{A}}(a'|\alpha'; \lambda) p_{\mathcal{B}}(b|\beta, \lambda) p_{\mathcal{B}}(b'|\beta'; \lambda)$$

This framework also includes deterministic theories as a special case: the probability distributions above may reduce to Dirac delta distributions.

Quantum-mechanical prediction for a Bell state. In quantum mechanics, Aliceś and Bobś four measurements are represented by the Hermitian observables

$$A = (+1)|\alpha\rangle\langle\alpha| + (-1)|\alpha_\perp\rangle\langle\alpha_\perp| \qquad A' = (+1)|\alpha'\rangle\langle\alpha'| + (-1)|\alpha'_\perp\rangle\langle\alpha'_\perp|$$

and

$$B = (+1)|\beta\rangle\langle\beta| + (-1)|\beta_\perp\rangle\langle\beta_\perp| \qquad B' = (+1)|\beta'\rangle\langle\beta'| + (-1)|\beta'_\perp\rangle\langle\beta'_\perp|$$

At each trial n, the two-photon state is described by a ket $|\Psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Quantum mechanics predicts the following four correlation functions:

$$\langle\Psi|A \otimes B|\Psi\rangle, \langle\Psi|A \otimes B'|\Psi\rangle, \langle\Psi|A' \otimes B|\Psi\rangle, \langle\Psi|A' \otimes B'|\Psi\rangle$$

The corresponding CHSH quantity is

$$X_{MQ} = \langle\Psi|A \otimes B|\Psi\rangle + \langle\Psi|A \otimes B'|\Psi\rangle - \langle\Psi|A' \otimes B|\Psi\rangle + \langle\Psi|A' \otimes B'|\Psi\rangle$$

We now evaluate this expression for the Bell state

$$|\Psi\rangle = |B_{00}\rangle$$

The first expectation value is conveniently evaluated by writing the Bell state as $\frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\alpha_\perp\alpha_\perp\rangle)$.

$$\begin{aligned}
\langle B_{00}|A \otimes B|B_{00}\rangle &= \frac{1}{2}\langle\alpha\alpha|A \otimes B|\alpha\alpha\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp|A \otimes B|\alpha_\perp\alpha_\perp\rangle \\
&\quad + \frac{1}{2}\langle\alpha\alpha|A \otimes B|\alpha_\perp\alpha_\perp\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp|A \otimes B|\alpha\alpha\rangle \\
&= \frac{1}{2}\langle\alpha|A|\alpha\rangle\langle\alpha|B|\alpha\rangle + \frac{1}{2}\langle\alpha_\perp|A|\alpha_\perp\rangle\langle\alpha_\perp|B|\alpha_\perp\rangle \\
&= \frac{1}{2}\cdot 1\cdot\left(|\langle\alpha|\beta\rangle|^2 - |\langle\alpha|\beta_\perp\rangle|^2\right) + \frac{1}{2}\cdot(-1)\cdot\left(|\langle\alpha_\perp|\beta\rangle|^2 - |\langle\alpha_\perp|\beta_\perp\rangle|^2\right) \\
&= \frac{1}{2}\left(\cos^2(\alpha-\beta) - \sin^2(\alpha-\beta)\right) - \frac{1}{2}\left(\sin^2(\alpha-\beta) - \cos^2(\alpha-\beta)\right) \\
&= \cos^2(\alpha-\beta) - \sin^2(\alpha-\beta) = \cos 2(\alpha-\beta)
\end{aligned}$$

Carrying out the analogous calculation for the other three expectation values gives

$$X_{MQ} = \cos 2(\alpha-\beta) + \cos 2(\alpha-\beta') - \cos 2(\alpha'-\beta) + \cos 2(\alpha'-\beta')$$

This expression is maximized by the following choice of angles (and by any common rotation of all four settings; see Figure **6.3**):

$$\alpha = 0,\ \alpha' = -\frac{\pi}{4},\ \beta = \frac{\pi}{8},\ \beta' = -\frac{\pi}{8}$$

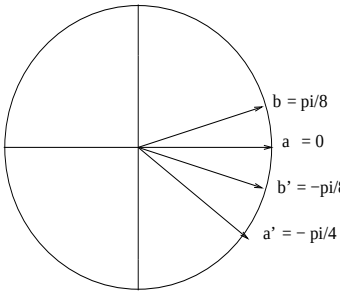


Figure 6.3 Analyzer orientations that maximize the CHSH violation.

For these settings the maximal value is

$$X_{MQ} = \cos\frac{\pi}{4} + \cos\frac{\pi}{4} - \cos\frac{3\pi}{4} + \cos\frac{\pi}{4} = 2\sqrt{2}$$

Thus the CHSH inequality is violated, since $2\sqrt{2} > 2$. The other Bell states lead to the same maximal violation for appropriately chosen analyzer orientations.

Quantum mechanics also predicts the four joint outcome distributions

$$\begin{aligned}
\mathbb{P}_1[a,b] &= \frac{1}{4}(1 + ab\cos 2(\alpha-\beta)) \\
\mathbb{P}_2[a',b] &= \frac{1}{4}(1 + ab'\cos 2(\alpha-\beta')) \\
\mathbb{P}_3[a,b'] &= \frac{1}{4}(1 + a'b\cos 2(\alpha'-\beta)) \\
\mathbb{P}_4[a',b'] &= \frac{1}{4}(1 + a'b'\cos 2(\alpha'-\beta'))
\end{aligned}$$

For example, $\mathbb{P}_2[+1,-1] = |\langle\alpha\beta'_\perp|B_{00}\rangle|^2 = \frac{1}{4}(1-\cos 2(\alpha-\beta'))$. For suitable choices of α, α', β, and β', these four distributions cannot be the marginals of any single classical distribution $\mathbb{P}[a,b,a',b']$. If such a distribution existed, the CHSH bound $-2 \le X \le 2$ would necessarily hold. The observed quantum correlations therefore cannot be described by a local classical joint probability distribution.

Remark. Entangled states are often said to exhibit "nonlocal correlations" because Bell inequalities can remain violated even when the two photons are separated by an arbitrarily large distance. This terminology must be used with care. The local measurements themselves are ordinary local physical interactions, and Bell correlations do not provide a mechanism for faster-than-light signaling. What is nonclassical is the structure of the

joint correlations, not a superluminal force acting between the particles. Moreover, entanglement cannot be demonstrated by local operations alone; the outcomes obtained at the two sites must ultimately be compared.

Experiments. The experiments of Aspect, Grangier, and Roger in the early 1980s found results consistent with quantum mechanics and incompatible with the relevant local classical models. A major experimental challenge is to choose or switch the analyzer settings rapidly enough that the measurement events at Alicés and Bobś sites are spacelike separated. In practice, the settings must be changed on a timescale shorter than the time required for light to travel between the two laboratories. This closes the possibility that an ordinary subluminal signal exchanged during the measurement could account for the observed correlations. Modern Bell tests have progressively tightened such locality and detection loopholes.

6.3 Quantum Teleportation

Suppose Alice and Bob are spatially separated and Alice possesses a qubit in the state

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

The state, i.e. the amplitudes α and β, need not be known to Alice and is not known to Bob. Alice and Bob also share an entangled pair

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and have access to a classical communication channel.

We shall show that by sending only two classical bits Alice can *teleport* the state of her qubit to Bob. Teleportation means that $|\Phi\rangle$ is destroyed in Alicés laboratory and reconstructed in Bobś. The destruction of the original state is essential because of the no-cloning theorem (Section **3.4**). After the protocol, Bob knows that his qubit is in state $|\Phi\rangle$, but he still need not know the amplitudes α and β. Importantly, teleportation requires the physical transmission of two classical bits from Alice to Bob. This classical communication cannot propagate faster than light, so the protocol is fully consistent with relativity. Also note that the physical carrier of the state $|\Phi\rangle$—for example photon polarization, electron spin, or an atomic degree of freedom— need not be the same in Alicés and Bobś laboratories.

The resource accounting for teleportation is often summarized as

Teleport 1 Qubit = Communicate 2 Cbits + Share 1 EPR pair

Teleportation can thus be viewed as a communication protocol that combines a classical channel with a pre-shared entangled pair.

The protocol.

- A source prepares an EPR pair in the Bell state $|B_{00}\rangle_{23}$. Particle 2 is sent to Alice and particle 3 to Bob. Their joint state belongs to $\mathcal{H}_2 \otimes \mathcal{H}_3 = \mathbb{C}^2 \otimes \mathbb{C}^2$.

- Alice prepares particle 1 in the state $|\Phi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$. The Hilbert space of the particle 1 is $\mathcal{H}_1 = \mathbb{C}^2$.

  The total Hilbert space of particles 1, 2, 3 is $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. The joint state is

  $$|\Psi\rangle = |\Phi\rangle_1 \otimes |B_{00}\rangle_{23}$$

  At this point, a short calculation will be useful:

  $$|\Psi\rangle = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

- Alice performs a local measurement on particles 1 and 2 in her laboratory. She measures in the Bell basis of $\mathcal{H}_1 \otimes \mathcal{H}_2$:

  $$\{|B_{00}\rangle_{12}, |B_{01}\rangle_{12}, |B_{10}\rangle_{12}, |B_{11}\rangle_{12}\}$$

  The corresponding projectors on the full three-particle system are

  $$P_{00} = |B_{00}\rangle\langle B_{00}|\otimes\mathbb{1}_3, P_{01} = |B_{01}\rangle\langle B_{01}|\otimes\mathbb{1}_3, P_{10} = |B_{10}\rangle\langle B_{10}|\otimes\mathbb{1}_3, P_{11} = |B_{11}\rangle\langle B_{11}|\otimes\mathbb{1}_3$$

  As usual, the measurement outcome is one of four possible projected states (up to normalization; one may verify that each outcome occurs with probability $\frac{1}{4}$):

  $$P_{00}|\Psi\rangle = \frac{1}{2}|B_{00}\rangle_{12} \otimes (\alpha|0\rangle_3 + \beta|1\rangle_3)$$

  $$P_{10}|\Psi\rangle = \frac{1}{2}|B_{10}\rangle_{12} \otimes (\alpha|0\rangle_3 - \beta|1\rangle_3)$$

  $$P_{01}|\Psi\rangle = \frac{1}{2}|B_{01}\rangle_{12} \otimes (\alpha|1\rangle_3 + \beta|0\rangle_3)$$

  $$P_{11}|\Psi\rangle = \frac{1}{2}|B_{11}\rangle_{12} \otimes (\alpha|1\rangle_3 - \beta|0\rangle_3)$$

- For these four possible outcomes, Bobś qubit is respectively in one of the states

  $$\begin{aligned}
  \alpha|0\rangle_3 + \beta|1\rangle_3 &= |\Phi\rangle \\
  \alpha|0\rangle_3 - \beta|1\rangle_3 &= Z|\Phi\rangle \\
  \alpha|1\rangle_3 + \beta|0\rangle_3 &= X|\Phi\rangle \\
  \alpha|1\rangle_3 - \beta|0\rangle_3 &= -iY|\Phi\rangle
  \end{aligned}$$

  but he does not know which one because he does not yet know Aliceś measurement outcome.

- Alice knows which Bell-state outcome she obtained. The four possibilities can be encoded by two classical bits, which she sends to Bob over the classical channel:

  $$00, 01, 10, 11$$

Once Bob receives Aliceś two-bit message, he knows which correction to apply. He performs the corresponding unitary operation on his qubit to recover $|\Phi\rangle$:

$$\mathbb{1}(\alpha|0\rangle_3 + \beta|1\rangle_3) = |\Phi\rangle$$
$$Z(\alpha|0\rangle_3 - \beta|1\rangle_3) = |\Phi\rangle$$
$$X(\alpha|1\rangle_3 + \beta|0\rangle_3) = |\Phi\rangle$$
$$iY(\alpha|1\rangle_3 - \beta|0\rangle_3) = |\Phi\rangle$$

After Aliceś Bell measurement, the original state $|\Phi\rangle$ no longer exists in her laboratory. Bob, after applying the appropriate correction, has reconstructed exactly that state on his qubit. The state has therefore been teleported from Alice to Bob.

6.4 Superdense coding

Suppose Alice and Bob have access to a quantum channel through which Alice can send qubits to Bob, and that they already share an EPR pair. Suppose also that Alice and Bob share a pair EPR. How many classical bits can Alice communicate by sending a single qubit through the quantum channel?

The answer is two classical bits, provided that Alice and Bob share one EPR pair in advance. The protocol that achieves this is called *superdense coding*. that they share a pair EPR. The protocol which implements this is called "superdense coding" (dense coding).

The resource accounting can be summarized as

Communicate 2 Cbits = Send 1 Qubit + Share 1 EPR pair

The protocol.

- An EPR pair in state $|B_{00}\rangle$ is prepared, with one particle sent to Alice and the other to Bob.
- Alice wishes to communicate two classical bits to Bob:
  - To send 00, she leaves her particle unchanged (equivalently, applies $\mathbb{1}$) and sends it to Bob. Bob now possesses the two-particle state
  $$|B_{00}\rangle$$
  - To send 01, Alice applies X to her particle and then sends it to Bob. The joint state becomes its particle to Bob. Bob is now in possession of the pair in the state
  $$X_1 \otimes \mathbb{1}_2|B_{00}\rangle = |B_{01}\rangle$$
  - To send 10, Alice applies Z to her particle and sends it to Bob. The joint state becomes in possession of the pair in the state
  $$Z_1 \otimes \mathbb{1}_2|B_{00}\rangle = |B_{10}\rangle$$

  - To send 11, Alice applies iY to her particle and sends it to Bob. The joint state becomes is now in possession of the pair in the state

$$(iY)_1 \otimes \mathbb{1}_2 |B_{00}\rangle = |B_{11}\rangle$$

- Bob now possesses both particles in one of the four Bell states $|B_{xy}\rangle$. To determine the two classical bits sent by Alice, he need only identify which Bell state he has. Because all four Bell states are mutually orthogonal, Bob can perform a local Bell-basis measurement on the two particles and recover the two-bit string xy.

Experiments. Quantum teleportation and superdense coding have both been demonstrated experimentally. An accessible overview is given, for example, in reviews of experimental quantum communication and entanglement.

7 Quantum Entropy

We have seen that density matrices describe both statistical ensembles of quantum states and reduced states of subsystems of multipartite systems. A density matrix is the quantum analogue of a classical probability distribution, and one can associate with it an entropy analogous to Shannon entropy. This quantity is the *von Neumann entropy*, introduced by von Neumann in 1927 in the context of quantum statistical mechanics, by analogy with Gibbs entropy. Just as Shannon entropy is fundamental to classical information theory, von Neumann entropy underlies quantitative descriptions of the compression, transmission, and accessibility of quantum information. In this chapter we introduce only the basic elements of this theory, whose development was strongly influenced by Holevoś work in the 1970s. Some properties of quantum entropy have no classical counterpart. In particular, for pure bipartite states the entropy of a reduced density matrix provides a useful measure of entanglement.

7.1 Shannon Entropy

Let X be a random variable taking values x in a finite discrete alphabet, with probabilities $p_x = \mathbb{P}_{\mathrm{X}}[X = x]$. By definition, the Shannon entropy of X is

$$H(X) = -\sum_x p_x \log p_x \tag{7.1}$$

This quantity measures the *average uncertainty* about X. We leave the base of the logarithm unspecified; base 2 and the natural logarithm are the most common choices, depending on the context.

The joint entropy of two random variables (X, Y) with joint distribution $p_{x,y} = \mathbb{P}_{\mathrm{X,Y}}[X = x, Y = y]$ is

$$H(X, Y) = -\sum_{x,y} p_{x,y} \log p_{x,y} \tag{7.2}$$

and the conditional entropy is

$$H(X|Y) = -\sum_y p_y \sum_x p_{x|y} \log p_{x|y} \tag{7.3}$$

where $p_{x|y} = \frac{p_{x,y}}{p_y}$. Equivalently, $H(X|Y) = \sum_y p_y H(X|Y = y)$, where $H(X|Y = y) =$

$-\sum_x p_{x|y} \log p_{x|y}$ is the entropy of X conditioned on the observation $Y = y$. It follows directly that

$$H(X|Y) = H(X, Y) - H(Y)$$

This formula has a simple interpretation: once Y is known, the joint uncertainty $H(X, Y)$ is reduced by the uncertainty $H(Y)$.

The mutual information between X and Y is the reduction in the uncertainty about X obtained by observing Y:

$$I(X; Y) = H(X) - H(X|Y) \tag{7.4}$$

This quantity is symmetric under exchange of X and Y, since

$$\begin{aligned} I(X; Y) &= H(X) - H(X|Y) \\ &= H(X) + H(Y) - H(X, Y) \\ &= H(Y) - H(Y/X) \\ &= I(Y; X) \end{aligned}$$

One can verify that $I(X; Y) = 0$ if and only if $p_{x,y} = p_x p_y$. Mutual information therefore quantifies the statistical dependence between X and Y.

Another important quantity is the Kullback–Leibler divergence, or relative entropy, between two probability distributions $\mathbb{P}_X$ and $\mathbb{Q}_X$:

$$D(\mathbb{P}_X \| \mathbb{Q}_X) = -\sum_x p_x \log q_x + \sum_x p_x \log p_x = \sum_x p_x \log\left(\frac{p_x}{q_x}\right)$$

This quantity behaves in some respects like a distance, although it is not symmetric: $D(\mathbb{P}_X \| \mathbb{Q}_X) \neq D(\mathbb{Q}_X \| \mathbb{P}_X)$. It is related to mutual information by

$$I(X; Y) = I(Y; X) = D(\mathbb{P}_{X,Y} \| \mathbb{P}_X \mathbb{P}_Y)$$

Thus mutual information can also be interpreted as the relative entropy between the joint distribution and the product of its marginals.

7.2 Basic Properties of Shannon Entropy

We now list, without proof, several basic inequalities satisfied by classical information measures and indicate which properties require modification in the quantum setting. Some proofs will be given directly in the quantum case.

- $H(X)$ is maximized by the uniform distribution. For an alphabet of cardinality d, $0 \leq H(X) \leq \log d$, with equality in the upper bound when $p_x = 1/d$.

• $H(X)$ is a concave functional of $\mathbb{P}_X$. If $\mathbb{P}_Z = \sum_k a_k \mathbb{P}_{X_k}$ with $0 \le a_k \le 1$ and $\sum_k a_k = 1$, then

$$H(Z) \ge \sum_k a_k H(X_k)$$

• Entropy is subadditive. If $\mathbb{P}_{X,Y}$ is a joint distribution with marginals $\mathbb{P}_X$ and $\mathbb{P}_Y$, then

$$H(X,Y) \le H(X) + H(Y)$$

In particular, this implies $I(X;Y) \ge 0$. From the definition of conditional entropy it also follows that

$$H(X|Y) \le H(X) \qquad \text{and} \qquad H(Y|X) \le H(Y)$$

• Conditional entropy is nonnegative: $H(X|Y) \ge 0$.

Equivalently, $H(X,Y) \ge H(X)$ and $H(X,Y) \ge H(Y)$: classically, the entropy of a whole system cannot be smaller than the entropy of one of its parts. This seemingly natural statement is false for quantum entropy. For an entangled bipartite pure state, the entropy of the joint state can vanish while the entropy of either subsystem is maximal, as for an EPR pair.

• Conditioning and strong subadditivity. Conditioning cannot increase entropy:

$$H(X|Y,Z) \le H(X|Y)$$

or, equivalently,

$$H(X,Y,Z) + H(Y) \le H(X,Y) + H(Y,Z)$$

The latter relation is the *strong subadditivity inequality*. Equality holds if and only if $X \to Y \to Z$ forms a Markov chain, i.e. $p_{x,y,z} = p_{z|y} p_{y|x} p_x$. Equivalently, $Z \to Y \to X$ is a Markov chain, or X and Z are conditionally independent given Y: $p_{x,z|y} = p_{x|y} p_{z|y}$.

• If $X \to Y \to Z$ forms a Markov chain, the data-processing inequality gives

$$H(X|Z) \ge H(X|Y)$$

Indeed, strong subadditivity gives $H(X|Z) \ge H(X|Y,Z)$, and the Markov property implies $H(X|Y,Z) = H(X|Y)$ because X and Z are conditionally independent given Y.

• Relative entropy is nonnegative: $D(\mathbb{P}_X \| \mathbb{Q}_X) \ge 0$. This follows from a convexity argument that also extends to the quantum case.

• The following algebraic identities follow directly from the definitions of entropy

and mutual information:

$$H(X_1, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_{i+1}, \ldots, X_n)$$

$$I(X_1, \ldots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y|X_{i+1}, \ldots, X_n)$$

7.3 von Neumann Entropy

We now consider a quantum system in a statistical state, or a subsystem that is not isolated from its environment. It is described by a density matrix $\rho : \mathcal{H} \longrightarrow \mathcal{H}$ satisfying $\rho = \rho^\dagger$, $\rho \geq 0$, and $\mathrm{Tr}\,\rho = 1$. The von Neumann entropy is defined by

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \tag{7.5}$$

More explicitly, if the spectral decomposition of ρ is $\rho = \sum_i \lambda_i |\chi_i\rangle\langle\chi_i|$, with $\rho|\chi_i\rangle = \lambda_i|\chi_i\rangle$, then

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

which is simply the Shannon entropy of the discrete probability distribution $\{\lambda_1, \ldots, \lambda_d\}$, where $d = \dim \mathcal{H}$.

Remark: For a preparation described by an ensemble $\{|\varphi_i\rangle, p_i\}$ whose states are not necessarily orthogonal, the von Neumann entropy is generally not equal to the Shannon entropy of the probabilities p_i. If X is a random variable with $\mathbb{P}_X[X = x_i] = p_i$, then $S(\rho) \leq H(X)$. The reason is that nonorthogonal quantum states cannot be perfectly distinguished by measurement. If the $|\varphi_i\rangle$ are orthonormal, equality holds: $S(\rho) = H(X)$.

For a system bipartite of hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ describes by the density matrix ρ_{AB}, the entropy of von Neumann is $S(\rho_{AB}) = -\mathrm{Tr}_{\mathcal{H}_A \otimes \mathcal{H}_B}(\rho_{AB} \log \rho_{AB})$. One can associate an entropy to each density matrix reduced $\rho_A = \mathrm{Tr}_{\mathcal{H}_B} \rho_{AB}$ and $\rho_B = \mathrm{Tr}_{\mathcal{H}_A} \rho_{AB}$, that is

$$S(\rho_A) = -\mathrm{Tr}(\rho_A \log \rho_A) \qquad \text{and} \qquad S(\rho_B) = -\mathrm{Tr}(\rho_B \log \rho_B)$$

We shall see that these quantities play an important role as measurement quantitative of entanglement.

Example: Entropy of systems simple. For a pure state $|\psi\rangle$, we have $\rho = |\psi\rangle\langle\psi|$ which has an eigenvalue equal to 1 and the other which are zero. Therefore, $S(|\psi\rangle\langle\psi|) = 0$. A pure state not contains no "uncertainty".

Now consider a pure entangled bipartite state and its reduced density matrices. The canonical example is an EPR pair, $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$. Since $\rho_A = \rho_B =$

$\frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, we have $S(\rho_{AB}) = 0$ while $S(\rho_A) = S(\rho_B) = \log 2$. Thus the joint pure state has zero entropy although each subsystem has maximal entropy. This phenomenon is general: for a bipartite pure state, the entropy of either reduced state is called the *entanglement entropy*. It is a genuinely quantum quantity and is not the entropy of a classical statistical ensemble.

Example: Entropy of one qubit. For one qubit, the density matrix is of the form $\rho = \frac{1}{2}\left(\mathbb{1} + \vec{a}\cdot\vec{\Sigma}\right)$ where $\|\vec{a}\| \leq 1$ is a vector of the sphere of Bloch. It is clear that to obtain the eigenvalues, one can do an unitary transformation which performs a rotation of the axes such that $\vec{a} \to (0, 0, \|\vec{a}\|)$. The two eigenvalues are therefore $\lambda_1 = \frac{1}{2}(1 + \|\vec{a}\|)$ and $\lambda_2 = \frac{1}{2}(1 - \|\vec{a}\|)$. The entropy of von Neumann of one qubit is therefore

$$\begin{aligned} S(\rho) &= -\frac{1}{2}(1 + \|\vec{a}\|)\log\left(\frac{1}{2}(1 + \|\vec{a}\|)\right) - \frac{1}{2}(1 - \|\vec{a}\|)\log\left(\frac{1}{2}(1 - \|\vec{a}\|)\right) \\ &= \log(2) - \frac{1}{2}(1 + \|\vec{a}\|)\log(1 + \|\vec{a}\|) - \frac{1}{2}(1 - \|\vec{a}\|)\log(1 - \|\vec{a}\|) \end{aligned}$$

Figure 7.1 The von Neumann entropy of a qubit is maximal at the center of the Bloch ball and decreases to zero on the surface, where the states are pure.

One may define quantum analogues of conditional entropy and mutual information by direct analogy with the corresponding Shannon expressions. For example:

$$\begin{aligned} S(\rho_A|\rho_B) &= S(\rho_{AB}) - S(\rho_B) \\ I(\rho_A;\rho_B) &= S(\rho_A) - S(\rho_A|\rho_B) \\ &= S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \\ &= S(\rho_B) - S(\rho_B|\rho_A) \end{aligned}$$

Although these definitions are sometimes useful, their operational meaning is subtler than in the classical case. In particular, there is no immediate quantum analogue of an ordinary conditional probability, because measuring one part of a quantum system generally changes its state. Several inequivalent notions of quantum conditional entropy and mutual information can therefore arise. We shall not pursue these alternatives here.

An important quantity is the quantum Kullback–Leibler divergence, or quantum relative entropy, between two density matrices:

$$D(\rho\|\sigma) = \mathrm{Tr}(\rho\log\rho) - \mathrm{Tr}(\rho\log\sigma) \tag{7.6}$$

We shall show that $D(\rho\|\sigma) \geq 0$, with equality if and only if $\rho = \sigma$. Although it is not symmetric, it is useful to think of relative entropy as a measure of distinguishability between density matrices.

7.4 Properties of Quantum Entropy

We now discuss several inequalities analogous to familiar classical entropy inequalities, together with genuinely quantum results such as the Araki–Lieb inequality.

• Maximum von Neumann entropy. In a Hilbert space of dimension d, $S(\rho)$ is maximized by the maximally mixed state $\rho = \frac{1}{d}\mathbb{1}_d$. Indeed, if λ_i are the eigenvalues of ρ, then $S(\rho) = -\sum_i \lambda_i \log \lambda_i$, which is maximal for the uniform spectrum $\lambda_i = 1/d$. Hence

$$0 \leq S(\rho) \leq \log d$$

• The entropy of von Neumann is concave.

$$S(t\rho + (1-t)\sigma) \geq tS(\rho) + (1-t)S(\sigma) \qquad 0 \leq t \leq 1 \tag{7.7}$$

for two density matrices ρ and σ. The proof is based on Kleinś inequality.

Lemma: Let A and B be Hermitian matrices and let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be a convex function. Then

$$\mathrm{Tr}\,(f(A) - f(B) - (A-B)f'(B)) \geq 0$$

Proof: Let $A|\phi_i\rangle = a_i|\phi_i\rangle$ and $B|\psi_j\rangle = b_j|\psi_j\rangle$. The trace on the left-hand side is

$$\begin{aligned}
&\sum_i \langle\phi_i|f(A) - f(B) - (A-B)f'(B)|\phi_i\rangle \\
&= \sum_i f(a_i) - \langle\phi_i|f(B)|\phi_i\rangle - a_i\langle\phi_i|f'(B)|\phi_i\rangle + \langle\phi_i|Bf'(B)|\phi_i\rangle \\
&= \sum_{i,j} |\langle\phi_i|\psi_j\rangle|^2 \Big\{f(a_i) - f(b_j) - (a_i - b_j)f'(b_j)\Big\}
\end{aligned}$$

where we used the completeness relation $\mathbb{1} = \sum_j |\psi_j\rangle\langle\psi_j|$ and $\sum_j |\langle\phi_i|\psi_j\rangle|^2 = 1$. Convexity gives $f(a_i) - f(b_j) \geq (a_i - b_j)f\prime(b_j)$ term by term, proving the lemma.

Corollary 1: Let A and B be positive semidefinite Hermitian matrices. Then

$$\mathrm{Tr}(A\log A) - \mathrm{Tr}(A\log B) \geq \mathrm{Tr}(A - B)$$

Proof: Apply Kleinś inequality to the convex function $f(x) = x\log x$ for $x \geq 0$.

Corollary 2: Quantum relative entropy is nonnegative.

Proof: Set $A = \rho$ and $B = \sigma$ and use $\mathrm{Tr}(\rho - \sigma) = 0$.

To complete the proof that von Neumann entropy is concave, choose $A = \rho$ and $B = t\rho + (1-t)\sigma$. The preceding corollaries imply

$$\mathrm{Tr}(\rho\log\rho) - \mathrm{Tr}(\rho\log(t\rho + (1-t)\sigma)) \geq (1-t)\,\mathrm{Tr}(\rho - \sigma) = 0 \tag{7.8}$$

Then, with $A = \sigma$ and $B = t\rho + (1-t)\sigma$, we obtain

$$\mathrm{Tr}(\sigma \log \sigma) - \mathrm{Tr}(\sigma \log(t\rho + (1-t)\sigma)) \geq t\,\mathrm{Tr}(\sigma - \rho) = 0 \tag{7.9}$$

Multiplying (7.8) by t and (7.9) by $(1-t)$, then adding the two inequalities, gives (7.7).

• Subadditivity of quantum entropy. Classically, subadditivity follows from

$$H(X) + H(Y) - H(X,Y) = D_{KL}(\mathbb{P}_{X,Y} \| \mathbb{P}_X \mathbb{P}_Y) \geq 0$$

The quantum proof is completely analogous once the Kullback–Leibler divergence is replaced by quantum relative entropy.

$$\begin{aligned} S(\rho_A) + S(\rho_B) - S(\rho_{AB}) &= -\mathrm{Tr}(\rho_A \log \rho_A) - \mathrm{Tr}(\rho_B \log \rho_B) + \mathrm{Tr}(\rho_{AB} \log \rho_{AB}) \\ &= -\mathrm{Tr}(\rho_{AB} \log \rho_A \otimes \mathbb{1}_B) - \mathrm{Tr}(\rho_{AB} \log \mathbb{1}_A \otimes \rho_B) + \mathrm{Tr}(\rho_{AB} \log \rho_{AB}) \\ &= \mathrm{Tr}(\rho_{AB} \log \rho_{AB}) - \mathrm{Tr}(\rho_{AB}(\log \rho_A \otimes \mathbb{1}_B + \log \mathbb{1}_A \otimes \rho_B)) \\ &= \mathrm{Tr}(\rho_{AB} \log \rho_{AB}) - \mathrm{Tr}(\rho_{AB} \log \rho_A \otimes \rho_B) \\ &= D(\rho_{AB} \| \rho_A \otimes \rho_B) \geq 0 \end{aligned}$$

Note that the identity $\log(\rho_A \otimes \mathbb{1}_B) + \log(\mathbb{1}_A \otimes \rho_B) = \log(\rho_A \otimes \rho_B)$ follows from the spectral decompositions of ρ_A and ρ_B, and the final inequality follows from Corollary 2.

• Strong subadditivity. Consider a tripartite state ρ_{ABC} on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, with reduced states $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_C} \rho_{ABC}$, $\rho_{BC} = \mathrm{Tr}_{\mathcal{H}_A} \rho_{ABC}$, and $\rho_B = \mathrm{Tr}_{\mathcal{H}_A \otimes \mathcal{H}_C} \rho_{ABC}$. Strong subadditivity states that

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$$

This inequality is analogue to the under-additivity strong classical. Nevertheless, in the case quantum, the proof is different and also much more complicated. It acts of an of the inequalities the more profondes of the theory of quantum information. We omettons completely this proof here and we mentionnons just that it is based on the concavity joint of the functional

$$f(A,B) = \mathrm{Tr}\left(M^\dagger A^s M B^{1-s}\right)$$

for any matrix M and $0 \leq s \leq 1$. The concavity joint of this functional was a conjecture of Wigner, Yanase and Dyson and was finally proved by Lieb. More later, Lieb and Ruskai showed that it implies the under-additivity strong.

• Araki–Lieb inequality. We already noted that the classical inequality $H(X,Y) \geq H(X)$ does not extend directly to quantum systems. For example, for the Bell state $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$, one has $S(\rho_{AB}) = 0$ while $\rho_A = \rho_B = \frac{1}{2}\mathbb{1}$ and hence $S(\rho_A) = S(\rho_B) = \log 2$. More generally, Schmidt decomposition implies that for any bipartite pure state the two reduced density matrices have the same nonzero eigenvalues and therefore the same entropy. The Araki–Lieb inequality generalizes this observation to arbitrary mixed states.

Let ρ_{AB} be a bipartite mixed state. The Araki–Lieb inequality states

$$S(\rho_{AB}) \geq |S(\rho_A) - S(\rho_B)|$$

The proof uses the method of the purification. The system AB can be purified in introduisant a "environment" C such that $\rho_{ABC} = |\psi\rangle_{ABC}\langle\psi|_{ABC}$ is pure and $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_C}(\rho_{ABC})$. By the under-additivity. We have

$$S(\rho_{AC}) \leq S(\rho_A) + S(\rho_C) \tag{7.10}$$

By the Schmidt theorem, since ρ_{ABC} is pure, we have

$$S(\rho_{AB}) = S(\rho_C) \quad \text{and} \quad S(\rho_{AC}) = S(\rho_B) \tag{7.11}$$

Of (7.10) and (7.11), it follows that

$$S(\rho_B) \leq S(\rho_A) + S(\rho_{AB})$$

that is $S(\rho_{AB}) \geq S(\rho_B) - S(\rho_A)$. By symmetry, we have also $S(\rho_{AB}) \geq S(\rho_A) - S(\rho_B)$. This completes the proof of the inequality of araki-Lieb.

7.5 No-Communication Principle

We have already encountered two fundamental quantum impossibility results in Chapter 3: the no-cloning theorem and the impossibility of perfectly distinguishing nonorthogonal states. We now introduce another important constraint, the *no-signaling* principle.

For a system bipartite, an operation local (unitary or of measurement) on a part cannot be detected by the other part without communication between the two parts.

To formulate it precisely, consider a bipartite system with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, density matrix ρ_{AB}, and reduced states ρ_A and ρ_B. A local unitary operation on subsystem A transforms the joint state into

$$(U_A \otimes \mathbb{1}_B)\, \rho_{AB}\, (U_A^\dagger \otimes \mathbb{1}_B)$$

A measurement projective local in A projects the state on

$$\sigma_{AB}^i = \frac{(P_A^i \otimes \mathbb{1}_B)\, \rho_{AB}\, (P_A^i \otimes \mathbb{1}_B)}{\mathrm{Tr}\Big((P_A^i \otimes \mathbb{1}_B)\, \rho_{AB}\, (P_A^i \otimes \mathbb{1}_B)\Big)}$$

with probability

$$p_i = \mathrm{Tr}\Big((P_A^i \otimes \mathbb{1}_B)\, \rho_{AB}\, (P_A^i \otimes \mathbb{1}_B)\Big) = \mathrm{Tr}\Big(P_A^i\, \rho_A\Big)$$

The reduced density matrices of A and B after this local unitary operation are

$$\rho_A^{\text{after}} = \mathrm{Tr}_B\Big((U_A \otimes \mathbb{1}_B)\, \rho_{AB}\, (U_A^\dagger \otimes \mathbb{1}_B)\Big) = U_A \rho_A U_A^\dagger$$
$$\rho_B^{\text{after}} = \mathrm{Tr}_A\Big((U_A \otimes \mathbb{1}_B)\, \rho_{AB}\, (U_A^\dagger \otimes \mathbb{1}_B)\Big) = \mathrm{Tr}_A\, \rho_{AB} = \rho_B$$

We let us see that after the unitary operation local at A, the density matrix of B is unchanged and therefore the operation at A is not detected in B.

After the operation of measurement local in A, the state of A is described by

$$\sigma_A^i = \mathrm{Tr}_B(\sigma_{AB}^i) = \frac{P_A^i \rho_A P_A^i}{\mathrm{Tr}\left(P_A^i \rho_A\right)}$$

with probability $p_i = \mathrm{Tr}\left(P_A^i \rho_A\right)$. In B, the result of the measurement is not observed therefore the description is given by the mixture statistical of the states σ_B^i:

$$\sigma_B^i = \mathrm{Tr}_A(\sigma_{AB}^i) = \frac{\mathrm{Tr}_A(P_A^i \otimes \mathbb{1}_B \rho_{AB})}{\mathrm{Tr}\left(P_A^i \rho_A\right)}, \qquad p_i = \mathrm{Tr}\left(P_A^i \rho_A\right)$$

The density matrix corresponding to this mixture is

$$\sum_i p_i \sigma_B^i = \sum_i \mathrm{Tr}_A(P_A^i \otimes \mathbb{1}_B \rho_{AB}) = \mathrm{Tr}_A(\rho_{AB}) = \rho_B$$

because $\sum_i P_A^i = \mathbb{1}_A$. Again, we concluons that the measurement local of A let the density matrix of B unchanged and this measurement is undetectable.

Let us denote that if we allows a communication between A and B, then A could communicate B that the result of the measurement local is j (or well σ_A^j). In this case, B can in deduce that its state is described by σ_B^j (which is different of ρ_B). The concavity of the entropy implies

$$S(\rho_B) = S(\sum_i p_i \sigma_B^i) \geq \sum_i p_i S(\sigma_B^i) \geq S(\sigma_B^j)$$

After communication between A and B, the entropy of B is therefore reduced. But before all communication, it there is no of change of entropy.

Example: Process of teleportation. Suppose that A and B share an EPR pair in the state $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$ and that A additionally holds a qubit $|\varphi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$. The reduced density matrices of A and B are

$$\rho_A = \frac{1}{2}|\varphi\rangle_A\langle\varphi|_A \otimes \mathbb{1}_A \qquad \rho_B = \frac{1}{2}\mathbb{1}_B$$

For the entropies, we have $S(\rho_{AB}) = 0$, $S(\rho_A) = S(\rho_B) = \log 2$. During of the measurement in the basis of Bell at A, the state total becomes equal to

$$|B_{ij}\rangle_A\langle B_{ij}|_A \otimes |\varphi^{ij}\rangle_B\langle\varphi^{ij}|_B$$

with probability $p_{ij} = \frac{1}{4}$, where $|\varphi^{ij}\rangle_B = X^i Z^j |\varphi\rangle_B$. The reduced density matrices become

$$\rho_A^{\text{after}} = |B_{ij}\rangle_A\langle B_{ij}|_A$$

if (i, j) is observed at A and

$$\rho_B^{\text{after}} = \frac{1}{4} \sum_{i,j=0,1} |\varphi^{ij}\rangle_B \langle\varphi^{ij}|_B = \frac{1}{2} \mathbb{1}_B$$

which remains unchanged. The entropies correspondantes are $S(\rho_A^{\text{after}}) = 0$ (if (i, j) is observed) and $S(\rho_B^{\text{after}}) = \ln 2$. For achever the process of teleportation, A communique (i, j) to B and the state of B is therefore describes by $|\varphi^{ij}\rangle_B \langle\varphi^{ij}|_B$ which has an entropy zero.

In summary, before the communication classical, during of the process of measurement local at A, no information not is transferred to B. This not is that after the communication classical that the information was transferred and that the entropy (≡ the uncertainty) becomes zero.

7.6 Entropy of a Mixture of Mixed States

In this section we prove the following theorem, which plays an important role in quantum information theory.

Theorem. Let X be a random variable with distribution $\mathbb{P}_X[X = x] = p_x$, and let $\rho = \sum_x p_x \rho_x$, where the ρ_x may themselves be mixed states. Then

$$S(\rho) \leq \sum_x p_x S(\rho_x) + H(X)$$

The interpretation of this inequality is straightforward. The uncertainty associated with ρ cannot exceed the average uncertainty of the component states plus the classical uncertainty in the preparation label X. In particular, if $\rho_x = |\varphi_x\rangle\langle\varphi_x|$ are pure states, then $S(\rho) \leq H(X)$, as discussed in the remark in Section 7.3.

Proof. We first consider a mixture of pure states

$$\rho_S = \sum_x p_x |\phi_x\rangle_S \langle\phi_x|_S$$

Purify this system by introducing an environment $\mathcal{H}_\mathcal{E}$ whose dimension is at least the number of states $|\phi_x\rangle_S$. Let $|x\rangle_\mathcal{E}$ be an orthonormal basis of $\mathcal{H}_\mathcal{E}$. A purification is

$$|\Psi\rangle_{S\mathcal{E}} = \sum_x \sqrt{p_x} |\phi_x\rangle_S \otimes |x\rangle_\mathcal{E}$$

It is immediate that $\text{Tr}_\mathcal{E}(|\Psi\rangle\langle\Psi|_{S\mathcal{E}}) = \rho_S$. Moreover,

$$\begin{aligned} \rho_\mathcal{E} &= \text{Tr}_S(|\Psi\rangle\langle\Psi|_{S\mathcal{E}}) \\ &= \sum_{x,x'} \sqrt{p_x}\sqrt{p'_x} \langle\phi_x|\phi_{x'}\rangle_S |x\rangle\langle x'|_\mathcal{E} \end{aligned} \tag{7.12}$$

By the Schmidt theorem, $S(\rho_S) = S(\rho_\mathcal{E})$. Now consider the state $\rho'_\mathcal{E} = \sum_x p_x |x\rangle\langle x|_\mathcal{E}$. Positivity of the relative entropy gives

$$D(\rho_\mathcal{E} \| \rho'_\mathcal{E}) = \mathrm{Tr}\Big(\rho_\mathcal{E} \log \rho_\mathcal{E}\Big) - \mathrm{Tr}\Big(\rho_\mathcal{E} \log \rho'_\mathcal{E}\Big) \geq 0$$

Therefore

$$S(\rho_S) = S(\rho_\mathcal{E}) \leq -\mathrm{Tr}\Big(\rho_\mathcal{E} \log \rho'_\mathcal{E}\Big)$$

Since $\log \rho'_\mathcal{E} = \sum_x \log(p_x) |x\rangle\langle x|_\mathcal{E}$, this inequality becomes

$$\begin{aligned} S(\rho_S) &\leq -\sum_x \log(p_x)\, \mathrm{Tr}(\rho_\mathcal{E} |x\rangle\langle x|_\mathcal{E}) \\ &= -\sum_x \log(p_x) \langle x|\rho_\mathcal{E}|x\rangle_\mathcal{E} \end{aligned}$$

Using (7.12), we have $\langle x|\rho_\mathcal{E}|x\rangle_\mathcal{E} = p_x$, and hence

$$S(\rho_S) \leq H(X)$$

To extend the inequality to mixtures of mixed states, $\rho = \sum_x p_x \rho_x$, use the spectral decomposition $\rho_x = \sum_j \lambda_j^x |e_j^x\rangle\langle e_j^x|$, so that

$$\rho = \sum_{x,j} p_x \lambda_j^x |e_j^x\rangle\langle e_j^x|$$

By the previous result

$$\begin{aligned} S(\rho) &\leq -\sum_{x,j} p_x \lambda_j^x \log\Big(p_x \lambda_j^x\Big) \\ &= -\sum_{x,j} p_x \lambda_j^x \log(p_x) - \sum_{x,j} p_x \lambda_j^x \log\Big(\lambda_j^x\Big) \\ &= -\sum_x p_x \log(p_x) - \sum_x p_x \sum_j \lambda_j^x \log\Big(\lambda_j^x\Big) \\ &= H(X) + \sum_x p_x S(\rho_x) \end{aligned}$$

7.7 Accessible Information and the Holevo Bound

We now ask how much information can be obtained by measuring a mixture $\rho = \sum_x p_x \rho_x$. Imagine that a source prepares state ρ_x with probability p_x, described by a classical random variable X with $\mathbb{P}_\mathrm{X}[X = x] = p_x$. A projective measurement described by projectors P_y produces outcome y with probability $q_y = \mathrm{Tr}\Big(P_y \rho\Big)$, thereby defining a random variable Y. Conditioned on the preparation $X = x$, the outcome probability is $p_{y|x} = \mathrm{Tr}\Big(P_y \rho_x\Big)$, and the joint probability is $\mathbb{P}_{\mathrm{X,Y}}[X = x, Y = y] = p_x \,\mathrm{Tr}\Big(P_y \rho_x\Big)$. These definitions have the expected marginal distributions.

The information about the preparation X obtained from the measurement outcome Y

is quantified by the mutual information $I(X;Y) = H(X) + H(Y) - H(X,Y)$.

The accessible information of the ensemble is the maximum of $I(X;Y)$ over all allowed measurements:

$$\mathrm{Acc}\Big(\{p_x, \rho_x\}\Big) = \sup_{\{P_y\}} I(X;Y)$$

This is a functional of the ensemble $\{p_x, \rho_x\}$; knowledge of the average state ρ alone is not sufficient to determine it. Computing the accessible information is an optimization problem and can be difficult in practice.

A fundamental universal upper bound is provided by the Holevo bound.

Theorem (Holevo Bound)

Define the Holevo quantity

$$\chi\Big(\{p_x, \rho_x\}\Big) \equiv S(\rho) - \sum_x p_x S(\rho_x)$$

Then the accessible information satisfies

$$\mathrm{Acc}\Big(\{p_x, \rho_x\}\Big) \leq \chi\Big(\{p_x, \rho_x\}\Big)$$

Proof. Let $\mathcal{H}_S$ be the Hilbert space on which ρ acts. Introduce $\mathcal{H}_X \otimes \mathcal{H}_S \otimes \mathcal{H}_Y$, where $\{|x\rangle\}$ and $\{|y\rangle\}$ are orthonormal bases of $\mathcal{H}_X$ and $\mathcal{H}_Y$, respectively, and consider the state $\rho_{XSY} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \otimes |0\rangle\langle 0|$. Let $U_{XSY} = \mathbb{1}_X \otimes U_{SY}$ be the unitary operation defined by

$$U_{SY}|\phi\rangle_S \otimes |a\rangle_Y = \sum_y P_y |\phi\rangle_S \otimes |a \oplus y\rangle_Y$$

where $a \oplus y$ is computed modulo $\dim(\mathcal{H}_Y)$. One can verify that U_{SY} is unitary because it preserves inner products. Define $\rho'_{XSY} = U_{XSY} \rho_{XSY} U_{XSY}^\dagger$. Since unitary transformations preserve eigenvalues, $S(\rho_{XSY}) = S(\rho'_{XSY})$.

Now consider the reduced density matrices ρ_{SY} and ρ'_{SY}.

$$\begin{aligned}
\rho_{SY} &= \mathrm{Tr}_{\mathcal{H}_X}\left(\sum_x p_x |x\rangle\langle x| \otimes \rho \otimes |0\rangle\langle 0|\right) \\
&= \rho \otimes |0\rangle\langle 0| \\
\rho'_{SY} &= \mathrm{Tr}_{\mathcal{H}_X}\left(\sum_{x,y,y'} p_x |x\rangle\langle x| \otimes P_y \rho P'_y \otimes |y\rangle\langle y'|\right) \\
&= P_y \rho P'_y |y\rangle\langle y'|
\end{aligned}$$

These two density matrices are likewise related by U_{SY} and therefore have the same

entropy: $S(\rho_{SY}) = S(\rho'_{SY})$.

By strong subadditivity,

$$S(\rho'_{XSY}) - S(\rho'_{SY}) \leq S(\rho'_{XY}) - S(\rho'_Y)$$

and therefore

$$S(\rho_{XSY}) - S(\rho_{SY}) \leq S(\rho'_{XY}) - S(\rho'_Y) \tag{7.13}$$

The remainder of the proof consists of evaluating each entropy appearing in this inequality. Clearly,

$$S(\rho_{XSY}) = H(X) + \sum_x p_x S(\rho_x)$$

because the pure state $|0\rangle\langle 0|$ contributes no entropy and the states $|x\rangle$ are mutually orthogonal. On the other hand,

$$S(\rho_{SY}) = S(\rho)$$

since $|0\rangle\langle 0|$ has zero entropy. Moreover,

$$\begin{aligned}\rho'_{XY} &= \sum_{x,y,y'} p_x |x\rangle\langle x| \otimes |y\rangle\langle y'| \operatorname{Tr}_{\mathcal{H}_S}(P_y \rho_x P_{y'}) \\ &= \sum_{x,y,y'} p_x |x\rangle\langle x| \otimes |y\rangle\langle y'| \delta_{yy'} p_{y|x} \\ &= \sum_{x,y} p_x p_{y|x} |x\rangle\langle x| \otimes |y\rangle\langle y|\end{aligned}$$

because $\operatorname{Tr}_{\mathcal{H}_S}(P_y \rho_x P_{y'}) = \operatorname{Tr}_{\mathcal{H}_S}(P_{y'} P_y \rho_x) = \delta_{yy'} \operatorname{Tr}_{\mathcal{H}_S}(P_y \rho_x)$. Therefore,

$$S(\rho'_{XY}) = H(X, Y)$$

Finally, $\rho'_Y = \sum_{x,y} p_{x,y} |y\rangle\langle y| = \sum_y p_y |y\rangle\langle y|$, so

$$S(\rho'_Y) = H(Y)$$

Substituting these expressions into (7.13) gives

$$I(X;Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$$

This inequality holds for every projective measurement $\{P_y\}$. Maximizing the left-hand side over all projective measurements yields the Holevo bound.

Example

Let $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}\begin{pmatrix} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \frac{\langle 0|+\langle 1|}{\sqrt{2}} \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$.

The eigenvalues of ρ are $\frac{1}{2} \pm \frac{\sqrt{2}}{4}$, so in this case the Holevo bound is $S(\rho) = 0.59 \ln 2$. Thus no measurement can extract more than 0.59 bits of information

from this ensemble. Consider, for example, a measurement in the computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. We obtain

$$p_y = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \end{pmatrix}, \qquad p_{y|x} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}, \qquad p_{x,y} = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} \\ 0 & \frac{1}{4} \end{pmatrix}$$

A direct calculation gives $I(X;Y) = \frac{3}{2}\log 2 - \frac{3}{4}\log 3 = 0.31 \ln 2$. Thus this particular measurement extracts 0.31 bits of information.

8 Local Operations and Classical Communication

The teleportation protocol studied in Chapter **6** is a representative example of *local operations and classical communication* (LOCC). Alice and Bob share an entangled pair, perform only local unitary operations and local measurements, and communicate solely through a classical channel. It is natural to study this class of operations more generally, with the long-term goal of understanding quantum-communication protocols on multipartite networks whose nodes share entangled resources.

In this chapter we introduce the basic ideas of this subject. We begin with a simple example that illustrates entanglement dilution and distillation. We then formalize LOCC and its stochastic counterpart, SLOCC, and discuss asymptotically optimal dilution and distillation protocols using the von Neumann entropy introduced in Chapter **7**. Finally, we show how SLOCC transformations lead to a classification of entangled resources into equivalence classes, with particular emphasis on two- and three-qubit pure states.

8.1 Dilution Transformations

A Simple Example

Consider the following problem. Alice and Bob share two qubits in the Bell state $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. They wish to convert it into a less entangled state $|\psi_\theta\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ with $\theta \neq \frac{\pi}{4}$. The state is less entangled in the sense that the entropy of either reduced density matrix is smaller than $\ln 2$. Because Alice and Bob are spatially separated and share only a classical communication channel, all quantum operations must be local.

Alice performs a POVM[1] with

$$M_0 = \begin{pmatrix} \cos\theta & 0 \\ 0 & \sin\theta \end{pmatrix} \quad \text{and} \quad M_1 = \begin{pmatrix} \sin\theta & 0 \\ 0 & \cos\theta \end{pmatrix}$$

[1] A positive-operator-valued measurement (POVM) generalizes an ordinary projective measurement. It provides the most general description of a measurement on a subsystem when an environment or ancillary system may be involved. Mathematically, $\{M_0, \ldots, M_n\}$ defines a POVM when $\sum_i M_i^\dagger M_i = \mathbb{1}$. Conditional on outcome i, the state of the measured system is proportional to $M_i|\psi\rangle$, and that outcome occurs with probability $\langle\psi|M_i^\dagger M_i|\psi\rangle$.

Note that $\{M_0, M_1\}$ is a POVM because $M_0^\dagger M_0 + M_1^\dagger M_1 = \mathbb{1}$. The state resulting after the measurement is proportional to one of the two states

$$M_0 \otimes \mathbb{1}|B_{00}\rangle = \frac{1}{\sqrt{2}}\Big(\cos\theta\,|00\rangle + \sin\theta\,|11\rangle\Big)$$
$$M_1 \otimes \mathbb{1}|B_{00}\rangle = \frac{1}{\sqrt{2}}\Big(\sin\theta\,|00\rangle + \cos\theta\,|11\rangle\Big)$$

with probabilities

$$p_0 = \langle B_{00}|(M_0 \otimes \mathbb{1})^\dagger (M_0 \otimes \mathbb{1})|B_{00}\rangle = \frac{1}{2}$$
$$p_1 = \langle B_{00}|(M_1 \otimes \mathbb{1})^\dagger (M_1 \otimes \mathbb{1})|B_{00}\rangle = \frac{1}{2}$$

If Alice obtains outcome $i = 0$ or 1, she applies the local unitary X^i to her qubit. She then sends the classical bit i to Bob, who applies X^i to his qubit. The final state of the protocol is therefore

$$(\mathbb{1} \otimes X^i)(X^i \otimes \mathbb{1})(M_i \otimes \mathbb{1})|B_{00}\rangle \propto |\psi_\theta\rangle \quad \text{for } i = 0, 1$$

Alice and Bob have thus implemented the transformation $|B_{00}\rangle \longrightarrow |\psi_\theta\rangle$ by LOCC.

A Theorem Characterizing Dilution Transformations

The transformation above is deterministic: the final state is always $|\psi_\theta\rangle$. This is a consequence of the following general theorem, stated here without proof.

Theorem

Let $|\phi\rangle$ and $|\psi\rangle$ be bipartite pure states on $\mathcal{H}_A \otimes \mathcal{H}_B$, with $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. Let $\vec{\lambda}_\phi = \{\lambda_\phi^1, \ldots, \lambda_\phi^d\}$ and $\vec{\lambda}_\psi = \{\lambda_\psi^1, \ldots, \lambda_\psi^d\}$ denote the spectra of the corresponding reduced density matrices.

If $\vec{\lambda}_\phi$ is majorized by $\vec{\lambda}_\psi$, equivalently if $\vec{\lambda}_\phi = P\vec{\lambda}_\psi$ for some doubly stochastic matrix P, then the transformation $|\phi\rangle \longrightarrow |\psi\rangle$ can be implemented deterministically by LOCC. Conversely, any deterministic LOCC transformation between bipartite pure states satisfies this majorization condition.

Remark. A doubly stochastic matrix has nonnegative entries, with every row sum and every column sum equal to 1. In particular, both P and P^T can be interpreted as transition matrices of Markov chains.

It follows from standard properties of majorization that $\vec{\lambda}_\phi = P\vec{\lambda}_\psi$ implies $S(\rho_\phi^A) \geq S(\rho_\psi^B)$. Thus $\vec{\lambda}_\phi$ is more mixed than $\vec{\lambda}_\psi$. Intuitively, the LOCC transformation is possible because $|\phi\rangle$ contains at least as much entanglement as $|\psi\rangle$.

Entropy of Dilution

For every two-qubit pure state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, the transformation $|B_{00}\rangle \longrightarrow |\psi\rangle$ can be performed deterministically by LOCC. Indeed, the preceding theorem requires a doubly stochastic matrix P satisfying $\lambda_{|B_{00}\rangle} = P\vec{\lambda}_\psi$. Since $\lambda_{|B_{00}\rangle} = (\frac{1}{2}, \frac{1}{2})^T$, the matrix $P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ always satisfies this condition.[2]

The natural next question is quantitative: given n Bell pairs, how many copies of $|\psi\rangle$ can Alice and Bob produce? Clearly they can produce at least $m = n$ copies, but asymptotically they may be able to produce more. If a Bell pair is regarded as a unit of entanglement, this asks for the entanglement cost of $|\psi\rangle$. The situation is illustrated in Figure **8.1**. Ancillary qubits in Aliceś and Bobś laboratories are allowed.

The transformation $|B_{00}\rangle^{\otimes n} \longrightarrow |\psi\rangle^{\otimes m}$ with $m \geq n$ is called *entanglement dilution*. We define the dilution entropy of $|\psi\rangle$ by

$$E_{\text{dilution}}(|\psi\rangle) = \sup\left\{ \frac{n}{m} \;\middle|\; |B_{00}\rangle^{\otimes n} \longrightarrow |\psi\rangle^{\otimes m} \quad \text{via a LOCC} \right\}$$

One can show that the supremum is attained asymptotically as $n, m \to \infty$ and that $E_{\text{dilution}}(|\psi\rangle) = S(\rho_\psi^A) = S(\rho_\psi^B)$. Thus the asymptotic entanglement cost of a bipartite pure state is its entanglement entropy.

[2] The reduced density matrix ρ_ψ^B is positive semidefinite and has unit trace, so its two eigenvalues are nonnegative and sum to one.

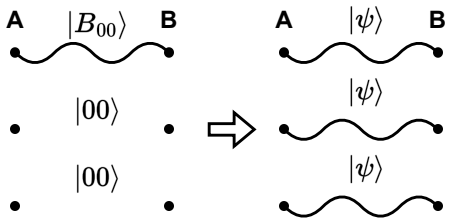


Figure 8.1 Dilution of Bell pairs into several copies of $|\psi\rangle$.

8.2 Distillation Transformation

A Simple Example

We now consider the reverse process. Suppose Alice and Bob share the bipartite state

$$|\psi_\theta\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$$

For $\theta \neq \frac{\pi}{4}$ this state is not maximally entangled. Alice and Bob would like to distill from it a perfect Bell pair using only local operations and classical communication. Unlike dilution, the transformation $|\psi_\theta\rangle \longrightarrow |B_{00}\rangle$ can in general succeed only probabilistically. If $\theta = 0$ or $\theta = \frac{\pi}{2}$, the state is a product state and the success probability is zero, because local operations cannot create entanglement from an unentangled state.

Alice performs first a measurement with a POVM $\left\{M_0, M_1\right\}$ as before, but this times-here on the state $|\psi_\theta\rangle$. The result is an of the two states proportional to

$$M_0 \otimes \mathbb{1}|\psi_\theta\rangle = \cos^2\theta\,|00\rangle + \sin^2\theta\,|11\rangle$$
$$M_1 \otimes \mathbb{1}|\psi_\theta\rangle = \sin\theta\,\cos\theta\left(|00\rangle + |11\rangle\right)$$

with the probabilities

$$p_0 = \langle\psi_\theta|(M_0 \otimes \mathbb{1})^\dagger(M_0 \otimes \mathbb{1})|\psi_\theta\rangle = \cos^4\theta + \sin^4\theta$$
$$p_1 = \langle\psi_\theta|(M_1 \otimes \mathbb{1})^\dagger(M_1 \otimes \mathbb{1})|\psi_\theta\rangle = 2(\sin\theta\,\cos\theta)^2$$

Thus, the state $|B_{00}\rangle$ occurs with probability $2(\sin\theta\,\cos\theta)^2$ which is the probability of success. In this case, Alice communique the bit classical of information $i = 1$ to Bob. If this is the state $\cos^2\theta\,|00\rangle + \sin^2\theta\,|11\rangle$ which survient, Alice communique the bit of information classical $i = 0$ to Bob and they ignorent the result.

For $\theta = 0$ or $\frac{\pi}{2}$, we sees although the probability of success is zero. For $\theta = \frac{\pi}{4}$, in revanche, the state of start was already $|B_{00}\rangle$ and the probability of success is of 1 (i.e. The two states obtenables after have measured with the POVM restent $|B_{00}\rangle$).

Unlike dilution, the distillation protocol succeeds only probabilistically. Protocols whose final outcome is not deterministic, such as this distillation procedure, are referred to as SLOCC protocols (stochastic local operations and classical communication).[3]

Entropy of Distillation

Given m copies of a bipartite state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, one may ask how many Bell pairs can be extracted using LOCC. In the simple protocol above the transformation succeeds with probability less than one; for $|\psi_\theta\rangle$ the success probability is $2(\sin\theta\cos\theta)^2$. Thus, for large m and n, this elementary protocol extracts approximately n Bell pairs from $m \simeq n/[2(\sin\theta\cos\theta)^2]$ copies of $|\psi_\theta\rangle$.

The operation of transformation $|\psi_\theta\rangle^{\otimes m} \longrightarrow |B_{00}\rangle^{\otimes n}$ The transformation $|\psi_\theta\rangle^{\otimes m} \longrightarrow |B_{00}\rangle^{\otimes n}$ is called *entanglement distillation*. The *distillable entanglement* of a pure state $|\psi\rangle$ is defined asymptotically by

$$E_{\text{distillation}}(|\psi\rangle) = \sup\left\{ \frac{n}{m} \;\middle|\; |\psi\rangle^{\otimes m} \longrightarrow |B_{00}\rangle^{\otimes n} \quad \text{via a LOCC} \right\}$$

More precisely, one requires the success probability to approach one as $m, n \to \infty$, while the approximation error ϵ tends to zero. For bipartite pure states the optimal asymptotic rate is $E_{\text{distillation}}(|\psi\rangle) = S(\rho_\psi^A) = S(\rho_\psi^B)$. Thus the distillable entanglement equals the entropy of entanglement.

For bipartite pure states, the optimal asymptotic dilution and distillation rates are therefore inverse processes governed by the same entropy. This reversibility is not obvious from the elementary one-copy protocols, whose success probabilities are generally asymmetric.

8.3 Optimal Dilution and Distillation Protocols

We now analyze the transformations $|B_{00}\rangle^{\otimes n} \to |\psi\rangle^{\otimes m}$ and $|\psi\rangle^{\otimes m} \to |B_{00}\rangle^{\otimes n}$ using standard methods from information theory. The aim is to prove that the optimal asymptotic dilution and distillation rates are both determined by the entanglement entropy $S(\rho_\psi^A) = S(\rho_\psi^B)$.

This requires to perform use to the notion of *typicality* in theory of the information classical and we faisons therefore a digression to this about.

[3] Both protocols involve quantum measurements, which are themselves probabilistic. The distinction is that dilution succeeds with probability one as an overall transformation and is therefore an LOCC protocol, whereas distillation has a nonzero failure probability and is therefore stochastic.

Typicality in Classical Information Theory

Be $x_1, x_2, \ldots, x_n$ n copies independent and identically distributed of a variable random of distribution $p(x)$, $x \in \mathcal{X}$ where $\mathcal{X}$ is an alphabet finite (for example $\mathcal{X} = \{0, 1\}$).

Definition

Given $\epsilon > 0$, a sequence $x_1, x_2, \ldots, x_n$ is called ϵ-typical if

$$\left| \frac{1}{n} \sum_{k=1}^{n} \log p\left(\frac{1}{x_k}\right) - H(X) \right| \leq \theta \tag{8.1}$$

In other words, a sequence of symboles emitted by the source $X \sim \mathbb{P}_X$ is typical if its entropy empirical is close of the entropy of Shannon $H(X) = \frac{1}{n} \sum_{x \in \mathcal{X}} p(x) \log p\left(\frac{1}{x}\right)$.

Theorem of the sequences typical

Let $\epsilon > 0$ and $x_1, \ldots, x_n \overset{\text{i.i.d}}{\sim} \mathbb{P}_X$. Let $T_{n,\epsilon}$ the set of the sequences ϵ-typical. For all $\delta > 0$, one can take n enough large such that (a)

$$\mathbb{P}\left[T_{n,\epsilon}\right] \geq 1 - \delta$$

and

$$(1 - \delta) 2^{n(H(X) - \epsilon)} \leq \left| T_{n,\epsilon} \right| \leq 2^{n(H(X) + \epsilon)}$$

[a] Here, $\mathbb{P}\left[T_{n,\epsilon}\right]$ wants say $\mathbb{P}\left[x_1, \ldots x_n \in T_{n,\epsilon}\right] = \sum_{\substack{x_1, \ldots, x_n \\ \in T_{n,\epsilon}}} p(x_1) \ldots p(x_n)$.

The theorem states that for every $\delta > 0$, and for sufficiently large n, at least a fraction $1 - \delta$ of all sequences are typical and their number is approximately $2^{nH(X)}$. This asymptotic equipartition property is the basis of Shannonś source-coding theorem: approximately $nH(X)$ bits are sufficient to represent the typical length-n sequences emitted by a source with distribution $\mathbb{P}_X$.

Proof of the Theorem

The proof is an application of the law of the large numbers. As $x_1, x_2, \ldots, x_n$ are independent and identically distributed with $\mathbb{P}_X$, the sum $-\frac{1}{n} \sum_{i=1}^{n} \log \mathbb{P}_X(x = x_i)$ concentrates on its average which not is other that $H(X)$. More formellement, the law of the large numbers states

$$\mathbb{P}\left[\left| -\frac{1}{n} \sum_{i=1}^{n} \log \mathbb{P}_X(x = x_i) - H(X) \right| \leq \epsilon \right] \geq 1 - \epsilon$$

for n enough large.

to obtain the bound on $\left|T_{n,\epsilon}\right|$, we note

$$\begin{aligned}\mathbb{P}\left[T_{n,\epsilon}\right] &= \sum_{\substack{x_1,\ldots,x_n \\ \in T_{n,\epsilon}}} p(x_1)\ldots p(x_n) \\ &= \sum_{\substack{x_1,\ldots,x_n \\ \in T_{n,\epsilon}}} 2^{-\sum_{i=1}^{n}\log\frac{1}{p(x_i)}}\end{aligned}$$

Or, the definition (8.1) of the sequences typical implies that

$$\left|T_{n,\epsilon}\right|2^{-n(H(X)+\epsilon)} \leq \mathbb{P}\left[T_{n,\epsilon}\right] \leq \left|T_{n,\epsilon}\right|2^{-n(H(X)-\epsilon)} \tag{8.2}$$

Of the first inequality of (8.2), it follows

$$\left|T_{n,\epsilon}\right|2^{-n(H(X)+\epsilon)} \leq \mathbb{P}\left[T_{n,\epsilon}\right] \leq 1$$

and therefore

$$\left|T_{n,\epsilon}\right| \leq 2^{n(H(X)+\epsilon)}$$

From the second inequality in (8.2), we obtain

$$1-\delta \leq \mathbb{P}\left[T_{n,\epsilon}\right] \leq \left|T_{n,\epsilon}\right|2^{-n(H(X)-\epsilon)}$$

and therefore

$$\left|T_{n,\epsilon}\right| \geq (1-\delta)2^{n(H(X)-\epsilon)}$$

We are now ready to establish the statements made above about entanglement dilution and distillation.

Optimal Dilution Protocol

Assume that Alice and Bob initially share n Bell pairs $|B_{00}\rangle$ and wish to prepare m copies of $|\psi\rangle$. If $m > n$, any additional local ancillary qubits are supplied independently to Alice and Bob. We describe an asymptotically optimal LOCC dilution protocol in the limit $n, m \to \infty$.

Suppose that $|\psi\rangle$ has the Schmidt decomposition

$$|\psi\rangle = \sum_x \sqrt{p(x)}|x\rangle_A \otimes |x\rangle_B$$

For the two-qubit case considered here, $x \in \{0,1\}$. We write the Schmidt coefficients as $\sqrt{p(x)}$, where $p(x) \in \{p_0, p_1\}$ defines a binary probability distribution.

The state that one wants build by of the operations SLOCC is

$$|\psi\rangle^{\otimes m} = \sum_{\substack{x_1,\ldots,x_n \\ \in \{0,1\}^n}} \sqrt{p(x_1)\ldots p(x_n)}\,|x_1 x_2 \ldots x_n\rangle_A \otimes |x_1 x_2 \ldots x_n\rangle_B \tag{8.3}$$

We shall consider an approximation of this state. This is this approximation which will

be in fact prepared. Let

$$|\varphi_m\rangle = \sum_{\substack{x_1,\ldots,x_n \\ \in T_{n,\epsilon}}} \sqrt{p(x_1)\ldots p(x_n)}\, |x_1 x_2 \ldots x_n\rangle_A \otimes |x_1 x_2 \ldots x_n\rangle_B$$

where the sum gate on the sequences typical associated to the distribution $p(x)$. The norme of this vector is

$$\langle\varphi_m|\varphi_m\rangle = \sum_{\substack{x_1,\ldots,x_n \\ \in T_{n,\epsilon}}} p(x_1)\ldots p(x_n) = \mathbb{P}\left[T_{n,\epsilon}\right]$$

Let $|\varphi'_m\rangle = |\varphi_m\rangle / \sqrt{\langle\varphi_m|\varphi_m\rangle}$ be the corresponding normalized state. Then

$$\begin{aligned}\langle\varphi'_m|\psi\rangle^{\otimes m} &= \frac{\sum_{\substack{x_1,\ldots,x_n \\ \in T_{n,\epsilon}}} p(x_1)\ldots p(x_n)}{\sqrt{\langle\varphi_m|\varphi_m\rangle}} \\ &= \sqrt{\mathbb{P}\left[T_{n,\epsilon}\right]} \geq \sqrt{1-\delta}\end{aligned}$$

Thus, for sufficiently large m, $|\varphi'_m\rangle$ is an arbitrarily good approximation to $|\psi\rangle^{\otimes m}$. As $m \to \infty$, one may choose $\delta \to 0$ so that $\left\||\varphi'_m\rangle - |\psi\rangle^{\otimes m}\right\|_2 \to 0$.

Moreover, the number of computational-basis terms in $|\varphi'_m\rangle$ is at most $\left|T_{m,\epsilon}\right| \leq 2^{m(H(p)+\epsilon)}$. Since $H(p) = S(\rho_\psi^A) = S(\rho_\psi^B)$, the typical component can be encoded using approximately $mS(\rho_\psi^A)$ qubits on each side.

We now describe how Alice and Bob can prepare $|\varphi'_m\rangle$ from Bell pairs. Suppose they share $n = mS(\rho_\psi^A) = mS(\rho_\psi^B)$ Bell pairs. They may use local ancillary qubits. Alice prepares both halves of the desired state locally and then teleports one half to Bob. Teleporting the relevant n qubits consumes the n Bell pairs and requires $2n$ classical bits. The teleportation protocol was introduced in Chapter **6**; the extension to this register-valued setting is immediate.

Consider first one typical term of Alicés local preparation, $|x_1 \ldots x_m\rangle_A \otimes |x_1 \ldots x_m\rangle_{A\text{-copy}}$. Because $x_1 \ldots x_m$ is typical, it can be compressed into approximately $mS(\rho_\psi^A) = n$ qubits by a local change of basis, giving a state of the form $|y_1 \ldots y_n 0 \ldots 0\rangle_A \otimes |y_1 \ldots y_n 0 \ldots 0\rangle_{A\text{-copy}}$. Alice teleports the nontrivial n-qubit register to Bob, after which local inverse basis changes reconstruct $|x_1 \ldots x_m\rangle_A \otimes |x_1 \ldots x_m\rangle_B$.

The state $|\varphi'_m\rangle$ is a coherent sum over typical sequences. Because the teleportation protocol is linear, the same local operations, measurements, and classical communication teleport the entire superposition coherently.

In summary, we have described a protocol that constructs $|\psi\rangle^{\otimes m}$ from $n = mS(\rho_\psi^A)$ Bell pairs. Therefore $E_{\text{dilution}}(|\psi\rangle) \geq S(\rho_\psi^A)$.

It remains to prove that this protocol is optimal, namely that $E_{\text{dilution}}(|\psi\rangle) \leq S(\rho_\psi^A)$. The proof of this inequality is omitted here.

Optimal Distillation Protocol

Alice and Bob now share m copies of $|\psi\rangle$ and wish to transform $|\psi\rangle^{\otimes m}$ into n EPR pairs $|B_{00}\rangle^{\otimes n}$. One expects $n \leq m$, so unlike the dilution protocol no additional entangled resource is required.

The typical sequences $T_{m,\epsilon}$ define a set of computational-basis states $\{|x_1 \dots x_m\rangle_A : (x_1 \dots x_m) \in T_{m,\epsilon}\}$. Their span is the *typical subspace*, denoted $\tau_{m,\epsilon} \subset (\mathbb{C}^2)^{\otimes m}$. Let $\mathcal{P}_{m,\epsilon}$ and $\mathcal{P}_{m,\epsilon}^{\perp}$ be the orthogonal projectors onto $\tau_{m,\epsilon}$ and its orthogonal complement. Since $\mathcal{P}_{m,\epsilon} + \mathcal{P}_{m,\epsilon}^{\perp} = \mathbb{1}$, they define a two-outcome projective measurement.

Alice performs this local measurement on her subsystem. Conditional on the typical outcome, $|\psi\rangle^{\otimes m}$ is projected onto a state proportional to

$$\mathcal{P}_{n,\epsilon} \otimes \mathbb{1} |\psi\rangle^{\otimes m} = \sum_{\substack{x_1,\dots,x_n \\ \in T_{n,\epsilon}}} \sqrt{p(x_1) \dots p(x_n)}\, |x_1 x_2 \dots x_n\rangle_A \otimes |x_1 x_2 \dots x_n\rangle_B$$

with probability $\langle\psi|^{\otimes m} \mathcal{P}_{n,\epsilon} \otimes \mathbb{1} |\psi\rangle^{\otimes m} = \mathbb{P}\left[T_{n,\epsilon}\right] \geq 1 - \epsilon$, whereas the complementary outcome gives the state

$$\mathcal{P}_{n,\epsilon}^{\perp} \otimes \mathbb{1} |\psi\rangle^{\otimes m} = \sum_{\substack{x_1,\dots,x_n \\ \in T_{n,\epsilon}^C}} \sqrt{p(x_1) \dots p(x_n)}\, |x_1 x_2 \dots x_n\rangle_A \otimes |x_1 x_2 \dots x_n\rangle_B$$

with complementary probability $\mathbb{P}\left[T_{n,\epsilon}^C\right] \leq \epsilon$.

The first state is precisely $|\varphi'_m\rangle$. Denote the orthogonal second state by $|\varphi'^{\perp}_m\rangle$. Alice sends Bob one classical bit indicating which measurement outcome occurred. Hence Alice and Bob transform $|\psi\rangle^{\otimes m}$ into $|\varphi'_m\rangle$ with success probability at least $1 - \delta$, where $\delta \to 0$ as $m \to \infty$.

The next step is to distill Bell pairs from $|\varphi'_m\rangle$. Since $\left|T_{m,\epsilon}\right| \approx 2^{mH(X)}$, the typical subspace can be represented using approximately $n = mH(X) = mS(\rho_{\varphi'_m}^{A/B})$ qubits. Alice and Bob may therefore choose local unitaries $U_A \otimes U_B$ such that

$$U_A \otimes U_B |\varphi'_m\rangle = \frac{1}{\sqrt{\mathbb{P}\left[T_{n,\epsilon}\right]}} \sum_{\substack{y_1 \dots y_n \\ \in \{0,1\}^n}} \sqrt{p(y_1) \dots p(y_n)}\, |y_1 \dots y_n\, 0 \dots 0\rangle_A \otimes |y_1 \dots y_n\, 0 \dots 0\rangle_B$$

Alice and Bob may discard the trailing qubits $|0 \dots 0\rangle_A \otimes |0 \dots 0\rangle_B$. The remaining registers can then be converted into n Bell pairs. The corresponding reduced density matrices are

$$\tilde{\rho}_{\varphi'_m}^{A,B} = \frac{1}{\sqrt{\mathbb{P}\left[T_{n,\epsilon}\right]}} \sum_{\substack{y_1 \dots y_n \\ \in \{0,1\}^n}} p(y_1 \dots y_n)\, |y_1 \dots y_n\rangle\langle y_1 \dots y_n|_{A,B}$$

with eigenvalues

$$\lambda_{y_1\dots y_n} = \frac{p(y_1\dots y_n)}{\sqrt{\mathbb{P}\,[T_{n,\epsilon}]}} \leq \frac{2^{-n(H(X)-\epsilon)}}{1-\delta}$$

Choose n such that

$$\frac{2^{-n(H(X)-\epsilon)}}{1-\delta} \leq 2^{-n} \tag{8.4}$$

the uniform vector $(2^{-n},\dots,2^{-n})$ is majorized by the vector $(\lambda_{y_1\dots y_n} \mid (y_1\dots y_n) \in \{0,1\}^n)$.

The theorem of Section **8.1** implies that $U_A \otimes U_B|\varphi'_m\rangle$ can be transformed into $|B_{00}\rangle^{\otimes n}$ whenever (8.4) is satisfied. For this protocol the largest admissible value is $n = m(H(X)-\epsilon) + \log(1-\delta)$. Taking $\epsilon,\delta \to 0$ and $m,n \to \infty$ gives $n/m \to H(X) = S(\rho_\psi^A) = S(\rho_\psi^B)$.

To conclude, we state without proof that this protocol achieves the optimal asymptotic value of $\frac{n}{m}$.

8.4 Tripartite States

For bipartite pure states, product states and entangled states form the two basic SLOCC classes. In general multipartite systems, however, the classification of entanglement resources is substantially richer and remains an active subject. Already for three qubits there are several inequivalent types of entanglement that cannot be converted into one another by SLOCC. These transformations partition multipartite pure states into natural equivalence classes. Any protocol that uses one state as a resource can use any SLOCC-equivalent state instead, at the price of adding the corresponding stochastic local conversion.

In the remainder of this chapter, we focus on the well-understood case of three qubits. We identify six SLOCC classes of tripartite pure states and discuss some of their basic properties. A detailed mathematical analysis, including the proof that these six classes are exhaustive, is deferred to Section **8.5**.

Triproduct States

A *fully separable* three-qubit state has the form $|\psi\rangle_{ABC} = |\varphi_A\rangle \otimes |\varphi_B\rangle \otimes |\varphi_C\rangle$, with $|\varphi_i\rangle \in \mathbb{C}^2$. A convenient representative is $|000\rangle$. Every fully separable state is obtained from this representative by local unitaries $U_A \otimes U_B \otimes U_C$.

Biproduct States

A second possibility is a biseparable state in which one party is unentangled while the other two share entanglement, for example $|\psi\rangle_{ABC} = |\varphi_A\rangle \otimes |\phi_{BC}\rangle$. A natural representative is $|0\rangle_A \otimes |B_{00}\rangle_{BC}$. By the Schmidt decomposition, any two-qubit pure state can be

written $|\phi_{BC}\rangle = \sqrt{\lambda_0}|\chi_0\rangle_B|\bar{\chi}_0\rangle_C + \sqrt{\lambda_1}|\chi_1\rangle_B|\bar{\chi}_1\rangle_C$. Starting from a Bell pair, an appropriate stochastic local filtering operation adjusts the Schmidt coefficients, while local unitaries U_B and U_C map the computational bases to the Schmidt bases. Hence all states in this biseparable class are connected by SLOCC transformations.

By symmetry, we sees that there exists 3 classes of equivalences of states bi-products corresponding to the bipartitions $A - BC$ (discussed here-above), $B - AC$ and $C - AB$. It is clear that of the operations local cannot do pass of a class to the other. Moreover, it is also clear that the operations local cannot transform the states tri-products in bi-products.

States with Tripartite Entanglement

We montrerons to the paragraph following that there exists two classes disjointes of states entangled under the relation of equivalence SLOCC: the states obtained from the state $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |111\rangle\Big)$ and those obtained from the state $|\text{W}\rangle = \frac{1}{\sqrt{3}}\Big(|001\rangle + |010\rangle + |100\rangle\Big)$.

It is useful to compare several properties of these two states. The one-qubit reduced density matrices are $\rho_A^{\text{GHZ}} = \frac{1}{2}\mathbb{1}$ and $\rho_A^{\text{W}} = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$, with analogous expressions for subsystems B and C. Thus each individual qubit has a diagonal reduced state and, when considered locally, behaves like a classical binary random variable. The genuinely quantum distinction between the GHZ and W states lies in their multipartite correlation structure rather than in any single-qubit reduced state.

The density matrix to 2 qubits, say of the system AB, is for GHZ:

$$\rho_{AB}^{\text{GHZ}} = \frac{1}{2}\Big(|00\rangle\langle 00| + |11\rangle\langle 11|\Big)$$

which is also diagonal and equivalent to a variable random binary. In particular, in the state GHZ, it n'y a no entanglement bipartite. For example, A and B cannot use the state GHZ for of the teleportation or of the dense coding between them.

For W, the density matrix to 2 qubits of the system AB is

$$\begin{aligned}\rho_{AB}^{\text{W}} &= \frac{1}{3}\Big\{|00\rangle\langle 00| + |01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|\Big\} \\ &= \frac{1}{3}|00\rangle\langle 00| + \frac{2}{3}|B_{01}\rangle\langle B_{01}|\end{aligned}$$

with $|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Thus Alice and Bob share an entangled resource in the form of a mixed, nonseparable state. If subsystem C decoheres locally, ρ_{AB}^{W} is unchanged; the bipartite entanglement between A and B therefore survives the loss of coherence in C.

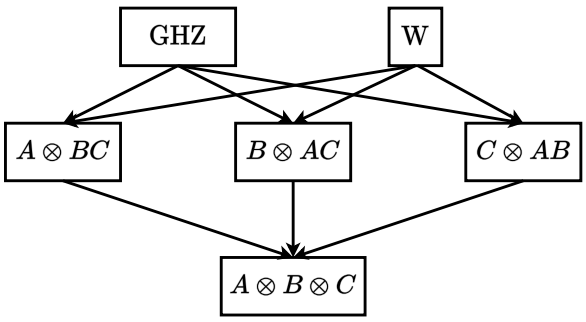


Figure 8.2 LOCC/SLOCC transformations between entanglement classes. Reverse transformations are not generally possible.

Hierarchy under LOCC Transformations

Applying the theorem of Section **8.1** shows that LOCC transformations exist from the GHZ and W classes to biseparable states such as $|0\rangle \otimes |B_{00}\rangle$, and from biseparable states to the fully separable state $|0\rangle \otimes |0\rangle \otimes |0\rangle$. For the chosen class representatives these transformations can succeed with probability one; for arbitrary states in the same classes, SLOCC conversion has nonzero success probability. These transformations are not reversible.

8.5 Analysis of the SLOCC Equivalence Relation

General Characterization of SLOCC Transformations

We now formalize SLOCC equivalence for general multipartite systems and give a useful criterion for characterizing the equivalence classes. Applied to three qubits, the criterion shows that the six classes described in Section **8.4** are exhaustive.

Definition

Two multipartite pure states $|\psi\rangle$ and $|\varphi\rangle$ are *SLOCC-equivalent* if each can be converted into the other with nonzero probability by local operations and classical communication. The SLOCC equivalence class of $|\psi\rangle$ is the set of all states related to it in this way.

SLOCC equivalence is reflexive, symmetric, and transitive, and therefore partitions multipartite pure states into disjoint equivalence classes.

At the level of a successful branch, a SLOCC transformation can be represented by a product of local operators $A_1 \otimes A_2 \otimes \cdots \otimes A_n$. For equivalence, these local operators may be taken invertible: a nonzero-probability inverse branch must exist in the opposite

direction. Classical communication coordinates which local branch has occurred, but does not change this product form for a fixed successful branch.

Two states $|\psi\rangle$ and $|\varphi\rangle$ are therefore SLOCC-equivalent if we have

$$|\psi\rangle = A_1 \otimes A_2 \otimes \ldots \otimes A_n |\varphi\rangle$$

with probability $p_1 p_2 \ldots p_n \neq 0$ and

$$|\varphi\rangle = A'_1 \otimes A'_2 \otimes \ldots \otimes A'_n |\psi\rangle$$

with probability $p'_1 p'_2 \ldots p'_n \neq 0$.

Theorem

Two states $|\psi\rangle$ and $|\varphi\rangle$ are SLOCC-equivalent if and only if one can find of the transformations local inversibles such as

$$|\psi\rangle = A_1 \otimes A_2 \otimes \ldots \otimes A_n |\varphi\rangle$$
$$|\varphi\rangle = A_1^{-1} \otimes A_2^{-1} \otimes \ldots \otimes A_n^{-1} |\psi\rangle$$

Proof

we considers first the case of transformations where this is only A_1 which fact of the transformations local and $A_2 = \ldots = A_n = \mathbb{1}$. The case general is not much more complicated. Suppose first that there exists a transformation local invertible such that

$$|\psi\rangle = A_1 \otimes \mathbb{1} |\varphi\rangle$$
$$|\varphi\rangle = A_1^{-1} \otimes \mathbb{1} |\psi\rangle$$

Since $\langle\psi|\psi\rangle = \langle\varphi|\varphi\rangle = 1$, it follows that $\langle\varphi|A_1^\dagger A_1|\varphi\rangle = \langle\psi|(A_1^{-1})^\dagger A_1^{-1}|\psi\rangle = 1$. Therefore, $\left\{\sqrt{p_1}A_1,\ \sqrt{1-p_1}A_1^\dagger A_1\right\}$ and $\left\{\sqrt{q_1}A_1^{-1},\ \sqrt{1-q_1}(A_1^{-1})^\dagger A_1^{-1}\right\}$ are of the POVM so much that $0 \leq p_1, q_1 \leq 1$ are of the probabilities sufficiently petites so that $p_1 A_1^\dagger A_1 < \mathbb{1}$ and $q_1 (A_1^{-1})^\dagger A_1^{-1} < \mathbb{1}$. Thanks to these POVM, on performs the transformation $|\psi\rangle \to |\varphi\rangle$ with probability p_1 and $|\varphi\rangle \to |\psi\rangle$ with probability q_1.

to prove the converse, on commence by supposer that there exists a transformation SLOCC with probability of success p_1 such that $|\psi\rangle = A_1 \otimes \mathbb{1}|\varphi\rangle$. we wants show that it is always possible of choose A_1 invertible. Be λ_i^ψ and λ_i^φ the eigenvalues density matrices reduced $\rho_{A_1}^\psi$ and $\rho_{A_1}^\varphi$ and be $|\chi_i\rangle$ and $|\tau_i\rangle$ the bases of the decomposition of Schmidt for $|\varphi\rangle$:

$$|\varphi\rangle = \sqrt{\lambda_0^\varphi}\,|\chi_0\rangle \otimes |\tau_0\rangle + \sqrt{\lambda_1^\varphi}\,|\chi_1\rangle \otimes |\tau_1\rangle$$

If U_{A_1} is the unitary for pass of the basis of Schmidt of the part A_1 of $|\varphi\rangle$ to the part A_1 of $|\psi\rangle$, we have:

$$|\psi\rangle = \sqrt{\lambda_0^\psi}\, U_{A_1}|\chi_0\rangle \otimes |\tau_0\rangle + \sqrt{\lambda_1^\psi}\, U_{A_1}|\chi_1\rangle \otimes |\tau_1\rangle$$

Let now

$$\tilde{A}_1 = \sqrt{\frac{\lambda_0^\psi}{\lambda_0^\varphi}}\, |\chi_0\rangle\langle\chi_0| + \sqrt{\frac{\lambda_1^\psi}{\lambda_1^\varphi}}\, |\chi_1\rangle\langle\chi_1|$$

On satisfies easily that $A_1 = U_{A_1}\tilde{A}_1$.

Since

$$\tilde{A}_1^{-1} = \sqrt{\frac{\lambda_0^\varphi}{\lambda_0^\psi}}\, |\chi_0\rangle\langle\chi_0| + \sqrt{\frac{\lambda_1^\varphi}{\lambda_1^\psi}}\, |\chi_1\rangle\langle\chi_1|$$

we have although A_1 is invertible with $A_1^{-1} = \tilde{A}_1^{-1}U_{A_1}^\dagger$.

Application to Two-Qubit States

We first show that bipartite pure states fall into exactly two SLOCC classes: product states and entangled states.

Let $|\psi\rangle_{AB}$ be a bipartite pure state. By the Schmidt theorem, the two reduced density matrices have the same rank, which for two qubits is either 1 or 2. If the rank is 1, both reduced states are pure and $|\psi\rangle_{AB}$ is a product state. All product states are related by invertible local unitary transformations, so they form a single SLOCC class represented by $|0\rangle \otimes |0\rangle$.

If the rank is 2, the Schmidt decomposition gives

$$|\psi\rangle_{AB} = \sqrt{\lambda_0}\, |\chi_0\rangle_A \otimes |\chi_0\rangle_B + \sqrt{\lambda_1}\, |\chi_1\rangle_A \otimes |\chi_1\rangle_B$$

where $\lambda_i > 0$ are the nonzero Schmidt coefficients and the $|\chi_i\rangle$ form orthonormal Schmidt bases. Local unitary transformations bring this state to

$$|\tilde{\psi}\rangle_{AB} = \sqrt{\lambda_0}\, |0\rangle_A \otimes |0\rangle_B + \sqrt{\lambda_1}\, |1\rangle_A \otimes |1\rangle_B$$

Since $\lambda_0 + \lambda_1 = 1$, write $\sqrt{\lambda_0} = \cos\theta$ and $\sqrt{\lambda_1} = \sin\theta$. The discussion in Section **8.1**, or directly the preceding SLOCC criterion, shows that every rank-2 two-qubit pure state is SLOCC-equivalent to the Bell state $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The Bell state is therefore a representative of the unique entangled two-qubit SLOCC class.

Application to Three-Qubit States

We now show that three-qubit pure states fall into the six SLOCC classes listed in Section **8.4**. Begin with the bipartition $A|BC$ and the corresponding reduced density matri-

ces ρ_A and ρ_{BC}. By the Schmidt theorem, $\mathrm{rank}(\rho_A) = \mathrm{rank}(\rho_{BC})$ and this rank is either 1 or 2.

If the rank is 1, the state factorizes as $|\psi\rangle_{ABC} = |\varphi_A\rangle \otimes |\varphi_{BC}\rangle$. The two-qubit state $|\varphi_{BC}\rangle$ is SLOCC-equivalent either to a product state or to a Bell state, while $|\varphi_A\rangle$ is locally unitarily equivalent to $|0\rangle_A$. This gives the fully separable class represented by $|000\rangle$ and the $A|BC$ biseparable class represented by $|0\rangle_A \otimes |B_{00}\rangle_{BC}$. Repeating the argument for the bipartitions $B|AC$ and $C|AB$ yields the other two biseparable classes.

Now consider the case $\mathrm{rank}(\rho_A) = \mathrm{rank}(\rho_{BC}) = 2$. The Schmidt decomposition gives

$$|\psi\rangle_{ABC} = \sqrt{\lambda_0}\,|\chi_0\rangle_A \otimes |\phi_0\rangle_{BC} + \sqrt{\lambda_1}\,|\chi_1\rangle_A \otimes |\phi_1\rangle_{BC}$$

where $|\chi_i\rangle$ and $|\phi_i\rangle$ are orthonormal eigenbases of ρ_A and ρ_{BC} and both λ_i are nonzero. A local unitary on A transforms this state into

$$\sqrt{\lambda_0}\,|0\rangle_A \otimes |\phi_0\rangle_{BC} + \sqrt{\lambda_1}\,|1\rangle_A \otimes |\phi_1\rangle_{BC}$$

There are two possibilities: $|\phi_0\rangle_{BC}$ is either a product state or an entangled state. An invertible local transformation on B and C can map it respectively to $|0\rangle_B \otimes |0\rangle_C$ or to a Bell state. The same transformation acts on $|\phi_1\rangle_{BC}$, so the full state is SLOCC-equivalent to

$$\sqrt{a_0}\,|0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C + \sqrt{a_1}\,|1\rangle_A \otimes |\tilde{\phi}_1\rangle_{BC} \tag{8.5}$$

where a_0 and a_1 are nonzero real numbers. If $a_1 = 0$, the state reduces to one of the product classes already considered.

First suppose that $|\tilde{\phi}_1\rangle_{BC}$ is a product state. One may apply the invertible local transformation

$$\frac{1}{\sqrt{2}}\begin{pmatrix} \frac{1}{\sqrt{a_0}} & 0 \\ 0 & \sqrt{a_1} \end{pmatrix} \otimes \begin{pmatrix} 1 & -\frac{s_B}{t_B} \\ 0 & \frac{1}{t_B} \end{pmatrix} \otimes \begin{pmatrix} 1 & -\frac{s_C}{t_C} \\ 0 & \frac{1}{t_C} \end{pmatrix}$$

to obtain

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |111\rangle\Big)$$

It remains to consider the case in which $|\tilde{\phi}_1\rangle_{BC}$ is entangled. As shown below, without loss of generality it can be brought to $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. In this case $|\psi\rangle_{ABC}$ is equivalent to

$$\sqrt{a_0}\,|000\rangle + \sqrt{\frac{a_1}{2}}|101\rangle + \sqrt{\frac{a_1}{2}}|110\rangle$$

Applying the invertible local transformation $X_A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gives

$$\sqrt{a_0}\,|100\rangle + \sqrt{\frac{a_1}{2}}|001\rangle + \sqrt{\frac{a_1}{2}}|010\rangle$$

Finally, applying the invertible local transformation

$$\frac{1}{\sqrt{3}}\begin{pmatrix}1 & 0\\ 0 & \frac{1}{\sqrt{a_0}}\end{pmatrix}\otimes\begin{pmatrix}\frac{2}{\sqrt{a_1}} & 0\\ 0 & 1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & \frac{2}{\sqrt{a_1}}\end{pmatrix}$$

produces

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}\big(|100\rangle + |010\rangle + |001\rangle\big)$$

It remains to justify the statement above. In the entangled case, write $|\tilde{\phi}_1\rangle_{BC}$ as a linear combination of $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Then (8.5) takes the form

$$\sqrt{a_0}\,|0\rangle\otimes|00\rangle + \sqrt{a_1}\,|1\rangle\otimes\big\{x\,|00\rangle + y\,|01\rangle + z\,|10\rangle + t\,|11\rangle\big\} =$$
$$\big(\sqrt{a_0}\,|0\rangle + x\sqrt{a_1}\,|1\rangle\big)\otimes|00\rangle + \sqrt{a_1}\,|1\rangle\otimes\big\{y\,|01\rangle + z\,|10\rangle + t\,|11\rangle\big\}$$

An invertible change of basis on subsystem A, for example with the matrix $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, brings the state to

$$\alpha\,|0\rangle\otimes|00\rangle + \beta\,|1\rangle\otimes\big\{y\,|01\rangle + z\,|10\rangle + t\,|11\rangle\big\}$$

This shows that, without loss of generality, the $|00\rangle$ component can be eliminated from $|\tilde{\phi}_1\rangle_{BC}$. We now note that

$$\rho_{BC} = \alpha^2\,|00\rangle\langle 00| + \beta^2\,\big\{y\,|01\rangle + z\,|10\rangle + t\,|11\rangle\big\}\big\{y\,\langle 01| + z\,\langle 10| + t\,\langle 11|\big\}$$

Thus every vector in the image of ρ_{BC} is a linear combination of $|00\rangle$ and $y|01\rangle+z|10\rangle+t|11\rangle$. To remain in the genuinely entangled case, no independent linear combination of these two vectors may be a product state; otherwise the problem reduces to the product case. Hence

$$\lambda\,|00\rangle + \big\{y\,|01\rangle + z\,|10\rangle + t\,|11\rangle\big\}$$

must be non-product for every λ. For a two-qubit pure state this requires $\lambda t \neq yz$ for all λ, which is possible only if $t = 0$. Therefore the $|11\rangle$ component can also be eliminated from $|\tilde{\phi}_1\rangle_{BC}$.

9 Quantum Circuit Model and Quantum Algorithms

This chapter introduces the circuit model of quantum computation. We begin with a brief historical perspective (Section **9.1**) and recall the classical circuit model (Section **9.2**). We then introduce Deutsch's model of quantum circuits (Section **9.3**), which provides both a precise definition of a quantum algorithm and a concrete graphical representation of quantum computations.

The basic ideas are illustrated with the Deutsch–Jozsa algorithm (Section **9.6**). Although simple, this algorithm already contains several ingredients that reappear in more powerful algorithms for finding hidden structure and symmetries. Shor's factoring algorithm, discussed in Chapter **11**, is the most celebrated example. For these problems, quantum algorithms can provide dramatic—and in some cases exponential—reductions in the number of required computational steps relative to known classical approaches.

9.1 Brief Historical Introduction

Every computation is ultimately implemented by a physical device. It is therefore natural to ask what fundamental limits the laws of physics impose on computation. Landauer made a pioneering contribution to this question in the 1960s and 1970s by showing that erasing one bit—an irreversible process—is necessarily accompanied by heat dissipation. At a fundamental level, erasure reduces the information stored in the computational degrees of freedom, and thermodynamics relates the corresponding entropy balance to heat exchanged with the environment.

Consequently, computations built from logically irreversible gates (such as AND and OR) are associated with dissipation. This raises a natural question: is there a fundamental lower bound on the heat that must be dissipated during computation, or can dissipation in principle be avoided? Bennett, Benioff, and others showed that *every irreversible computation can be embedded in a reversible computation* using suitable elementary gates. The price is additional memory: information that would otherwise be erased must instead be retained.

If a computation is implemented reversibly and the physical information carriers approach molecular or atomic scales, particularly at sufficiently low temperatures, the quantum nature of matter and the coherence of quantum states become important. This leads to a second question: how does quantum physics change the possibilities and

limitations of computation? Can genuinely quantum effects be used as computational resources?

These questions were raised by Feynman, Benioff, and Manin in the early 1980s. Quantum mechanics does not simply impose additional limitations. On the contrary, the superposition principle applied to systems of many qubits allows a single coherent state to contain amplitudes for many computational-basis configurations. This phenomenon is often called *quantum parallelism*. When combined with interference and suitable measurements, it can lead to substantial—sometimes exponential—speedups over known classical algorithms. Feynman emphasized in particular that generic quantum dynamics cannot be simulated efficiently by straightforward classical methods. He therefore proposed using controllable quantum systems themselves to simulate quantum processes efficiently.

The basic difficulty of classical simulation can already be seen from state-space dimension. A general pure state of N qubits is a superposition of 2^N computational-basis states:

$$|\Psi\rangle = \sum_{b_1 \dots b_N \in \{0,1\}^N} C(b_1 \dots b_N)|b_1 \dots b_N\rangle$$

Here $|b_1 \dots b_N\rangle = |b_1\rangle \otimes \cdots \otimes |b_N\rangle$, with $b_i \in \{0, 1\}$. These vectors form the computational basis. A direct classical simulation must in general keep track of 2^N complex amplitudes. By contrast, a physical quantum system evolves the entire coherent state under a unitary transformation U. A controllable device that implements such unitary dynamics on encoded qubits can therefore serve as a quantum computer.

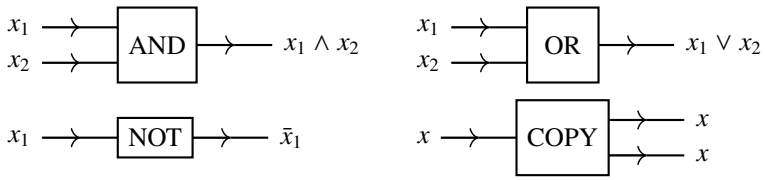
Classical computation can be represented by a circuit model built from a fixed universal set of elementary gates applied sequentially to the input. In 1985 David Deutsch showed that an analogous construction exists for quantum computation: arbitrary unitary transformations can be approximated to any desired accuracy using a finite universal set of elementary quantum gates.

Other models of quantum computation exist, but Deutschś quantum-circuit model is the most widely used. One purpose of this chapter is to explain this model. Its main advantage is universality: in principle every quantum computation can be represented by a circuit built from a small universal gate set. The circuit picture is also concrete and well suited to algorithm design.

There is also a quantum analogue of the Turing machine, which provides a natural framework for defining quantum complexity classes. The quantum Turing-machine model and the quantum-circuit model are computationally equivalent. We shall not discuss this equivalence further here.

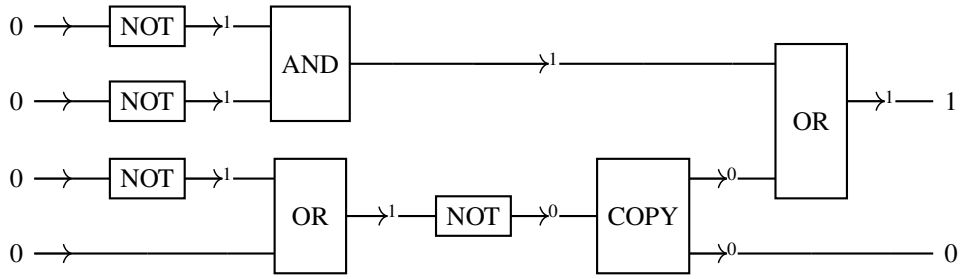
9.2 Circuit Model for Classical Computation

We begin with a brief review of classical computation in terms of Boolean circuits. Consider Boolean variables $x_i \in \mathbf{F}_2 = \{0, 1\}$ and the following elementary logical gates.



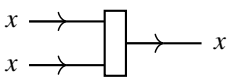
The COPY operation is also called FANOUT. These elementary gates can be combined to define Boolean circuits.

A Boolean circuit is a directed acyclic graph with n input bits and m output bits. Its vertices are Boolean gates and its directed wires carry bits from one gate to the next. If desired, a fixed all-zero input can be converted into any computational input $(x_1, \ldots, x_n)$ by applying NOT gates to selected wires. The following diagram illustrates a simple Boolean circuit.



A classical universality result due to Emil Post implies that every Boolean function $f : \mathbf{F}_2^n \to \mathbf{F}_2^m$ can be implemented by a Boolean circuit. More precisely, for any such function there exists a directed acyclic circuit that maps the input bits $(x_1, \ldots, x_n)$ to the output bits $(y_1, \ldots, y_m) = f(x_1, \ldots, x_n)$. The circuit can be built entirely from NOT, AND, OR, and COPY gates. We therefore say that the gate set {NOT, AND, OR, COPY} is universal for Boolean computation.

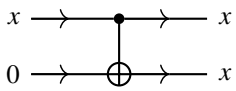
The NOT gate is logically reversible: its input can be recovered uniquely from its output. By contrast, AND and OR are logically irreversible because their outputs do not determine their inputs. Logical irreversibility has thermodynamic consequences. According to Landauer's principle, erasing information is necessarily accompanied by entropy production and, in a physical implementation, by heat dissipation to the environment. The status of COPY requires some care. In a reversible implementation one retains the original input and copies its value into an auxiliary bit; the inverse operation then recovers the auxiliary bit without erasing information. By contrast, an operation that simply discards one of the two copies is irreversible. Indeed, the inverse operation



erases one bit and therefore carries the thermodynamic cost identified by Landauer's principle.

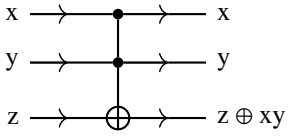
Bennett showed that any Boolean computation can be embedded in a reversible computation, provided that suitable auxiliary bits are introduced. There also exist universal sets of logically reversible gates. We shall not give the full construction here; the essential point is that irreversible gates such as AND and OR can be implemented reversibly by retaining enough information in auxiliary bits.

Consider first the COPY operation. It can be implemented reversibly as



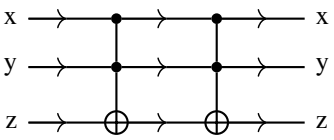
This is the reversible controlled-NOT gate (CNOT), acting on two bits. The upper bit is the *control bit*; the lower one is the *target* or storage bit, initialized here to 0.

AND and OR can be implemented reversibly using the *Toffoli gate*, also called the controlled-controlled-NOT (CCNOT) gate. It acts on three bits.



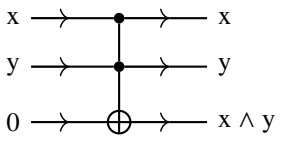
$\equiv \quad T(x, y, z) = (x, y, z \oplus xy)$

The Toffoli gate flips the target bit z if and only if both control bits x and y are equal to 1; otherwise z is unchanged. The gate is reversible because



$\equiv \quad T^2(x, y, z) = (x, y, z)$

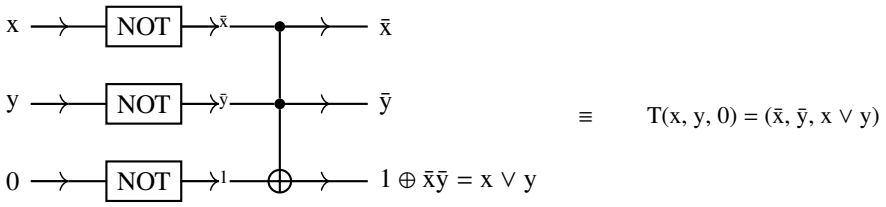
The gate AND corresponds to the case where z = 0. In this case, T(x, y, 0) = (x, y, xy) returns x ∧ y for the third bit.



$\equiv \quad T(x, y, 0) = (x, y, x \wedge y)$

For the gate OR, we uses

Summary. Any Boolean circuit built from {AND, OR, COPY, NOT} can be embedded in a reversible circuit built from the universal gate set {CNOT, Toffoli, NOT}. The



usual Boolean gate set contains operations on one or two bits, whereas a convenient universal reversible set contains the three-bit Toffoli gate. One can show that, for classical reversible computation, restricting to one- and two-bit gates is not sufficient for universality. Quantum computation is different: universal quantum gate sets using only one- and two-qubit gates do exist.

9.3 Quantum Circuits

Quantum circuits are the natural quantum analogue of classical circuits. They are built from a small set of elementary *quantum gates*. A quantum gate is a unitary operation acting on a small number of qubits, typically one or two. Every such gate is reversible because a unitary operator is invertible: $UU^\dagger = U^\dagger U = \mathbb{1}$. We shall discuss physical implementations in later chapters. We begin by introducing several elementary gates that will be used repeatedly.

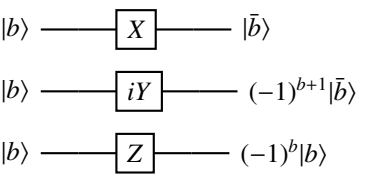
One-Qubit Gates

One-qubit gates are 2×2 unitary matrices acting on state vectors in $\mathbb{C}^2$. Several of them play a particularly important role.

- The three "matrices of Pauli" :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  These matrices are unitary and Hermitian. Their corresponding circuit symbols are shown below:



  The gate X is simply the quantum NOT gate. The essential difference from the

classical case is that its input may be an arbitrary coherent superposition of the basis states $\{|0\rangle, |1\rangle\}$, whereas a classical bit is either 0 or 1. For example,

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

Thus the NOT gate acts linearly on arbitrary qubit states, not merely on the two computational-basis states. This simple observation is fundamental and applies equally to all quantum gates discussed below.

- The Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$|b\rangle \text{ —} \boxed{H} \text{—} \; H|b\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b|1\rangle\right)$$

The Hadamard gate has no deterministic classical analogue: it maps computational-basis states to coherent superpositions.

- The T gate is $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$$|b\rangle \text{ —} \boxed{T} \text{—} \; e^{ib\pi/4}|b\rangle = \begin{cases} |0\rangle \\ e^{i\pi/4}|1\rangle \end{cases}$$

It acts on the superpositions as

$$T(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta e^{i\pi/4}|1\rangle$$

- The S gate is $S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$$|b\rangle \text{ —} \boxed{S} \text{—} \; e^{ib\pi/2}|b\rangle = \begin{cases} |0\rangle \\ i|1\rangle \end{cases}$$

It acts on the superpositions as

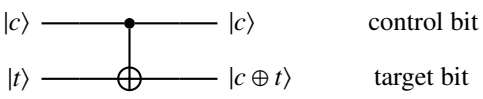
$$S(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + i\beta|1\rangle$$

More generally, any single-qubit unitary can be approximated to arbitrary accuracy, up to an irrelevant global phase, by a suitable product of elementary gates such as H and T. Note that $S = T^2$.

Two-Qubit Gates

Two-qubit gates are 4×4 unitary matrices acting on the Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. The most important example for our purposes is the controlled-NOT gate.

- The CNOT (controlled-NOT) gate is defined by:



In the basis

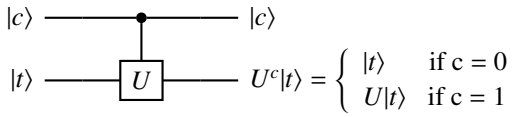
$$|0\rangle \otimes |0\rangle \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |0\rangle \otimes |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |1\rangle \otimes |0\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |1\rangle \otimes |1\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

the representation matricielle is

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

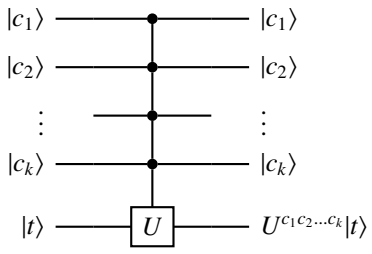
As with every quantum gate, CNOT acts linearly on arbitrary coherent superpositions of two-qubit basis states.

- An important generalization is the controlled-U gate, where U is an arbitrary single-qubit unitary:



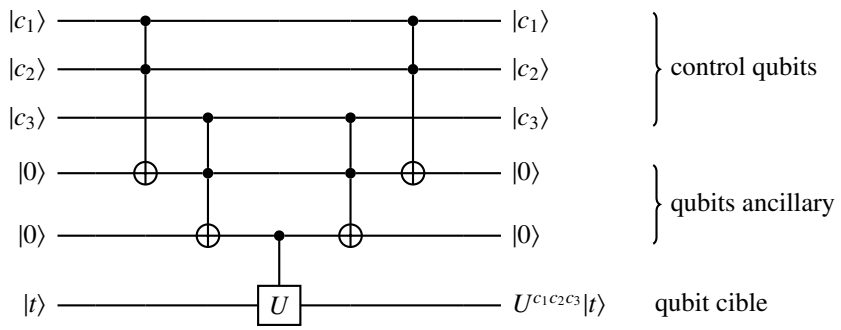
Multi-Controlled-U Gates

A generalization of the gates previous is

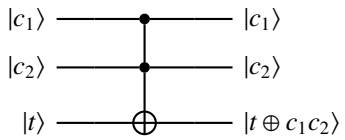


The unitary U acts on the target qubit if and only if all control qubits are in state $|1\rangle$. By linearity, the gate acts coherently on superpositions of computational-basis states. For an n-qubit register, such operations are represented by $2^n \times 2^n$ unitary matrices.

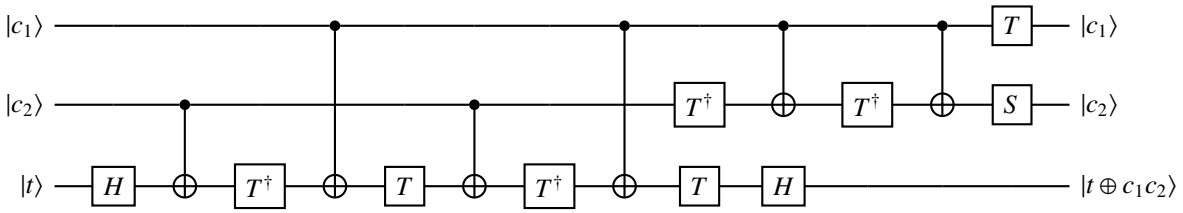
By introducing auxiliary qubits, a multiply controlled U gate can be decomposed into Toffoli gates and a singly controlled U. The following circuit illustrates the construction for three control qubits:



The controlled-controlled-NOT gate is also called the quantum Toffoli gate. Its action on computational-basis states is the same as the classical Toffoli gate, but its inputs may of course be arbitrary coherent superpositions. Remarkably, the Toffoli gate can be decomposed into one- and two-qubit gates. For example, a decomposition can be constructed from the set $\{T, S, H, \text{CNOT}\}$.



is equivalent to the following circuit:



To summarize, multiply controlled versions of a single-qubit unitary U can be decomposed into elementary controlled operations using auxiliary qubits. Since arbitrary single-qubit unitaries can themselves be approximated to arbitrary accuracy using H and T, the gate set $\{H, T, \text{CNOT}\}$ is sufficient for universal quantum computation.

Deutsch's Quantum Circuit Model

The preceding result extends to arbitrary registers. A fundamental universality theorem states that every unitary transformation on n qubits (that is, every $2^n \times 2^n$ unitary matrix) can be approximated to arbitrary accuracy by circuits built from the gate set $\{T, S, H, \text{CNOT}\}$. This theorem underlies the quantum-circuit model.

The computational complexity is measured by the number of elementary gates required to synthesize the desired unitary. For example, the unitary operations used in quantum integer factorization can be implemented with a number of elementary gates polynomial in the input size. By contrast, a generic n-qubit unitary requires an exponentially large circuit.

We may now summarize the quantum circuit model:

a). A quantum circuit is a directed acyclic graph whose vertices are elementary gates, here chosen from $\{T, S, H, \text{CNOT}\}$, and whose wires carry qubits of the form $\alpha|0\rangle + \beta|1\rangle$.

b). The input is given by the product state:

$$|0\rangle \otimes ... \otimes |0\rangle$$

c). The output of the unitary part of the computation has the general form

$$|\Psi\rangle = \sum_{c_1 ... c_n} A(c_1 ... c_n)|c_1 c_2 ... c_n\rangle$$

where the $A(c_1 \dots c_n)$ are complex amplitudes and $|c_1 c_2 \dots c_n\rangle = |c_1\rangle \otimes \cdots \otimes |c_n\rangle$ are the computational-basis states.

d). Finally, the state $|\Psi\rangle$ is measured in the computational basis $\{|c_1 c_2 \dots c_n\rangle : c_i \in \{0, 1\}\}$. The outcome $|c_1 \dots c_n\rangle$ occurs with probability $|A(c_1 \dots c_n)|^2$ by the Born rule. The result of a quantum computation is therefore generally probabilistic. In practice, an algorithm is useful when the probability is sufficiently concentrated on the desired answer. The computation is often repeated to amplify the probability of obtaining the correct result, as we shall see in concrete examples.

Several remarks are worth emphasizing:

1. Replacing qubits by higher-dimensional systems such as qutrits changes the elementary gate set but not the basic circuit model.
2. Allowing measurements at intermediate stages does not fundamentally change the computational model when classical feed-forward and suitable ancillas are available.
3. Measuring in another orthonormal basis is equivalent to applying a unitary change of basis followed by a computational-basis measurement. Thus such measurements can be absorbed into the circuit description. They may, however, affect the resource complexity of a particular implementation.
4. Likewise, starting from a different fixed input state is equivalent to preparing that state from $|0 \cdots 0\rangle$ by a unitary circuit. The cost of this preparation must of course be included when analyzing complexity.
5. Other universal quantum gate sets are also possible.
6. Unitary quantum evolution is reversible. Before measurement, no information is discarded by the ideal circuit, and the evolution itself is represented by an invertible operator.

7. Any reversible classical operation can be represented as a unitary quantum operation. Indeed,

$$\tilde{f}(x_1...x_n, y) = (x_1...x_n, y \oplus f(x_1...x_n))$$

induit the unitary

$$U_f|x_1...x_n, y\rangle = |x_1...x_n, y \oplus f(x_1...x_n)\rangle.$$

If the output $f(x_1...x_n)$ has m components, we takes y with m components and the addition modulo 2 (the XOR) is made component by component. It is straightforward to verify that U_f is unitary; equivalently, it preserves inner products.

8. Thus reversible classical computation is naturally contained within the quantum circuit model.
9. A quantum circuit acts linearly on all amplitudes in a superposition of computational-basis states. This feature is sometimes called *quantum parallelism*; it follows from the superposition principle together with the tensor-product structure of composite systems (Section **3.2**). It does not by itself guarantee a computational speedup, because a measurement reveals only limited information. The computational cost is measured by the size of the circuit, while the final measurement generally produces a random outcome whose distribution is determined by the algorithm. In general, one must repeat a certain number of times that the quantum computation to obtain the result voulu with a probability close of 1. This repetition can augmenter the complexity.

9.4 The Deutsch-Jozsa Problem

The Deutsch–Jozsa algorithm is one of the simplest examples of a quantum algorithm that outperforms a deterministic classical procedure in the oracle-query model. Deutsch introduced the original version of the algorithm in his foundational paper[1] in 1985. The algorithm was subsequently generalized by Deutsch and Jozsa (1992) and cast in the form used here by Cleve, Ekert, Macchiavello, and Mosca (1998). This final formulation makes the underlying interference mechanism particularly transparent. The algorithm is now understood as a prototype of a much broader family, developed in subsequent chapters, based on the *quantum Fourier transform* and on *interference between quantum computational paths*. It also provides a particularly clear illustration of how quantum parallelism can be converted into useful information through interference.

Let us first formulate the problem. Consider

$$f : \mathbf{F}_2^n \to \mathbf{F}_2, \qquad (x_1 \dots x_n) \mapsto f(x_1 \dots x_n) \in \{0, 1\}$$

a Boolean function that is promised in advance to be either *constant* or *balanced*. It is constant if it takes the same value for every input $(x_1 \dots x_n)$. There are 2^n possible

[1] *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer* Proc. Roy. Soc of London A **400** pp 97-117 (1985)

inputs. It is *balanced* if it takes the value 0 on exactly half of them, i.e. on 2^{n-1} inputs, and the value 1 on the remaining 2^{n-1} inputs.

The Deutsch–Jozsa problem is an *oracle decision problem*. The function f is not known explicitly; instead, we are given access to a classical *oracle* (Figure **9.1**) that returns $f(x_1 \dots x_n)$ for any submitted input $x_1 \dots x_n$.

Figure 9.1 Classical oracle returning the value of the function f.

The task is to decide whether f is constant or balanced. The number of oracle queries required to make this decision defines the relevant query complexity. The goal is to determine the answer with as few oracle calls as possible.

Consider first a deterministic classical algorithm. In the worst case it requires $2^{n-1} + 1$ oracle queries, which is exponential in the input size n. Indeed, suppose the oracle has returned 0 for each query made so far. After fewer than $2^{n-1} + 1$ queries, these observations are still compatible both with a constant function and with a balanced function whose unqueried inputs contain all the required ones. Only after observing the same value on $2^{n-1} + 1$ distinct inputs can one conclude with certainty that the function is constant, because a balanced function can take either value on at most 2^{n-1} inputs.

Thus a balanced function may be identified after as few as two queries, but the deterministic worst-case complexity is $2^{n-1} + 1$. The important point is that there are unfavorable instances for which an exponential number of oracle queries is necessary classically.

We shall now construct a quantum algorithm that determines whether f is constant or balanced using a single call to the oracle, independently of the particular promised function f. Relative to deterministic classical query complexity, this is an exponential separation.

9.5 The Quantum Oracle

For each input size n, we construct a circuit implementing the algorithm. Its elementary components are Hadamard gates and a *quantum oracle*. We first describe the oracle model.

The quantum oracle is a specified unitary gate (it may, for example, represent a physical device) that performs the following unitary transformation:

$$U_f|x_1 \dots x_n, y\rangle = |x_1 \dots x_n, y \oplus f(x_1 \dots x_n)\rangle$$

This operator acts on an $(n + 1)$-qubit state belonging to the Hilbert space

$$\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \dots \mathbb{C}^2}_{n \text{ times}} \otimes \mathbb{C}^2$$

and maps it to another state in the same Hilbert space. It is therefore represented by a $2^{n+1} \times 2^{n+1}$ unitary matrix.

The oracle may be viewed as a multi-controlled gate, with the first n qubits acting as controls for the target qubit. The corresponding quantum circuit is shown in Figure 9.2.

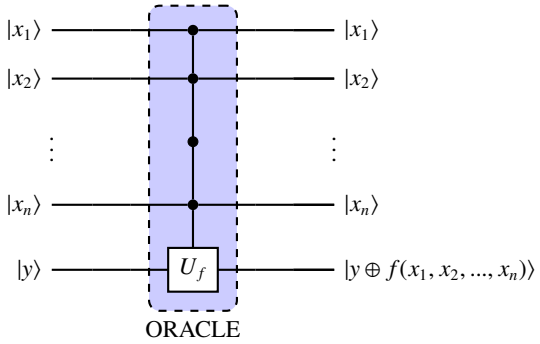


Figure 9.2 The quantum oracle stores the value of f in an auxiliary qubit.

Let us verify that U_f is unitary. It is sufficient to show that it preserves inner products. Consider two computational-basis states

$$U_f|x_1 \dots x_n, y\rangle \quad \text{and} \quad U_f|x'_1 \dots x'_n, y'\rangle$$

and compute their inner product after applying U_f:

$$\begin{aligned}
\langle x'_1 \dots x'_n, y'|U_f^\dagger U_f|x_1 \dots x_n, y\rangle &= \langle x'_1 \dots x'_n, y' \oplus f(x'_1 \dots x'_n)|x_1 \dots x_n, y \oplus f(x_1 \dots x_n)\rangle \\
&= \langle x'_1|x_1\rangle \dots \langle x'_n|x_n\rangle \langle y' + f(x'_1 \dots x'_n)|y + f(x_1 \dots x_n)\rangle \\
&= \delta_{x_1 x'_1} \dots \delta_{x_n x'_n} \langle y' + f(x'_1 \dots x'_n)|y + f(x_1 \dots x_n)\rangle \\
&= \delta_{x_1 x'_1} \dots \delta_{x_n x'_n} \delta_{y' y}
\end{aligned}$$

On the other hand

$$\begin{aligned}
\langle x'_1 \dots x'_n, y'|x_1 \dots x_n, y\rangle &= \langle x'_1|x_1\rangle \dots \langle x'_n|x_n\rangle \langle y'|y\rangle \\
&= \delta_{x'_1 x_1} \dots \delta_{x'_n x_n} \delta_{y' y}
\end{aligned}$$

9.6 Deutsch-Jozsa Quantum Algorithm

The Deutsch–Jozsa quantum circuit is shown in Figure 9.3. It is initialized at time t_0 in the state

$$\underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{n \text{ times}} \otimes |0\rangle = |\Psi_{in}\rangle$$

and terminates with a measurement of the first n qubits in the computational basis. The corresponding projectors are

$$P(b_1 \dots b_n) = |b_1 \dots b_n\rangle\langle b_1 \dots b_n|$$

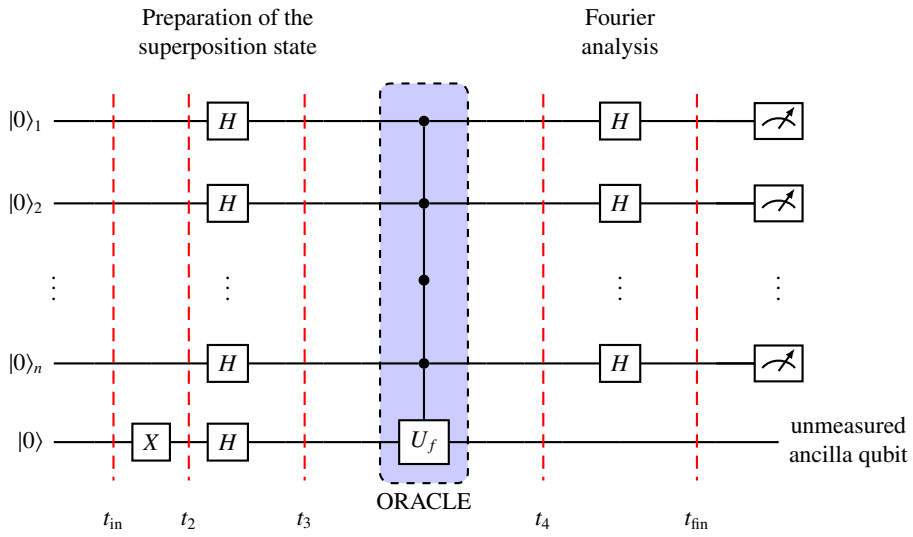


Figure 9.3 Quantum circuit for the Deutsch–Jozsa algorithm.

We now follow the state through the circuit at the successive times t_{in}, t_2, t_3, t_4, and t_{fin}. The final state is

$$|\Psi_{\text{fin}}\rangle = U(t_{\text{fin}}, t_{\text{in}})|\Psi_{\text{in}}\rangle = U(t_{\text{fin}}, t_4)U(t_4, t_3)U(t_3, t_2)U(t_2, t_{\text{in}})|\Psi_{\text{in}}\rangle$$

The unitary operation associated with each stage is

$$\begin{aligned}
U(t_2, t_{\text{in}}) &= (\underbrace{\mathbb{1} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{n \text{ times}}) \otimes X \\
U(t_3, t_2) &= (\underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}}) \otimes H \\
U(t_4, t_3) &= U_f \\
U(t_{\text{fin}}, t_4) &= (\underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}}) \otimes \mathbb{1}
\end{aligned}$$

State at time t_3.

$$
\begin{aligned}
U(t_3,t_2)U(t_2,t_{\text{in}})|\Psi_{\text{in}}\rangle &= \underbrace{(H\otimes H\otimes\cdots\otimes H)}_{n\text{ times}}\otimes HX\ \underbrace{|0\rangle\otimes\cdots\otimes|0\rangle}_{n\text{ times}}\otimes|0\rangle \\
&= \underbrace{(H|0\rangle\otimes H|0\rangle\otimes\cdots\otimes H|0\rangle)}_{n\text{ times}}\otimes HX|0\rangle \\
&= \left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\cdots\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)\otimes H|1\rangle \\
&= \left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\cdots\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\
&= \left(\frac{1}{2^{\frac{n}{2}}}\sum_{b_1\ldots b_n}|b_1\ldots b_n\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\equiv|\Psi_{t_3}\rangle
\end{aligned}
$$

At this stage, the first register is an equal coherent superposition of all possible classical inputs. The final qubit is the ancilla state $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, chosen so that the oracle value is transferred to a phase by phase kickback.

State at time t_4.

$$
\begin{aligned}
U(t_4,t_3)|\Psi_{t_3}\rangle &= U_f\frac{1}{2^{\frac{n}{2}}}\sum_{b_1\ldots b_n}|b_1\ldots b_n\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\
&= \frac{1}{2^{\frac{n}{2}}}\sum_{b_1\ldots b_n}\left(\frac{1}{\sqrt{2}}U_f|b_1\ldots b_n,0\rangle-\frac{1}{\sqrt{2}}U_f|b_1\ldots b_n,1\rangle\right) \\
&= \frac{1}{2^{\frac{n}{2}}}\sum_{b_1\ldots b_n}\left(\frac{1}{\sqrt{2}}|b_1\ldots b_n,f(b_1\ldots b_n)\rangle-\frac{1}{\sqrt{2}}|b_1\ldots b_n,\overline{f(b_1\ldots b_n)}\rangle\right)
\end{aligned}
$$

If $f(b_1\ldots b_n)=0$, the term in parentheses is

$$|b_1\ldots b_n\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

whereas if $f(b_1\ldots b_n)=1$ it is

$$|b_1\ldots b_n\rangle\otimes\frac{|1\rangle-|0\rangle}{\sqrt{2}}$$

The state at time t_4 can therefore be written as

$$\left(\frac{1}{2^{\frac{n}{2}}}\sum_{b_1\ldots b_n}(-1)^{f(b_1\ldots b_n)}|b_1\ldots b_n\rangle\right)\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Thus the oracle has converted the value of f into a relative phase. Each computational-basis input acquires a phase factor $(-1)^{f(b_1\ldots b_n)}$: inputs with $f=0$ acquire phase 0, whereas inputs with $f=1$ acquire phase π. This is the standard *phase-kickback* mechanism.[2]

[2] Indeed, $e^{i0}=1$ and $e^{i\pi}=-1$.

State at time t_{fin}. Finally we apply $\underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}} \otimes \mathbb{1}$. By linearity,

$$|\Psi_{\text{end}}\rangle = \left(\frac{1}{2^{\frac{n}{2}}} \sum_{b_1 \ldots b_n} (-1)^{f(b_1 \ldots b_n)} H|b_1\rangle \otimes \cdots \otimes H|b_n\rangle \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Using

$$H|b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b |1\rangle \right) = \frac{1}{\sqrt{2}} \sum_{c=0,1} (-1)^{cb} |c\rangle$$

we obtain

$$\begin{aligned} H|b_1\rangle \otimes \cdots \otimes H|b_n\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{b_1} |1\rangle \right) \otimes \cdots \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{b_n} |1\rangle \right) \\ &= \frac{1}{\sqrt{2}} \sum_{c_1=0,1} (-1)^{c_1 b_1} |c_1\rangle \otimes \cdots \otimes \sum_{c_n=0,1} (-1)^{c_n b_n} |c_n\rangle \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{c_1 \ldots c_n} (-1)^{\sum_{i=1}^n b_i c_i} |c_1 \ldots c_n\rangle \end{aligned}$$

Therefore

$$|\Psi_{\text{end}}\rangle = \sum_{c_1 \ldots c_n} \left\{ \frac{1}{2^n} \sum_{b_1 \ldots b_n} (-1)^{f(b_1 \ldots b_n)} (-1)^{\sum_{i=1}^n b_1 c_i} \right\} |c_1 \ldots c_n\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

The final state is again a coherent superposition of computational-basis states, with amplitudes

$$\frac{1}{2^n} \sum_{b_1 \ldots b_n} (-1)^{f(b_1 \ldots b_n)} (-1)^{\sum_{i=1}^n b_i c_i}$$

These amplitudes contain information about the function f. If all amplitudes were directly accessible, they would determine f. However, a quantum experiment gives us access only to the state as a whole; to extract classical information from it, we must perform a measurement.

Last Step of the Algorithm: Measurement

We now apply the measurement postulate. Measuring the first n qubits in the computational basis $\{|c_1 \ldots c_n\rangle : c_i \in \{0, 1\}\}$ projects the state onto one of the basis states $|c_1 \ldots c_n\rangle$ with probability given by the Born rule:

$$\begin{aligned} \mathbb{P}\,[c_1 \ldots c_n] &= [\text{squared modulus of the amplitude of } |c_1 \ldots c_n\rangle] \\ &= \frac{1}{2^{2n}} \left| \sum_{b_1 \ldots b_n} (-1)^{f(b_1 \ldots b_n)} (-1)^{\sum_{i=1}^n c_i b_i} \right|^2 \end{aligned}$$

A single run therefore produces one bit string $c_1 \ldots c_n$, and the particular outcome cannot in general be predicted. If the experiment is repeated on identically prepared states,

the empirical frequency of each outcome $|c_1 \dots c_n\rangle$ approaches the corresponding probability $\mathbb{P}[c_1 \dots c_n]$.

Let us evaluate this probability. If f is constant,

$$\begin{aligned}
\mathbb{P}[c_1 \dots c_n] &= \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} (-1)^{\sum_{i=1}^n c_i b_i} \right|^2 \\
&= \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} \prod_{i=1}^n (-1)^{c_i b_i} \right|^2 \\
&= \frac{1}{2^{2n}} \left| \prod_{i=1}^n \left((-1)^{c_i 0} + (-1)^{c_i 1} \right) \right|^2 \\
&= \begin{cases} 1 & \text{if } (c_1 \dots c_n) = (0 \dots 0) \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

Thus, when f is constant, the outcome $(0 \dots 0)$ is obtained with probability one in a single run. If f is balanced, on the other hand,

$$\mathbb{P}[0 \dots 0] = \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} (-1)^{f(b_1 \dots b_n)} \right|^2 = 0$$

and the outcome $(0 \dots 0)$ never occurs.

Consequently, observing $(0 \dots 0)$ implies that f is constant, whereas any other outcome implies that f is balanced.

Remarkably, the Deutsch–Jozsa algorithm requires only one call to the quantum oracle. This is unusual: in algorithms such as Shorś, the quantum procedure is typically repeated several times to obtain a sufficiently high probability of success.

Note on complexity. It is useful to distinguish the complexity of the circuit from the query complexity of the algorithm. For circuits, we shall use two elementary measures: *depth* and *width*. The circuit size may then be characterized, for this discussion, by their product. The Deutsch–Jozsa circuit contains three nontrivial sequential layers, so its depth is $3 = O(1)$. If an elementary quantum gate requires time τ, the ideal circuit execution time is therefore of order 3τ.

The width is the number of input and ancillary qubits, here $n + 1$. The circuit size is therefore $3(n + 1) = O(n)$.

From the oracle-query point of view, the decisive feature is that the problem is solved with a single call to U_f. Thus the quantum query complexity is $O(1)$, whereas the circuit itself has width $O(n)$.

9.7 Some Remarks on Experimental Implementations

We return to experimental implementations near the end of the course. This subsection may be skipped on a first reading.

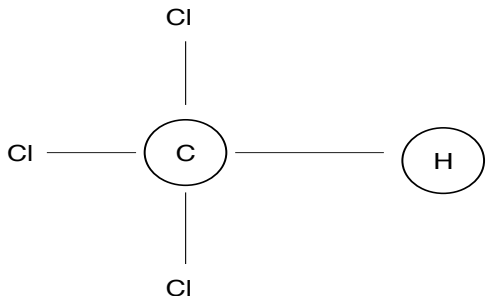


Figure 9.4 An NMR implementation of the Deutsch–Jozsa algorithm using $CHCl_3$. The two qubits are encoded in the nuclear spins of the hydrogen and carbon atoms.

The Deutsch–Jozsa algorithm was among the first quantum algorithms to be demonstrated experimentally. An implementation for $n = 1$ was reported around 2001 using nuclear magnetic resonance (NMR). The experiment used liquid $CHCl_3$ (chloroform; see Figure **9.4**). For $n = 1$, two qubits are required: one input qubit and one ancillary qubit. They can be encoded in the nuclear spins of the hydrogen and carbon atoms. Hadamard gates and the oracle can be implemented by radio-frequency pulses that selectively manipulate these nuclear spins.

One practical difficulty is preparing the molecular ensemble sufficiently close to the desired initial state $|00\rangle$. At finite temperature, thermal populations of unwanted states cannot be completely eliminated.

Increasing n requires molecules with more addressable nuclear spins. This creates a scalability problem: as molecular complexity grows, the spectrum becomes increasingly crowded, and selective control of individual qubits by radio-frequency transitions becomes progressively more difficult.

More recently, Deutsch–Jozsa-type demonstrations have also been performed using trapped ions and cavity-QED platforms. Such early experiments were necessarily limited to small numbers of qubits.

10 Simon's algorithm

This chapter introduces Simon's algorithm, which already contains several of the key ideas that reappear in Shor's algorithm (Chapter **11**). Shor's algorithm may in fact be viewed as a more elaborate instance of the same general hidden-period paradigm.

Simon's problem is an oracle problem for which every classical randomized algorithm requires exponentially many queries, whereas a quantum randomized algorithm solves it using polynomial time and polynomial space. It therefore provides a rigorous example of an exponential quantum speedup in the query model. This does not by itself prove an exponential advantage for ordinary computational problems without an oracle, but it gives strong motivation for the algorithmic ideas developed in the following chapters.

10.1 Simon's Problem

We are given a function of n Boolean variables,

$$f : \mathbf{F}_2^n \to X, \qquad (x_1 \dots x_n) \mapsto f(x_1 \dots x_n),$$

where X is a finite set, with the promise that

$$f(x_1 \dots x_n) = f(y_1 \dots y_n) \;\Leftrightarrow\; \vec{x} = \vec{y} \;\text{ or }\; \vec{x} - \vec{y} = \vec{d}$$

for some fixed nonzero vector $\vec{d}$. Thus each input $\vec{x}$ has a unique partner $\vec{x} + \vec{d}$ with the same function value. Inputs belonging to different pairs give different outputs. The 2^n inputs therefore split into 2^{n-1} equivalence classes of size two[1], so necessarily $|X| = 2^{n-1}$. An example is shown in Figure **10.1**.

[1] The equivalence relation is $\vec{x} \sim \vec{y}$ if and only if $f(\vec{x}) = f(\vec{y})$.

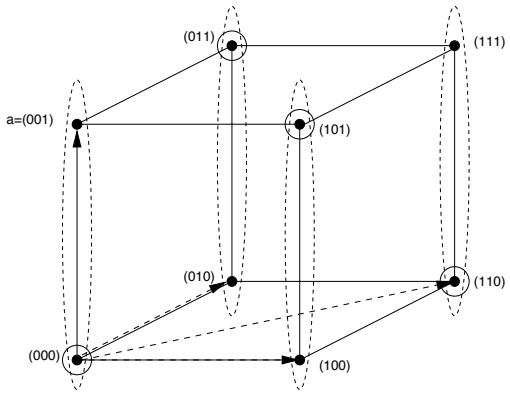


Figure 10.1 Simon's problem for $n = 3$, with hidden vector $\vec{a} = (0, 0, 1)$. Each ellipse represents an equivalence class on which f is constant. The circled points are arbitrary representatives of the classes. The quantum circuit returns vectors orthogonal to $\vec{a}$.

The classical problem is therefore the following. We are given oracle access to

$$\vec{x} \longrightarrow \boxed{f} \longrightarrow f(\vec{x})$$

and must determine $\vec{a}$ by querying the oracle. A deterministic classical algorithm is guaranteed to find $\vec{a}$ after at most $2^{n-1} + 1$ queries, while in the best case two queries suffice. In general, however, the required number of queries is exponential in n.

Consider the following randomized classical strategy:

1. Choose q unordered pairs $(\vec{x}_1^{(1)}, \vec{x}_2^{(1)}), \ldots, (\vec{x}_1^{(q)}, \vec{x}_2^{(q)})$ uniformly at random, with distinct elements inside each pair, and query the oracle on all inputs.
2. If, for some i, $f(\vec{x}_1^{(i)}) = f(\vec{x}_2^{(i)})$, output $\vec{a} = \vec{x}_1^{(i)} - \vec{x}_2^{(i)}$ and declare SUCCESS.
3. If no collision is observed, declare FAILURE.

Let us estimate the number of queries required to obtain success probability at least $1 - \epsilon$. By the union bound,

$$\mathbb{P}\,[\text{SUCCESS}] \leq \sum_i \mathbb{P}\left[f(\vec{x}_1^{(i)}) = f(\vec{x}_2^{(i)})\right].$$

For each pair, the probability of a collision is $\frac{1}{2^n-1}$: among the $\frac{2^n(2^n-1)}{2}$ unordered pairs of distinct inputs, exactly 2^{n-1} pairs have the same function value. Therefore

$$\mathbb{P}\,[\text{SUCCES}] \leq \frac{q}{2^n - 1}$$

Requiring $\mathbb{P}\,[\text{SUCCESS}] \geq 1 - \epsilon$ therefore implies

$$q \geq (1 - \epsilon)(2^n - 1). \tag{10.1}$$

For fixed ϵ, this particular classical procedure requires an exponential number of oracle queries.

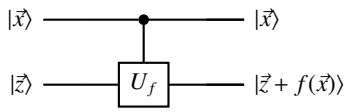
In fact, one can prove that every randomized classical algorithm for Simon's problem

requires an exponential number of oracle queries in the worst case[2]. Thus the simple argument above captures the essential classical difficulty of the problem.

By contrast, Simon's quantum algorithm uses a quantum oracle and determines $\vec{a}$ with success probability at least $1 - \epsilon$ in polynomial time, $O(|\ln \epsilon|\ \mathrm{poly}(n))$. As usual in the query model, the internal cost of implementing the oracle is not counted. The quantum oracle is represented by the unitary operator

$$U_f|\vec{x}, \vec{z}\rangle = |\vec{x}, \vec{z} + f(\vec{x})\rangle.$$

Since f takes 2^{n-1} distinct values, an $(n-1)$-qubit register is sufficient to encode its output and therefore also $\vec{z}$.



The same quantum circuit solves a slightly more general problem. Regard $\mathbf{F}_2^n$ as the vector space of binary vectors with n components, and let $H \subseteq \mathbf{F}_2^n$ be a k-dimensional subspace. If $\mathbf{F}_2^n$ were replaced by $\mathbb{R}^n$, one could visualize H as a k-dimensional plane through the origin, as in Figure **10.2**.

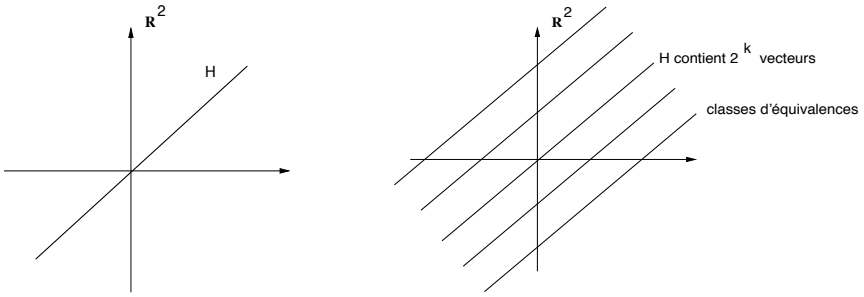


Figure 10.2 Left: the subspace H (illustrated in $\mathbb{R}^n$). Right: the affine cosets of H on which f is constant.

Assume access to an oracle that computes

$$f : \mathbf{F}_2^n \to X, \qquad \vec{x} \mapsto f(\vec{x})$$

such that $f(\vec{x}) = f(\vec{y}) \Leftrightarrow \vec{x} - \vec{y} \in H$. The original Simon problem corresponds to the one-dimensional subspace $H = \{0, \vec{a}\}$ generated by $\vec{a}$. The generalized problem is to determine a basis of H using as few oracle queries as possible. If $\dim H = k$, then H contains 2^k binary vectors, since every element can be written as $b_1\vec{h}_1 + \cdots + b_k\vec{h}_k$ with $b_i \in \{0, 1\}$. The cosets of H partition $\mathbf{F}_2^n$ into 2^{n-k} disjoint classes, and f takes one

[2] See A. Y. Kitaev, A. H. Shen, M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics vol. 47, American Mathematical Society (2002), p. 117.

distinct value on each coset. Therefore

$$|X| = \frac{2^n}{2^k} = 2^{n-k}.$$

10.2 Quantum Circuit for Simon's Algorithm

The circuit is shown in Figure **10.3**. Its width is $2n-k$ and its depth, excluding the oracle implementation, is constant. Hence its size is $O(n)$. We now follow the quantum state through the circuit.

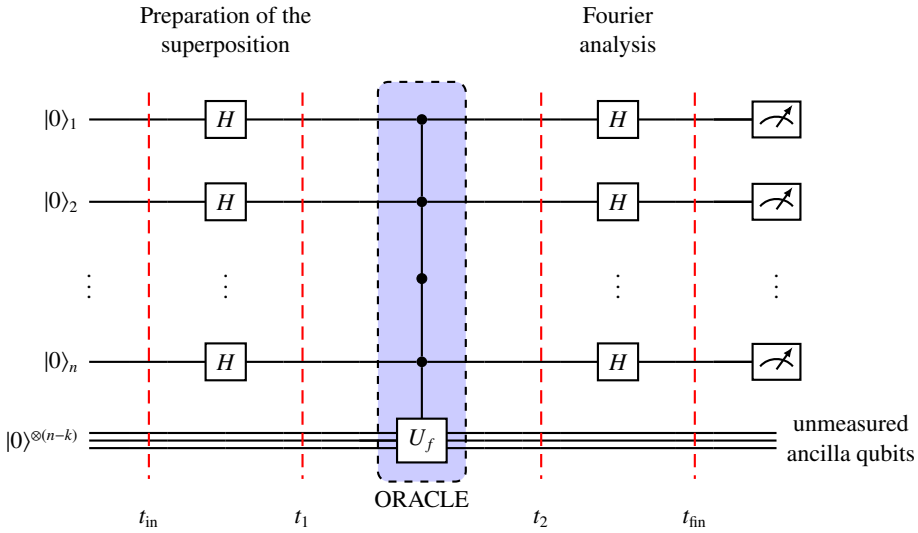


Figure 10.3 Quantum circuit for Simon's algorithm. The circuit uses $n + (n - k)$ qubits. The $n - k$ auxiliary qubits are not measured.

The initial state at time t_{in} is

$$|\Psi_{\text{in}}\rangle = \underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{n \text{ qubits}} \otimes \underbrace{|\vec{0}\rangle}_{n-k \text{ qubits}}$$

At time t_1, the state is

$$\begin{aligned} U(t_1, t_{\text{in}})|\Psi_{\text{in}}\rangle &= \Big(\underbrace{H \otimes \ldots \otimes H}_{n \text{ fois}} \otimes \mathbb{1}_{n-k}\Big) \underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{n \text{ qubits}} \otimes \underbrace{|\vec{0}\rangle}_{n-k \text{ qubits}} \\ &= H|0\rangle \otimes \ldots \otimes H|0\rangle \otimes |\vec{0}\rangle \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{x_1 \ldots x_n} |x_1 \ldots x_n, \vec{0}\rangle \end{aligned}$$

To obtain the state at time t_2, we apply the oracle, $U(t_2, t_1) = U_f$:

$$\begin{aligned} U(t_2,t_1)U(t_1,t_{\text{in}})|\Psi_{\text{in}}\rangle &= \frac{1}{2^{\frac{n}{2}}}\sum_{x_1\ldots x_n} U_f|x_1\ldots x_n,\vec{0}\rangle \\ &= \frac{1}{2^{\frac{n}{2}}}\sum_{x_1\ldots x_n}|x_1\ldots x_n, f(x_1\ldots x_n)\rangle \end{aligned}$$

Before proceeding, it is useful to reorganize this sum. Every vector $\vec{x} \in \mathbf{F}_2^n$ can be written uniquely as

$$\vec{v} + \vec{h},$$

where $\vec{h} \in H$ and $\vec{v}$ is a chosen representative of one of the 2^{n-k} cosets of H in $\mathbf{F}_2^n$ (see Figure **10.2**). In what follows, $\sum_{\vec{v}}$ denotes a sum over one representative from each coset. Hence

$$\begin{aligned} U(t_2,t_1)|\Psi_{\text{in}}\rangle &= \frac{1}{2^{\frac{n}{2}}}\sum_{\vec{v}}\sum_{\vec{h}\in H}|\vec{v}+\vec{h}, f(\vec{v}+\vec{h})\rangle \\ &= \frac{1}{2^{\frac{n}{2}}}\sum_{\vec{v}}\sum_{\vec{h}\in H}|\vec{v}+\vec{h}, f(\vec{v})\rangle \end{aligned}$$

where we used $f(\vec{v}+\vec{h}) = f(\vec{v})$. It remains to apply the final Hadamard transform to the first register:

$$U(t_{\text{end}},t_{\text{in}})|\Psi_{\text{in}}\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{\vec{v}}\sum_{\vec{h}\in H} H^{\otimes n}\otimes \mathbb{1}_{n-k}|\vec{v}+\vec{h}, f(\vec{v})\rangle.$$

Using

$$\begin{aligned} H^{\otimes n}|\vec{v}+\vec{h}\rangle &= H|v_1+h_1\rangle\otimes\ldots\otimes H|v_n+h_n\rangle \\ &= \frac{1}{2^{\frac{n}{2}}}\left(|0\rangle+(-1)^{v_1+h_1}|1\rangle\right)\otimes\ldots\otimes\left(|0\rangle+(-1)^{v_n+h_n}|1\rangle\right) \\ &= \frac{1}{2^{\frac{n}{2}}}\sum_{y_1\ldots y_n}(-1)^{\sum_{i=1}^n (v_i+h_i)y_i}|y_1\ldots y_n\rangle \end{aligned}$$

The final state, before measurement, is

$$\begin{aligned} |\Psi_{\text{fin}}\rangle &= \frac{1}{2^n}\sum_{\vec{v}}\sum_{\vec{h}\in H}\sum_{\vec{y}\in\mathbf{F}_2^n}(-1)^{(\vec{v}+\vec{h})\cdot\vec{y}}|\vec{y}\rangle\otimes|f(\vec{v})\rangle \\ &= \frac{1}{2^n}\sum_{\vec{v}}\sum_{\vec{y}\in\mathbf{F}_2^n}(-1)^{\vec{v}\cdot\vec{y}}|\vec{y}\rangle\otimes|f(\vec{v})\rangle\left\{\sum_{\vec{h}\in H}(-1)^{\vec{h}\cdot\vec{y}}\right\} \end{aligned}$$

If $\vec{y} \in H^\perp$ (where[3]), then

$$\sum_{\vec{h}\in H}(-1)^{\vec{h}\cdot\vec{y}} = \sum_{\vec{h}\in H} 1 = |H| = 2^k.$$

[3] By definition $H^\perp = \{\vec{y} \mid \vec{y}\cdot\vec{h} \equiv 0 \mod 2 \quad \forall \vec{h} \in H\}$

If instead $\vec{y} \notin H^\perp$, there exists a nonzero $\vec{h}_0 \in H$ such that

$$\vec{y} \cdot \vec{h_0} \neq 0 \mod 2.$$

With the change of variables $\vec{h} = \vec{h'} + \vec{h}_0$, we obtain

$$\begin{aligned}\sum_{\vec{h}\in H}(-1)^{\vec{h}\cdot\vec{y}} &= \sum_{\vec{h'}\in H}(-1)^{(\vec{h'}+\vec{h_0})\cdot\vec{y}} \\ &= (-1)^{\vec{h_0}\cdot\vec{y}}\sum_{\vec{h'}\in H}(-1)^{\vec{h'}\cdot\vec{y}}\end{aligned}$$

Because $\vec{y}\cdot\vec{h}_0 = 1$ in $\mathbf{F}_2$, we have $(-1)^{\vec{h}_0\cdot\vec{y}} = -1$. Therefore

$$\sum_{\vec{h}\in H}(-1)^{\vec{h}\cdot\vec{y}} = 0 \quad \text{for} \quad \vec{y} \notin H^\perp.$$

Consequently, only vectors $\vec{y} \in H^\perp$ contribute to the final state, which can be written as

$$|\Psi_{\text{end}}\rangle = \frac{1}{2^{n-k}}\sum_{\vec{y}\in H^\perp}\sum_{\vec{v}}(-1)^{\vec{v}\cdot\vec{y}}|\vec{y}\rangle \otimes |f(\vec{v})\rangle$$

At this stage the quantum circuit has prepared $|\Psi_{\text{fin}}\rangle$. To extract classical information, we measure the first n qubits in the computational basis. The corresponding projectors are

$$P_{\vec{y}} = |\vec{y}\rangle\langle\vec{y}| \otimes \mathbb{1}_{n-k},$$

where the identity indicates that the $n-k$ auxiliary qubits are not measured. Conditioned on outcome $\vec{y}$, the post-measurement state is

$$\frac{P_{\vec{y}}|\Psi_{\text{end}}\rangle}{\|P_{\vec{y}}|\Psi_{\text{end}}\rangle\|},$$

with probability

$$\mathbb{P}\left[\vec{y}\right] = \langle\Psi_{\text{end}}|P_{\vec{y}}|\Psi_{\text{end}}\rangle.$$

- If $\vec{y} \notin H^\perp$ we have,

$$P_y|\Psi_{\text{fin}}\rangle = 0$$

  Therefore

$$\mathbb{P}\left[\vec{y}\right] = 0 \quad \text{if} \quad \vec{y} \notin H^\perp$$

- If $\vec{y} \in H^\perp$ we have,

$$\begin{aligned}P_{\vec{y}}|\Psi_{\text{fin}}\rangle &= \frac{1}{2^{n-k}}\sum_{\vec{y'}\in H^\perp}\sum_{\vec{v}}(-1)^{\vec{v}\cdot\vec{y'}}|\vec{y}\rangle\,\langle\vec{y}|\vec{y'}\rangle \otimes |f(\vec{v})\rangle \\ &= |\vec{y}\rangle \otimes \frac{1}{2^{n-k}}\sum_{\vec{v}}(-1)^{\vec{v}\cdot\vec{y}}|f(\vec{v})\rangle\end{aligned}$$

It follows that

$$\mathbb{P}[\vec{y}] = \frac{1}{2^{n-k}} \sum_{\vec{y} \in H^\perp} \sum_{\vec{v}} (-1)^{\vec{v}\cdot\vec{y}} \langle \vec{y} | \vec{y} \rangle \sum_{\vec{v}} (-1)^{\vec{v}\cdot\vec{y}} \langle f(\vec{v}) | f(\vec{v}) \rangle$$
$$= \begin{cases} \frac{1}{2^{n-k}} & \text{if} \quad \vec{y} \in H^\perp \\ 0 & \text{if} \quad \vec{y} \notin H^\perp. \end{cases}$$

Thus the measurement outcome is uniformly distributed over $H^\perp$.

10.3 Probabilistic Analysis of the Algorithm

We analyze the following randomized version of the algorithm:

1. Initialize the circuit in $|0_n\rangle \otimes |0_{n-k}\rangle$ and make one query to the quantum oracle.
2. Measure the first register of the final state $|\Psi_{\text{fin}}\rangle$. The outcome is a vector $\vec{y} \in H^\perp$.
3. Repeat steps 1 and 2 a total of $n-k$ times to obtain vectors $\vec{y}_1, \ldots, \vec{y}_{n-k} \in H^\perp$.
4. If these vectors are linearly independent, they form a basis of $H^\perp$. Compute a basis $\vec{h}_1, \ldots, \vec{h}_k$ of H by standard linear-algebra methods, for example Gaussian elimination, and output SUCCESS together with this basis.
5. If the sampled vectors are linearly dependent, output FAILURE.

We now show that one round of steps 1–5 succeeds with probability at least $\frac{1}{4}$. It is enough to prove that if $n-k$ vectors are sampled independently and uniformly from $H^\perp$, then

$$\mathbb{P}[\vec{y}_1, \ldots, \vec{y}_{n-k} \text{ independent}] \geq \frac{1}{4}.$$

Proof. The first vector must be nonzero, which occurs with probability $\frac{2^{n-k}-1}{2^{n-k}}$. Given a nonzero $\vec{y}_1$, the second vector must lie outside $\text{span}\{\vec{y}_1\}$, which has two elements; this occurs with probability $\frac{2^{n-k}-2}{2^{n-k}}$. Similarly, after j linearly independent vectors have been chosen, their span contains 2^j vectors, so the next sample lies outside that span with probability $\frac{2^{n-k}-2^j}{2^{n-k}}$. Multiplying these conditional probabilities gives

$$\mathbb{P}[\vec{y}_1, \ldots, \vec{y}_{n-k} \text{ linearly independent}]$$
$$= \frac{2^{n-k}-2^0}{2^{n-k}} \cdot \frac{2^{n-k}-2^1}{2^{n-k}} \cdot \frac{2^{n-k}-2^2}{2^{n-k}} \cdot \cdots \cdot \frac{2^{n-k}-2^{m-k-1}}{2^{n-k}}$$
$$= \prod_{j=1}^{n-k} \left(1 - \frac{1}{2^j}\right) = \exp\Big(\sum_{j=1}^{n-k} \ln\{1 - \frac{1}{2^j}\}\Big)$$

Using $\ln(1-x) \geq -2(\ln 2)x$ for $0 \leq x \leq \frac{1}{2}$ (see Figure **10.4**), we obtain the lower bound

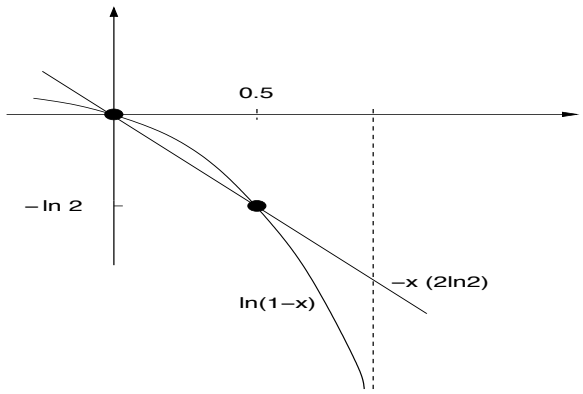


Figure 10.4 A useful inequality.

$$\begin{aligned} &\geq \exp\{-(2\ln 2)\sum_{j=1}^{n-k}\frac{1}{2^j}\} \\ &\geq \exp\{-(2\ln 2)\sum_{j=1}^{\infty}\frac{1}{2^j}\} \\ &= \exp(-2\ln 2) = \frac{1}{4} \end{aligned}$$

Since a single round succeeds with probability at least $\frac{1}{4}$, the probability of obtaining at least one successful round among T independent repetitions is

$$\begin{aligned} \mathbb{P}\,[\text{at least one success in } T \text{ rounds}] &= 1-(1-\mathbb{P}\,[\text{success in one round}])^T \\ &\geq 1-\left(1-\frac{1}{4}\right)^T = 1-\left(\frac{3}{4}\right)^T. \end{aligned}$$

This is at least $1-\epsilon$ if and only if

$$1-\left(\frac{3}{4}\right)^T \geq 1-\epsilon,$$

that is,

$$T \geq \frac{|\ln \epsilon|}{|\ln(3/4)|}.$$

In summary, a success probability of at least $1-\epsilon$ is achieved with $O(|\ln \epsilon|)$ rounds. Each round requires $O(n)$ operations for the repeated quantum sampling and $O\left(n^3\right)$ classical operations to compute the dual basis. The overall running time is therefore $O\left(|\ln \epsilon|\, n^3\right)$, while the quantum circuit itself has size $O(n)$.

Note on Computing the Dual Basis

Let $\vec{y}_1, \ldots, \vec{y}_{n-k}$ be a basis of $H^\perp$ obtained by the algorithm. A vector $\vec{h}$ belongs to H if and only if it is orthogonal to every basis vector of $H^\perp$, i.e. if it satisfies

$$\begin{aligned} \vec{h}^T \cdot \vec{y}_1 &= 0 \\ &\vdots \\ \vec{h}^T \cdot \vec{y}_{n-k} &= 0 \end{aligned}$$

Equivalently,

$$\vec{h}^T \cdot \underbrace{[\vec{y}_1 \ldots \vec{y}_{n-k}]}_{n \times (n-k) \text{ matrix of column vectors}} = 0.$$

Thus $\vec{h}$ lies in the kernel of a matrix of rank $n - k$. By the rank–nullity theorem,

$$\dim(\ker A) + \dim(\operatorname{im} A) = n,$$

so $\dim(\ker A) = k$. Hence the system has k linearly independent solutions $\vec{h}_1, \ldots, \vec{h}_k$, which form a basis of H. They can be found by Gaussian elimination, requiring $O\left(n^3\right)$ elementary operations in general.

11 Factorization and Shor's Algorithm

One of the most striking developments in quantum computation is Shorś algorithm, a polynomial-time quantum algorithm for integer factorization.

The fundamental theorem of arithmetic states that every integer N has a unique factorization into prime numbers. Given the factors of N, verifying their product is easy. For example, suppose that $N = p \cdot q$ with p and q prime numbers represented by $O(b)$ bits. If p and q are known, checking $N = pq$ requires only polynomial time, for example $O(b^2)$ elementary arithmetic operations. By contrast, no polynomial-time classical algorithm is known for factoring a general b-bit integer N; indeed, it is not known whether such a classical algorithm exists. There are classical algorithms substantially faster than naive exponential search. The asymptotically fastest general-purpose methods are subexponential in N, but they remain costly for sufficiently large integers. As a concrete illustration, the factorization of RSA-768, a 768-bit (232-decimal-digit) integer announced in December 2009, required a large distributed classical computation.

Shorś algorithm factors integers in polynomial time using a quantum circuit of polynomial size. More precisely, it reduces factorization to another number-theoretic problem called *order finding*. The reduction of factorization to order finding was known classically well before Shorś work; the quantum contribution is an efficient algorithm for the order-finding step.

To analyze Shorś algorithm we shall also need a few elementary facts about continued fractions and Eulerś totient function. We introduce these tools, together with the reduction from factorization to order finding, in the following section.

11.1 A Short Digression on Number Theory

Factorization Based on Order Finding

Let $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with $p_i \neq 2$ and $k \geq 2$. Thus N has no factor of 2 and is not a power of a single prime. Factors of 2 are trivial to extract by repeated division. Prime powers $N = p^e$ can also be recognized and treated efficiently by classical preprocessing. We therefore focus on the nontrivial case above.

Factorization algorithm based on order finding.

a. Choose $a \in \{2, \dots, N-1\}$ uniformly at random and compute $d = \mathrm{PGCD}(a, N)$ using Euclid's algorithm, whose bit complexity is polynomial in $\log N$.

b. If $d > 1$, then d is a nontrivial factor of N. Record this factor and, if necessary, repeat step **a** to continue the factorization.

c. If $d = 1$, so that a and N are coprime, determine the smallest positive integer r such that $a^r = 1 \pmod N$. This integer is the *order of a modulo N*, denoted $r = \mathrm{Ord}_N(a)$. No polynomial-time classical algorithm is known for this step in general; this is precisely the step accelerated by Shorś quantum algorithm.

d. If r is odd, output `Fail` and return to step **a**.

e. If r is even, use the factorization $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$. Since N divides $a^r - 1$, there are three relevant cases:

e1. If N divides $a^{r/2} - 1$, then $a^{r/2} = 1 \pmod N$, contradicting the minimality of r; this case is impossible. the order.

e2. If N divides $a^{r/2} + 1$, i.e. $a^{r/2} = -1 \pmod N$, output `Fail` and return to step **a**.

e3. Otherwise, N has nontrivial common factors with both $a^{r/2} - 1$ and $a^{r/2} + 1$. For instance, if $N = pq$, one prime factor divides one term and the other prime factor divides the other term. Thus the greatest common divisors

$$d_{\pm} = \mathrm{PGCD}\left(a^{\frac{r}{2}} \pm 1, N\right)$$

are nontrivial factors of N. They can again be computed efficiently with Euclid's algorithm.

f. Check whether the factors found so far multiply to N; if not, return to step **a**.

If an oracle could solve step **c**, the computational cost of one round would be polynomial and dominated by classical arithmetic such as Euclid's algorithm. The procedure is probabilistic because of the random choice in step **a**, so we must also show that the success probability is bounded away from zero. In fact one can prove $\mathbb{P}[\text{success}] \geq \frac{3}{4}$. Repeating the round independently therefore amplifies the success probability exponentially fast. After $T = O(|\ln \epsilon|)$ rounds, the overall success probability is at least $1 - \epsilon$.

Within a round, failure occurs only in steps **d** and **e2**, corresponding to the event

$$(r \text{ is odd}) \text{ or } (a^{\frac{r}{2}} = -1 \pmod N)$$

Thus

$$\mathbb{P}[\text{failure}] = \mathbb{P}\left[(r \text{ is odd}) \text{ or } (a^{\frac{r}{2}} = -1 \pmod N)\right].$$

Theorem. Let a be chosen uniformly at random from $\{2, \dots, N-1\}$ subject to $\mathrm{PGCD}(a, N) = 1$, and let r be the smallest positive integer satisfying $a^r = 1 \pmod N$. Then $\mathbb{P}[\text{failure}] \leq \frac{1}{4}$.

We omit the proof. The theorem implies that a single round of the order-finding-based factorization procedure succeeds with probability at least $3/4$. Independent repetitions can therefore raise the success probability to $1 - \epsilon$. The number of rounds required is $O(|\ln \epsilon|)$.

Continued Fractions

We now recall, without proof, several elementary results on continued fractions that will be used later in Shorś algorithm.

Every real number admits a continued-fraction expansion. We restrict attention here to rational numbers and begin with the example $x = 263/189$. The successive steps of Euclid's algorithm for computing PGCD $(263, 189)$ are

$$\begin{aligned} 263 &= 1 \cdot 189 + 74 \\ 189 &= 2 \cdot 74 + 41 \\ 74 &= 1 \cdot 41 + 33 \\ 41 &= 1 \cdot 33 + 8 \\ 33 &= 4 \cdot 8 + 1 \end{aligned}$$

This givesPGCD $(263, 189) = 1$. Since the remainder decreases by at least a constant factor over a bounded number of Euclidean steps, the number of divisions is $O(\log N)$ in general. Each division involves integers with $O(\log N)$ bits, so a simple implementation gives a polynomial bit complexity.

The continued-fraction expansion is obtained by repeatedly inverting the fractional remainder:

$$\frac{263}{189} = 1 + \frac{74}{189} = 1 + \frac{1}{\frac{189}{74}} = 1 + \cfrac{1}{2 + \frac{41}{74}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{\frac{74}{41}}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{33}{41}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\frac{41}{33}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{8}{33}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\frac{33}{8}}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{8}}}}}$$

We write the resulting continued fraction as

$$\frac{263}{189} = [1; 2; 1; 1; 4; 8]$$

The general form is

$$x = [a_0; a_1; \ldots; a_n]$$

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

If $x > 1$, then $a_0 \geq 1$, whereas if $0 < x < 1$, $a_0 = 0$. A finite rational continued fraction has the familiar twofold ambiguity obtained by replacing the last coefficient a_n by $a_n - 1, 1. \frac{1}{(a_n - 1) + \frac{1}{1}}$. Thus

$$x = [a_0; a_1; \ldots; a_{n-1}; a_n] = [a_0; a_1; \ldots; a_{n-1}; a_n - 1; 1]$$

Except for this final-term ambiguity, the continued-fraction expansion is unique. We remove the ambiguity by always choosing the shorter expansion. The number of arithmetic operations required to compute it is the same order as for Euclid's algorithm, $O\big((\log_2 N)^3\big)$, where $N = \max(\text{numerator, denominator})$. The number of coefficients is $O((\log_2 N))$.

Definition: Notion of Convergent. Let $x = [a_0; a_1; a_2; \ldots; a_n]$ be a continued-fraction expansion of x. Its *convergents* are the truncated continued fractions $[a_0; a_1; a_2; \ldots; a_m]$, $1 \leq m \leq n$. Each convergent is a rational number

$$[a_0; a_1; a_2; \ldots; a_m] = \frac{p_m}{q_m}.$$

Theorem: Properties of convergents. Let p_m/q_m denote the convergents of a continued fraction x. Then

a) $\mathrm{PGCD}\,(p_m, q_m) = 1$ (p_m and q_m are coprime) and $\left|x - \frac{p_m}{q_m}\right| \leq \frac{1}{q_m^2}$, so convergents provide particularly good rational approximations.

b) Conversely, every reduced rational approximation p/q satisfying $\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$ occurs among the convergents of x. Such approximations can therefore be found systematically by computing the continued fraction.

Property (b) is the one we shall use in the analysis of Shorś algorithm.

Euler's Function

For an integer $r > 2$, an integer $a \in \{1, 2, \ldots, r-1\}$ is said to be coprime to r if $\mathrm{PGCD}\,(a, r) = 1$. The number of such integers a is given by $\varphi(r)$, the *Euler's totient function*. If $N = p$ is prime, every integer $a = 1, 2, \ldots, p-1$ is coprime to p, and therefore $\varphi(p) = p - 1$. In general, if

$$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

is the unique prime factorization of N, then

$$\begin{aligned}\varphi(N) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1 - 1) p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1)\end{aligned}$$

Example. If $N = 9$, the integers coprime to N are $a = 1, 2, 4, 5, 7, 8$, and hence $\varphi(9) = 6$. Indeed, $\varphi(9) = 3^{2-1}(3 - 1) = 6$.

The following lower bound, valid for sufficiently large r, will be useful:

$$\varphi(r) \geq \frac{r}{4 \ln \ln r}$$

The denominator $\ln \ln r$ grows extremely slowly. For example, even for $r = 10^{1000}$ one has $\ln \ln r < 8$. Thus a non-negligible fraction of the integers below r are coprime to r. This observation will be important when reconstructing the order from a measured rational approximation. Fix r and choose $k \in \{1, 2, \ldots, r\}$ uniformly at random. Then:

$$\mathbb{P}\left[\mathrm{PGCD}\,(k, r) = 1\right] = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln \ln r)} \tag{11.1}$$

The right-hand side decreases only very slowly with r; for complexity estimates we may regard it as a slowly varying inverse-logarithmic factor.

11.2 Period Finding for an Arithmetic Function

As explained above, integer factorization can be reduced probabilistically to the problem of finding an order modulo N. We now turn to the quantum order-finding problem

for a number a chosen uniformly from $\{2, 3, \ldots, N-1\}$. The order $\mathrm{Ord}_N(a)$ is the smallest positive integer r such that

$$a^r = 1 \pmod{N}.$$

Equivalently, we seek the period of the arithmetic function

$$\begin{aligned} f_{a,N} &: \mathbb{Z} \to \mathbb{Z} \\ x &\to f_{a,N}(x) = a^x \pmod{N}. \end{aligned}$$

This period (or order) is the smallest positive integer r such that

$$f_{a,N}(x) = f_{a,N}(x + r), \qquad \forall x \in \mathbb{Z}.$$

We therefore begin with the more general problem of finding the period of an arithmetic function.

Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function with unknown period r, so that

$$f(x) = f(x + r), \qquad \forall x \in \mathbb{Z}.$$

A finite quantum register can represent only finitely many integers, so we restrict the domain to $\mathbb{Z}/M\mathbb{Z} = \{0, 1, 2, \ldots, M-1\}$, with M chosen much larger than r. Although r is unknown, we assume that an upper bound is available and hence that such a choice of M can be made. For order finding, for example, $r < N$, and we shall see that taking $M = O(N^2)$ is sufficient.

We must first encode the integers $x \in \{0, \ldots, M-1\}$ as quantum states. For convenience, take $M = 2^m$. Each integer x then has the binary expansion

$$x = 2^{m-1}x_{m-1} + 2^{m-2}x_{m-2} + \ldots + 2^2 x_2 + 2x_1 + x_0,$$

with m bits,

$$x = \underbrace{(x_{m-1} \ldots x_0)}_{\text{binary representation of } x}.$$

In particular $(0 \ldots 0) = 0$ and $(1 \ldots 1) = 2^m - 1$. The natural Hilbert space is therefore

$$\mathcal{H} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{m \text{ times}},$$

and the integer x is stored in the computational-basis state $|x\rangle \in \mathcal{H}$ of an m-qubit register,

$$|x\rangle = |x_{m-1}\rangle \otimes \ldots \otimes |x_0\rangle = |x_{m-1} \ldots x_0\rangle.$$

As usual, the function f is represented by the unitary operation

$$U_f : |x\rangle \otimes |0\rangle \to U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$$

where $|0\rangle$ and $|f(x)\rangle$ are m-qubit states. In Shorś algorithm we compute $f(x) \bmod N$, so m output qubits are certainly sufficient. We shall also need the *quantum Fourier transform* (Section **11.6**), defined by

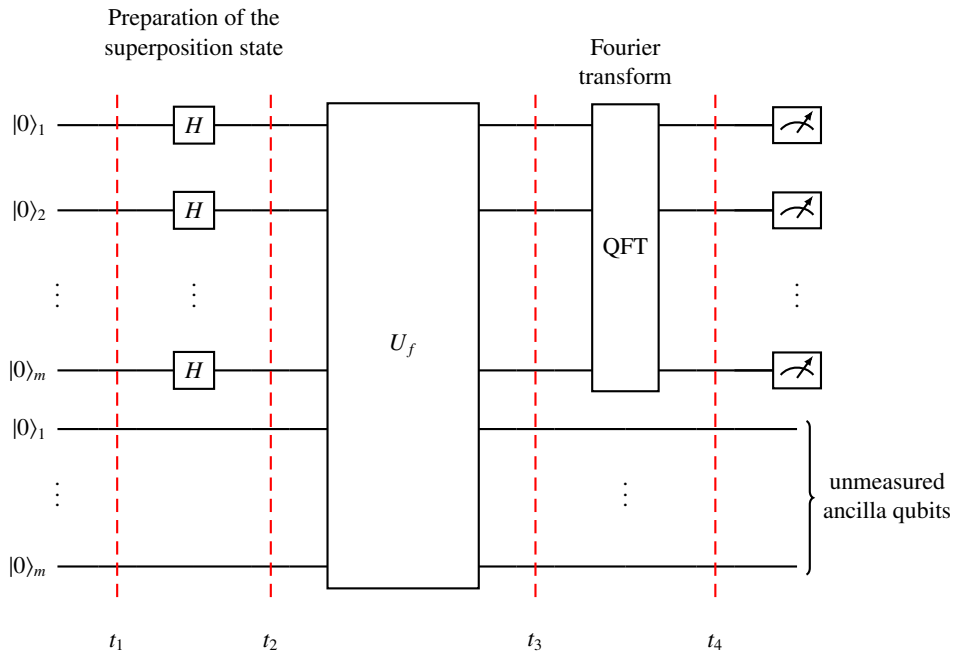


Figure 11.1 Quantum circuit for period finding.

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle = \frac{1}{2^{m/2}} \sum_{\substack{y_0 \dots y_{m-1} \\ \in \{0,1\}^m}} e^{2\pi i \frac{xy}{M}} |y_{m-1} \dots y_0\rangle \tag{11.2}$$

The QFT is linear: if $|\Psi\rangle = \sum_{x=0}^{M-1} c_x |x\rangle$, then

$$QFT|\Psi\rangle = \sum_{x=0}^{M-1} c_x QFT|x\rangle.$$

The QFT is unitary, as required for implementation by a quantum circuit.

11.3 Circuit for Period Finding

The circuit implementing the period-finding algorithm is shown in Figure **11.1**.

The implementation of U_f depends on the particular function. For order finding we use $f(x) = a^x \pmod N$; a circuit for this modular exponentiation is discussed in Section **11.7**. The QFT circuit is described in Section **11.6**.

We now follow the state through the period-finding circuit. At time t_1, the initial state is

$$|0\rangle \otimes |0\rangle = \underbrace{|0\ldots0\rangle}_{m \text{ times}} \otimes \underbrace{|0\ldots0\rangle}_{m \text{ times}}.$$

After the Hadamard gates (t_2), the state is

$$H^{\otimes m} \underbrace{|0\ldots0\rangle}_{m \text{ times}} \otimes |0\rangle^{\otimes m} = \left(\frac{1}{2^{\frac{m}{2}}} \sum_{\substack{x_0 \ldots x_{m-1} \\ \in \{0,1\}^m}} |x_{m-1} \ldots x_0\rangle \right) \otimes |0\rangle^{\otimes m}.$$

This is a coherent superposition of all classical input values. It may be written more compactly as

$$\left(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \right) \otimes |0\rangle^{\otimes m}.$$

After U_f (t_3), we obtain the state:

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle.$$

We now use the periodicity of f to rearrange this sum. The interval $[0, M-1]$ can be partitioned into blocks of length r, except possibly for the final shorter block (Figure **11.2**). The integers in the first period are $x_0 \in \{0, 1, \ldots, r-1\}$. If M were a multiple of

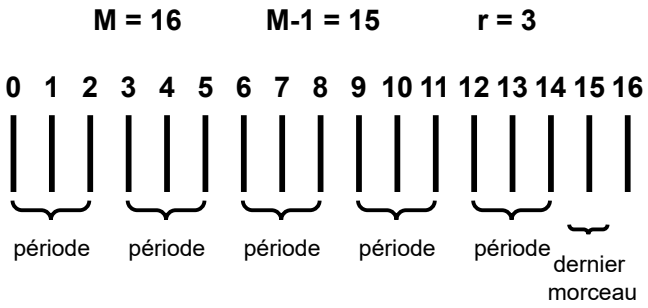


Figure 11.2 Example of decomposition of $\{0, 1, \ldots, M-1\}$ for $r = 3$ and $M = 16$.

r, each x could be written as

$$x = x_0 + jr \text{ with } 0 \leq j \leq \frac{M}{r} - 1.$$

In the general case (see Figure **11.2**), we obtain

$$x = x_0 + jr \text{ with } 0 \le j \le A(x_0) - 1,$$

where $A(x_0)$ is an integer depending on x_0 and satisfying

$$M - r \le x_0 + (A(x_0) - 1)r \le M - 1.$$

We therefore have

$$\begin{aligned}\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle &= \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0 + jr)\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0)\rangle.\end{aligned}$$

Finally, we apply the QFT to this state. The resulting state at time t_4 is

$$\begin{aligned}|\Psi_{\text{fin}}\rangle &= \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} QFT|x_0 + jr\rangle \otimes |f(x_0)\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{(x_0+jr)y}{M}} |y\rangle \otimes |f(x_0)\rangle \\ &= \frac{1}{M} \sum_{x_0=0}^{r-1} \left(\sum_{y=0}^{M-1} \left(e^{2\pi i \frac{x_0 y}{M}} \sum_{j=0}^{A(x_0)-1} e^{2\pi i \frac{jy}{M/r}} \right) |y\rangle \right) \otimes |f(x_0)\rangle.\end{aligned}$$

This last expression is the final state $|\Psi_{\text{fin}}\rangle$ immediately before the measurement.

11.4 The Process of Measurement

It remains to analyze the measurement step. We measure the first register in the computational basis, represented by the set of projectors

$$P_y = |y\rangle\langle y| \otimes \mathbb{1}_{m\times m}, \qquad y \in \{0, 1, 2, \ldots, M-1\}.$$

Immediately after obtaining outcome y, the quantum state is, up to normalization,

$$P_y|\Psi\rangle_{\text{fin}}$$

with probability

$$\mathbb{P}[y] = \langle\Psi_{\text{fin}}|P_y|\Psi_{\text{fin}}\rangle.$$

First compute $P_y|\Psi_{\text{fin}}\rangle$:

$$P_y|\Psi_{\text{fin}}\rangle = \frac{1}{M} \sum_{x_0=0}^{r-1} \left(e^{2\pi i \frac{x_0 y}{M}} \sum_{j=0}^{A(x_0)-1} e^{2\pi i \frac{jy}{M/r}} \right) |y\rangle \otimes |f(x_0)\rangle.$$

Then $\langle\Psi_{\text{fin}}|P_y|\Psi_{\text{fin}}\rangle = \langle\Psi_{\text{fin}}|P_yP_y|\Psi_{\text{fin}}\rangle$. This gives

$$\mathbb{P}[y] = \frac{1}{M^2}\sum_{x_0=0}^{r-1}\left|\sum_{j=0}^{A(x_0)=1} e^{2\pi i\frac{jy}{M/r}}\right|^2.$$

Note that the different terms in the sum over x_0 do not interfere, because the states $|f(x_0)\rangle$ are mutually orthogonal.

11.5 Analysis of the probability $\mathbb{P}[y]$

First Consider the Idealized Case Where M Is a Multiple of r

In this case, $A(x_0) = \frac{M}{r}$ and therefore

$$\mathbb{P}[y] = \frac{r}{M^2}\left|\sum_{j=0}^{\frac{M}{r}-1} e^{2\pi i\frac{jy}{M/r}}\right|^2.$$

If $y = k\frac{M}{r}$ with $k = \{0, 1, \ldots, r-1\}$, we have

$$e^{2\pi i\frac{jy}{M/r}} = e^{2\pi ijk} = 1.$$

Hence $\mathbb{P}[y] = \frac{r}{M^2}\left|\frac{M}{r}\right|^2 = \frac{1}{r}$. Since the probabilities must sum to one, it follows that the probability is zero for every other value $y \neq kM/r$. This The resulting distribution is shown in Figure **11.3**.

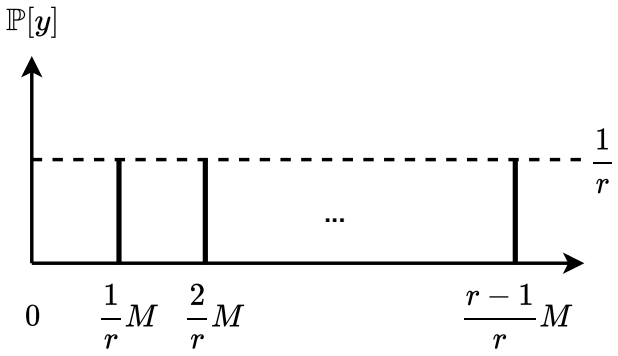


Figure 11.3 Probability distribution of the measurement outcomes when M is a multiple of r.

With probability one, the measurement outcome y has the form

$$y = k\frac{M}{r} \quad \text{with} \quad k \in \{0, 1, \ldots, r-1\}.$$

Since M is known, the measured value y determines the ratio y/M. There are two cases:

- If $\frac{y}{M} = \frac{k}{r}$ and PGCD $(k, r) = 1$, reduce the fraction y/M to lowest terms. Its denominator is then exactly r, so the order is recovered.
- If $\frac{y}{M} = \frac{k}{r}$ and PGCD $(k, r) \neq 1$, reducing the fraction yields only a proper divisor of r; the order cannot be recovered uniquely from this single sample.

In practice we do not know in advance whether k and r are coprime. We therefore reduce y/M to lowest terms and test whether the resulting denominator is a period of f. If not, the quantum sampling procedure is repeated.

The probability of success is the probability to have PGCD $(k, r) = 1$ when k is drawn uniformly in $\{0, 1, \ldots, r-1\}$. Using Eq. (11.1),

$$\mathbb{P}\left[\text{PGCD}\,(k,r) = 1, k \in \{0,1,\ldots,r-1\}\right] = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln\ln r)}.$$

Since $r < M$, we have *a probability of success for an experiment*:

$$\mathbb{P}\left[\text{succes}\right] \geq \frac{1}{4\ln\ln M} \quad \left(= \frac{1}{4\ln 2\ln m}\right).$$

Although this single-run probability can be small, it can be amplified by repeating the circuit independently. After T runs,

$$\mathbb{P}\left[\text{at least 1 success after T rounds}\right] \geq 1 - \left(1 - \frac{1}{4\ln\ln M}\right)^T,$$

which can be made at least $1 - \epsilon$ by choosing

$$T = O(|\ln\,\epsilon|\,\ln\ln\,M) = O(|\ln\,m|\,|\ln\,\epsilon|\,).$$

Indeed:

$$\begin{aligned}
&1 - \left(1 - \frac{1}{4\ln\,M}\right)^T \geq 1 - \epsilon \\
&\leftrightarrow \epsilon \geq \left(1 - \frac{1}{4\ln\,M}\right)^T \leftrightarrow \ln\,\epsilon \geq T\ln\left(1 - \frac{1}{4\ln\,M}\right) \\
&\leftrightarrow \ln\epsilon \geq -T\frac{1}{4\ln\ln M} \qquad (M \text{ large}) \\
&\leftrightarrow T \geq 4(\ln\ln\,M)|\ln\,\epsilon|
\end{aligned}$$

Now Consider the General Case Where M Is Not a Multiple of r

We shall use the following technical lemma, whose proof is omitted. The graphical interpretation in Figure **11.4** shows that the measurement distribution is concentrated near the integers closest to the rational values kM/r.

Lemma. Let $I = \cup_{k=0}^{r-1}\left[k\frac{M}{r} - \frac{1}{2}, k\frac{M}{r} + \frac{1}{2}\right] = \cup_{k=0}^{r-1} I_k$ a union of disjoint intervals I_k. Then

$$\mathbb{P}\left[y \in I\right] \geq \frac{2}{5}.$$

Thus the measurement produces an integer y lying close to kM/r for some $k \in \{0, 1, \ldots, r-1\}$ with probability at least $2/5$.

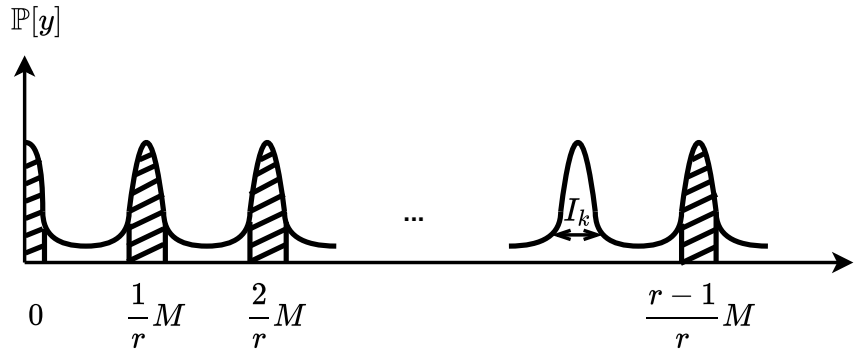


Figure 11.4 Measurement probability distribution. The shaded area has total probability greater than $2/5$. Each interval I_k has length 1, and neighboring intervals are separated by approximately $M/r \gg 1$.

If a measurement gives $y \in I$, then there exists an integer k such that

$$k\frac{M}{r} - \frac{1}{2} \leq y \leq k\frac{M}{r} + \frac{1}{2},$$

equivalently,

$$\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2M}. \tag{11.3}$$

If we choose $M > r^2$, then

$$\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2r^2} \quad \text{for } k \in \{0, 1, \ldots, r-1\}.$$

How can k and r be reconstructed from the known integers y and M? From the theory of continued fractions, if $\mathrm{PGCD}(k, r) = 1$, then k/r must occur as a convergent of the continued-fraction expansion of y/M.

Because y/M is rational, it has only finitely many convergents, all of which can be generated systematically using Euclid's algorithm in polynomial time. If $\mathrm{PGCD}(k, r) \neq 1$, however, the reduced fraction associated with k/r may have a smaller denominator, and this particular run need not reveal the true period r.

We therefore use the following procedure. Compute all convergents of y/M by the Euclidean algorithm, examine their denominators as candidates for r, and test each candidate by checking whether $a^r = 1 \pmod{N}$. The run succeeds when the measured y lies in one of the intervals I_k and k is coprime to r.

Summary. What is the success probability of a single run of the quantum circuit? The circuit starts in $|0\rangle \otimes |0\rangle$, evolves unitarily to $|\Psi_{\text{final}}\rangle$, and is then measured. The measurement produces an integer y. To recover r successfully from this outcome, two conditions are required:

- $y \in I$ for a certain $k \in \{0, 1, \ldots, r-1\}$.
- Conditioned on $y \in I_k$, the integers k and r must be coprime.

Therefore:

$$\mathbb{P}\,[\text{succes}] \geq \frac{2}{5} \times \frac{1}{4 \ln \ln r}.$$

Repeating the experiment $T = O(|\ln \epsilon|\, \ln \ln r)$ times amplifies the success probability to at least $1 - \epsilon$.

11.6 The QFT Circuit

In this section, we show how to implement the QFT as a quantum circuit. Recall the transformation to be implemented, Eq. (11.2):

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle = \frac{1}{2^{m/2}} \sum_{\substack{y_0 \ldots y_{m-1} \\ \in \{0,1\}^m}} e^{2\pi i \frac{xy}{M}} |y_{m-1} \ldots y_0\rangle$$

For $M = 2$, the QFT is simply the Hadamard gate, $QFT = H$:

$$(QFT)_{M=2}|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle).$$

For $M = 4$,

$$\begin{aligned}(QFT)_{M=4}|x\rangle &= \frac{1}{\sqrt{4}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle + e^{i\pi x}|2\rangle + e^{3i\frac{\pi}{2}x}|3\rangle\right) \\ &= \frac{1}{\sqrt{4}}\left(|00\rangle + e^{i\frac{\pi}{2}x}|01\rangle + e^{i\pi x}|10\rangle + e^{3i\frac{\pi}{2}x}|11\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle\right).\end{aligned}$$

In binary notation, $x \in \{0, 1, 2, 3\}$ is written as

$$x = 2x_1 + x_0 \quad , \quad x_0, x_1 \in \{0, 1\}$$

and hence $e^{i\pi x} = e^{2\pi i x_1} e^{i\pi x_0} = (-1)^{x_0}$ and $e^{i\frac{\pi}{2}x} = e^{i\pi x_1} e^{i\frac{\pi}{2}x_0} = (-1)^{x_1} e^{i\frac{\pi}{2}x_0}$. We therefore obtain

$$(QFT)_{M=4}|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1} e^{i\frac{\pi}{2}x_0}|1\rangle\right).$$

This factorization is the key to implementing the QFT as a quantum circuit. It leads directly to the circuit shown in Figure **11.5**.

The first SWAP operation exchanges the two qubits. It can be implemented using three CNOT gates (Figure **11.6**).

The second operation in Figure **11.5** is a Hadamard gate acting on $|x_1\rangle$, producing

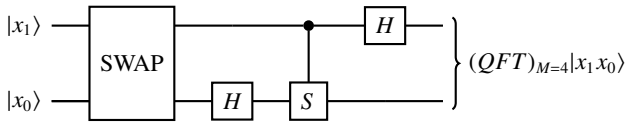


Figure 11.5 Circuit of the $(QFT)_{M=4}$.

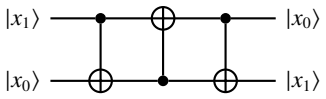


Figure 11.6 Circuit for a SWAP.

$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$. The third operation is a controlled phase shift determined by x_0: if $x_0 = 0$, no phase is added; if $x_0 = 1$, the amplitude of $|1\rangle$ acquires the phase $e^{i\pi/2}$. Finally, a Hadamard gate acts on $|x_0\rangle$ and produces $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}|1\rangle)$.

The general QFT circuit follows by extending the preceding construction.

QFT **general**

Lemma. For $x \in \{0, 1, \ldots, M-1\}$ and $M = 2^m$

$$QFT|x\rangle = \prod_{l-1}^{m} \frac{(|0\rangle + e^{i\frac{\pi}{2^{l-1}}x}|1\rangle)}{\sqrt{2}}.$$

Proof. Recall that the formula of the QFT is given by (11.2):

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}}|y\rangle = \frac{1}{2^{\frac{m}{2}}} \sum_{y=0}^{2^m-1} e^{2\pi i \frac{xy}{2^m}}|y\rangle.$$

Each $y \in \{0, 1, \ldots, 2^m - 1\}$ has a binary expansion

$$\begin{aligned} y &= 2^{m-1}y_{m-1} + 2^{m-2}y_{m-2} + \ldots + 2y_1 + y_0 \\ &= 2y' + y_0 \end{aligned}$$

where $y' = 2^{m-2}y_{m-1} + \ldots + y_1$. We split the sum over y into the contributions with $y_0 = 0$ and $y_0 = 1$; equivalently, we separate even and odd values of y.

$$\begin{aligned} QFT|x\rangle &= \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x2y'}{2^m}}|y'\rangle \otimes |0\rangle + \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x(2y'+1)}{2^m}}|y'\rangle \otimes |1\rangle \\ &= \left(\frac{1}{2^{\frac{m-1}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{xy'}{2^{m-1}}}|y'\rangle\right) \otimes (|0\rangle + e^{\frac{\pi i x}{2^{m-1}}}|1\rangle). \end{aligned}$$

This factorization can now be repeated on the first parenthesis. The only difference is that $m \to m-1$. We obtain

$$QFT|x\rangle = \left(\frac{1}{2^{\frac{m-2}{2}}} \sum_{y''=0}^{2^{m-2}-1} e^{2\pi i \frac{xy''}{2^{m-2}-1}} |y''\rangle \right) \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-2}}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-1}}}|1\rangle}{\sqrt{2}}.$$

Iterating this procedure proves the lemma.

The final step is to substitute the binary expansion of x, as in the $M = 4$ example:

$$x = 2^{m-1}x_{m-1} + \ldots + 2^2 x_2 + 2x_1 + x_0,$$

which implies, for every $1 \le l \le m$,

$$e^{i\frac{\pi}{2^{l-1}}x} = e^{i\pi x_{l-1}} e^{i\frac{\pi}{2}x_{l-2}} \ldots e^{i\frac{\pi}{2^{l-2}}x_1} e^{i\frac{\pi}{2^{l-1}}x_0}.$$

The crucial point is that bits x_i with $i \ge l$ do not contribute. Substituting this expression into the lemma gives the final factorization from which the circuit is constructed:

$$QFT|x\rangle = \prod_{l=1}^{m} \left(\frac{|0\rangle + e^{i\pi x_{l-1}} e^{i\frac{\pi}{2}x_{l-2}} \ldots e^{i\frac{\pi}{2^{l-1}}x_0}|1\rangle}{\sqrt{2}} \right). \tag{11.4}$$

Figure 11.7 shows the circuit corresponding to this formula for $m = 4$, i.e. $M = 16$.

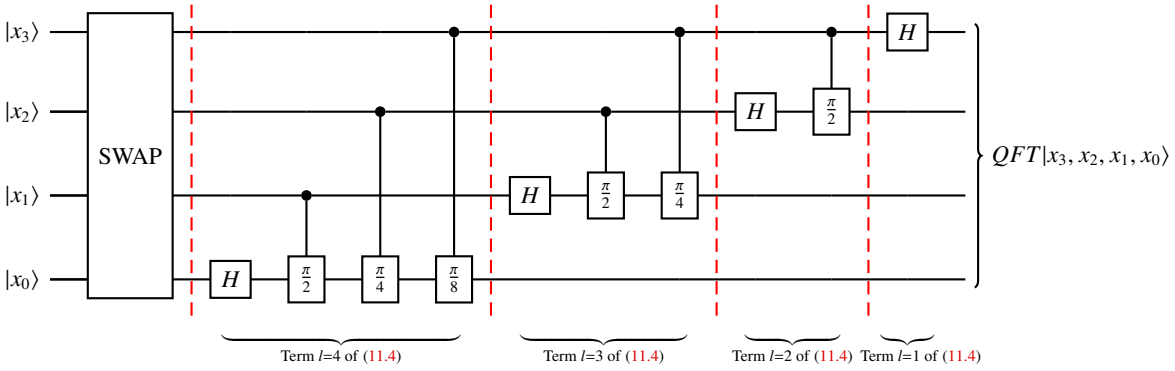


Figure 11.7 Circuit of the QFT for 4 qubits.

The final SWAP operations require $O(m)$ CNOT gates. The number of Hadamard gates and controlled phase-shift gates is

$$m + (m-1) + \ldots + 1 = \frac{m(m+1)}{2}.$$

The circuit depth is therefore of order $O(m^2)$. This depth describes how the QFT computation time scales with the input size. The circuit width is m, so the total circuit size, estimated as depth $\times$ width, is $O(m^3)$.

11.7 Circuit for $U_{f_{a,N}}$

In Section **11.3**, we introduced a randomized factoring algorithm based on period finding for modular exponentiation. More precisely, for a such that $\mathrm{PGCD}(a, N) = 1$, we seek the period of $f_{a,N}(x) = a^x \pmod N$. Equivalently, we seek $\mathrm{Ord}_N(a) = r$, the smallest positive integer r such that $a^r = 1 \pmod N$.

We must therefore construct a circuit implementing the unitary operator $U_{f_{a,N}}$ (Figure **11.8**).

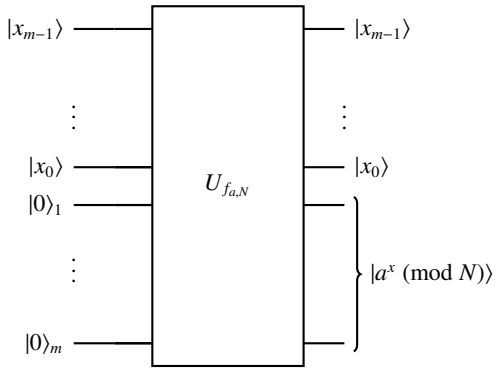


Figure 11.8 Unitary implementation of modular exponentiation.

First note that

$$\begin{aligned} a^x &= a^{2^{m-1}x_{m-1}} a^{2^{m-2}x_{m-2}} \dots a^{2x_1} a^{x_0} \\ &= \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} \dots \left(a^2\right)^{x_1} a^{x_0}. \end{aligned}$$

The powers $\{a, a^2, a^4, a^8, \dots, a^{2^{m-1}}\}$ can be precomputed using a polynomial number of arithmetic operations. Starting from the m-bit integer a, compute $a^2 \pmod N$, then square repeatedly modulo N. Each modular multiplication involves only $O(m)$-bit integers. Using elementary arithmetic, each such multiplication has polynomial cost, and only $O(m)$ powers are required. Thus the entire table of powers can be prepared in polynomial time. With a straightforward arithmetic model this requires $O(m^3)$ elementary bit operations. Reversible classical circuits can implement these modular multiplications and can therefore be promoted to unitary quantum circuits. Using the binary expansion of x and the identity above, controlled modular multiplications by the precomputed powers implement the circuit shown in Figure **11.9**.

The depth of this circuit is $O(m^3)$, its width $O(m)$ and its size $O(m^4)$.

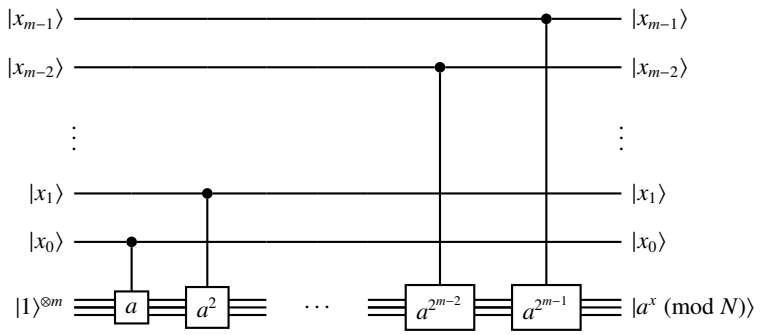


Figure 11.9 Circuit for modular exponentiation.

11.8 Summary of Shor's Algorithm

We can now summarize Shorś quantum algorithm for factoring an integer N.

input: an odd integer N with at least two distinct prime factors.

output: a nontrivial factor of N.

running time: polynomial in $\ln N$ and logarithmic in the inverse failure probability.

circuit size: polynomial in $\ln N$.

Algorithm:

1. Choose a uniformly at random from $\{2, \ldots, N-1\}$.

2. Compute $d = \mathrm{PGCD}(a, N)$ using Euclid's algorithm:

- if $d > 1$, SUCCESS: d is a nontrivial factor of N;
- otherwise $d = 1$, continue to step **3**.

3. Compute $r = \mathrm{Ord}_N(a)$, the smallest positive integer satisfying $a^r = 1 \pmod N$. Use the quantum order-finding circuit with m qubits and $M = 2^m \approx N^2$. Measure the first register to obtain y, then compute the convergents of y/M classically using Euclid's algorithm. Test the denominators of these convergents until a candidate r satisfying $a^r = 1 \pmod N$ is found.
- if such an r is found, continue to step **4**;
- otherwise, declare FAILURE and repeat with a new random value of a.

4. Check whether r is even and $a^{r/2} \neq -1 \pmod N$.
- if both conditions hold, continue to step **5**;
- otherwise, declare FAILURE and restart the procedure.

5. Compute PGCD $\left(a^{r/2}+1, N\right)$ and PGCD $\left(a^{r/2}-1, N\right)$. These greatest common divisors yield nontrivial factors of N.

A single round succeeds with probability of order $1/\ln\ln N$ and has running time $O((\ln N)^3)$. Repeating independent rounds amplifies the success probability. To achieve success probability at least $1-\epsilon$, the total running time is of order $O(|\ln \epsilon|(\ln\ln N)(\ln N)^3)$.

12 Grover's algorithm

Grover's algorithm addresses a problem fundamentally different from the structured problems considered in the preceding chapters. It searches for a marked element in an unstructured set, using only oracle access to a Boolean predicate.

A useful classical analogy is an unsorted database with N entries. If one is given a key for which the entries carry no useful ordering or structure, exhaustive search requires $O(N)$ oracle queries in the worst case, and random search has the same order of complexity. When $N = 2^n$, this is exponential in the number n of bits used to label the entries.

Grover's algorithm reduces the query complexity to $O\left(\sqrt{N}\right)$. This is a quadratic quantum speedup, and it is optimal in the black-box model: without additional structure, no quantum algorithm can solve the general search problem with asymptotically fewer than order $\sqrt{N}$ queries.

As an illustration, consider factoring $N = pq$. A naive search for a divisor needs only inspect integers up to $\sqrt{N}$, and therefore costs $O\left(\sqrt{N}\right)$ classical trials. Replacing this exhaustive search by Grover's algorithm would reduce the cost to $O\left(N^{1/4}\right)$. Shor's algorithm achieves an exponentially larger improvement because it exploits the periodic structure of modular arithmetic rather than treating factorization as an unstructured search problem.

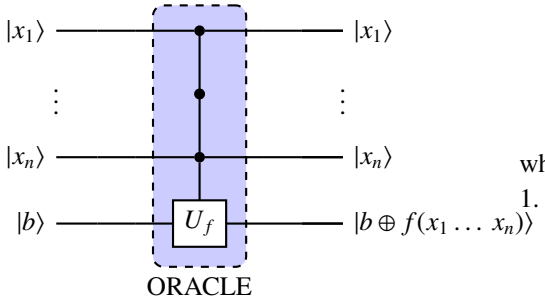
12.1 Mathematical Formulation of the Problem

Let $f : \mathbf{F}_2^n \to \mathbf{F}_2 = \{0, 1\}$. We seek a solution of

$$f(x_1 \ldots x_n) = 1.$$

The basic algorithm assumes that the total number M of solutions is known. We later explain how this assumption can be removed by a simple randomized extension.

We assume access to the quantum oracle



$U_f(|x_1 \dots x_n\rangle \otimes |b\rangle) =$
$|x_1 \dots x_n\rangle \otimes |b \oplus f(x_1 \dots x_n)\rangle$
where $x_1 \dots x_n \in \mathbf{F}_2^n$ and $b = 0$ or 1.

This formulation emphasizes the generality of unstructured search: the oracle supplies only the predicate f, with no additional structure to exploit.

12.2 Derivation of the algorithm

In the previous chapters we generally introduced the complete circuit first. Here it is more instructive to derive the algorithm geometrically, because Grover's iterate emerges naturally as the composition of two reflections. The initial state is

$$|\underbrace{0 \dots 0}_{n \text{ fois}}\rangle \otimes |1\rangle$$

The first n qubits form the input register and the last qubit is auxiliary. Applying Hadamard gates to the first register prepares the uniform superposition over all possible inputs:

$$(H \otimes \dots \otimes H \otimes \mathbb{1})|0 \dots 0\rangle \otimes |1\rangle = \frac{1}{2^{n/2}} \sum_{x \in \mathbf{F}_2^n} |x\rangle \otimes |1\rangle$$

Applying a Hadamard gate to the auxiliary qubit prepares the state $(|0\rangle - |1\rangle)/\sqrt{2}$, which allows us to use phase kickback. The state becomes

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbf{F}_2^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Applying U_f then gives

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbf{F}_2^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |\overline{f(x)}\rangle)$$

Using

$$|f(x)\rangle - |\overline{f(x)}\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle),$$

we obtain

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

The preceding operations are summarized in Figure **12.1**.

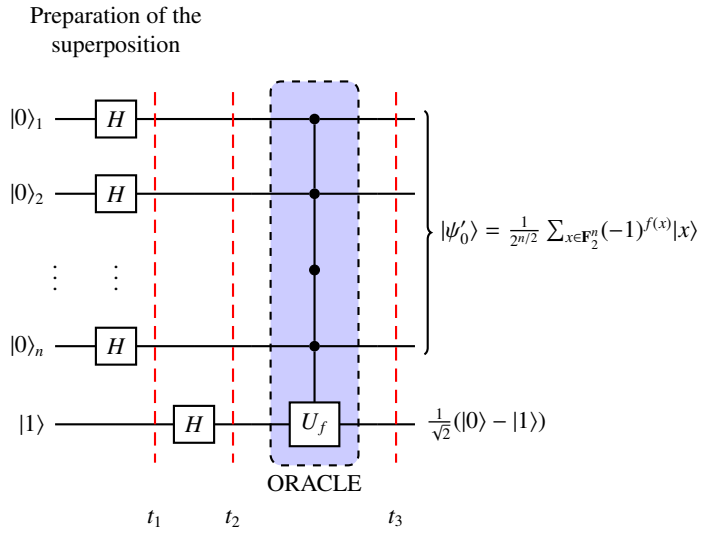


Figure 12.1 Initial part of Grover's circuit: preparation of the uniform superposition followed by the oracle phase flip.

In the resulting state, every solution of $f(x) = 1$ has acquired a phase -1. This phase marking is the first reflection in Grover's algorithm.

Suppose there are M solutions. Define the normalized superpositions of marked and unmarked states by

$$|S\rangle \equiv \frac{1}{\sqrt{M}} \sum_{x \text{ marked}} |x\rangle,$$
$$|P\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_{x \text{ unmarked}} |x\rangle,$$

where $N = 2^n$ is the total number of computational-basis states. Then

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \sqrt{\frac{M}{N}} |S\rangle + \sqrt{\frac{N-M}{N}} |P\rangle$$
$$|\psi_0'\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle = -\sqrt{\frac{M}{N}} |S\rangle + \sqrt{\frac{N-M}{N}} |P\rangle$$

Because the two coefficients satisfy $\frac{M}{N} + \frac{N-M}{N} = 1$, we may introduce an angle θ_0 such

that

$$\sin\theta_0 = \sqrt{\frac{M}{N}} \qquad \text{and} \qquad \cos\theta_0 = \sqrt{\frac{N-M}{N}}.$$

This gives a simple geometric interpretation. The state $|\psi_0\rangle$ lies in the two-dimensional plane spanned by $|P\rangle$ and $|S\rangle$ and makes an angle θ_0 with the $|P\rangle$ axis. The oracle changes the sign of the marked component, so $|\psi_0'\rangle$ is the reflection of $|\psi_0\rangle$ about the $|P\rangle$ axis; see Figure **12.2**.

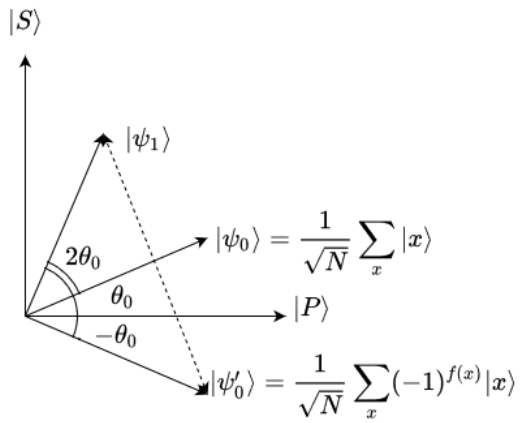


Figure 12.2

After the oracle, the marked basis states carry a phase -1. To increase their amplitudes, we reflect this state about $|\psi_0\rangle$, obtaining $|\psi_1\rangle$ as illustrated in Figure **12.2**. Two features are important:

- $|\psi_1\rangle$ is closer to the solution subspace spanned by $|S\rangle$, especially when $M \ll N$.
- The reflection axis $|\psi_0\rangle$ is independent of the unknown solutions.

We have

$$|\psi_1\rangle = \cos 3\theta_0 |P\rangle + \sin 3\theta_0 |S\rangle$$

A third crucial observation is that $|\psi_1\rangle$ is obtained from $|\psi_0\rangle$ by a rotation through $2\theta_0$ in the plane spanned by $|P\rangle$ and $|S\rangle$.

Repeating these two reflections—first the oracle reflection, then the reflection about $|\psi_0\rangle$—produces successive rotations by $2\theta_0$:

$$|\psi_k\rangle = \cos((2k+1)\theta_0)|P\rangle + \sin((2k+1)\theta_0)|S\rangle.$$

When $M \ll N$, θ_0 is small. If M is known, we can choose k so that $(2k+1)\theta_0 \approx \pi/2$, making the state nearly parallel to $|S\rangle$. A subsequent measurement then returns a solution with probability close to one.

We now turn to the implementation of the reflection about $|\psi_0\rangle$. Geometrically, reflecting a vector $\vec{v}$ about the unit vector $\vec{\psi_0}$ gives

$$\vec{v} \mapsto 2(\vec{\psi_0}^T \cdot \vec{v})\vec{\psi_0} - \vec{v}.$$

In Dirac notation,

$$\begin{aligned} |v\rangle \mapsto & 2|\psi_0\rangle \langle\psi_0|v\rangle - |v\rangle \\ = & (2|\psi_0\rangle\langle\psi_0| - \mathbb{1})|v\rangle \\ = & H^{\otimes n}(2|0\ldots 0\rangle\langle 0\ldots 0| - \mathbb{1})H^{\otimes n}|v\rangle \end{aligned}$$

The operator in parentheses, $2|0\ldots 0\rangle\langle 0\ldots 0| - \mathbb{1}$, leaves $|0\ldots 0\rangle$ unchanged and flips the phase of every other computational-basis state:

$$(2|0\ldots 0\rangle\langle 0\ldots 0| - \mathbb{1})|x\rangle = \begin{cases} |0\ldots 0\rangle & \text{if } x = (0\ldots 0), \\ -|x\rangle & \text{otherwise.} \end{cases} \tag{12.1}$$

We call the middle operator *Phase Cond*, for "conditional phase". The corresponding reflection about $|\psi_0\rangle$ is implemented by the circuit in Figure **12.3**.

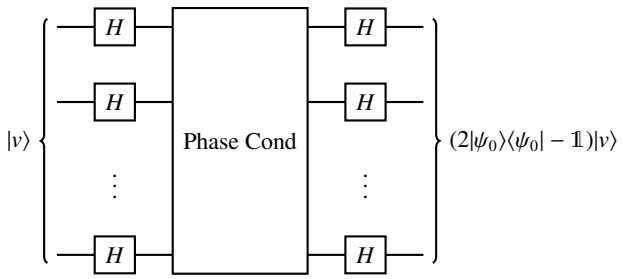


Figure 12.3 Circuit implementing the reflection of $|v\rangle$ about the axis $|\psi_0\rangle$.

Combining this reflection circuit with the oracle phase flip of Figure **12.1** gives one Grover iteration, shown in Figure **12.4**.

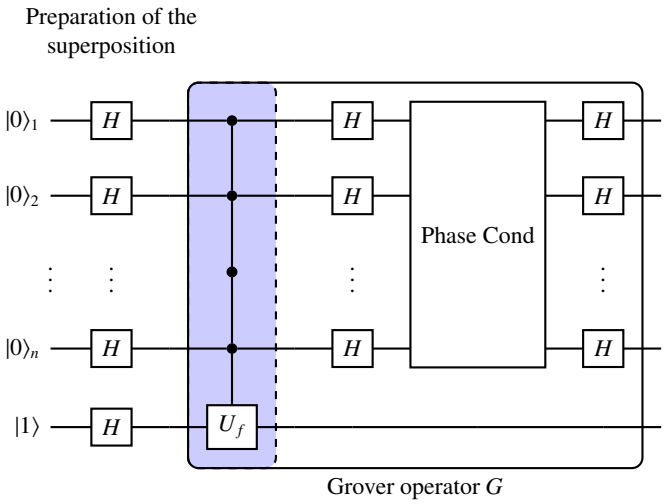


Figure 12.4 Definition of the Grover operator G. The oracle phase flip is followed by the reflection about $|\psi_0\rangle$.

The boxed part of the circuit is the *Grover operator*, denoted by G. Applied to

$$\frac{1}{\sqrt{N}}\sum_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = (\cos\theta_0|P\rangle + \sin\theta_0|S\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

it performs a rotation by $2\theta_0$ in the plane spanned by $|P\rangle$ and $|S\rangle$. The output is

$$(\cos 3\theta_0|P\rangle + \sin 3\theta_0|S\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Grover's algorithm consists of iterating the operator G an appropriate number k of times. The resulting circuit is shown in Figure **12.5**.

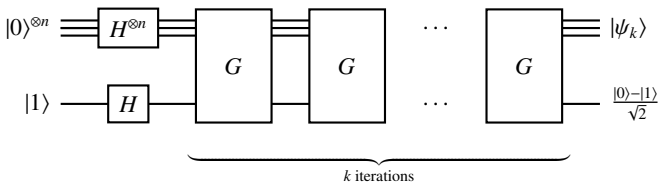


Figure 12.5 Circuit for Grover's algorithm. Each block G is the Grover iterate defined in Figure **12.4**.

The circuit depth is $O(k)$ Grover iterations, and it acts on $n+1$ qubits.

12.3 Probabilistic Analysis

We measure the first register in the computational basis. The probability of obtaining a marked state is

$$|\langle S|\psi_k\rangle|^2 = \sin^2\big((2k+1)\theta_0\big)$$

Recall that $\sin(\theta_0) = \sqrt{\frac{M}{N}}$ and $\cos(\theta_0) = \sqrt{1-\frac{M}{N}}$.

First consider the simple case $M = N/4$.
Then $\sin\theta_0 = 1/2$, so $\theta_0 = \pi/6$. After a single Grover iteration ($k = 1$), the state is aligned with $|S\rangle$ because $3\theta_0 = \pi/2$. A measurement therefore returns a solution with probability one, after one oracle query. This case is not especially challenging classically, since a uniformly random query already succeeds with probability $1/4$; nevertheless it illustrates the geometry of amplitude amplification clearly.

Now consider $M = 1$,
the most demanding case intuitively. Here $\sin\theta_0 = 1/\sqrt{N}$, so for large N, $\theta_0 \simeq 1/\sqrt{N}$. Hence

$$\sin^2((2k+1)\theta_0) \simeq \sin^2\left(\frac{2k+1}{\sqrt{N}}\right).$$

Choosing k close to $\frac{\pi}{4}\sqrt{N}$ makes $(2k+1)/\sqrt{N}$ close to $\pi/2$, so the success probability approaches one. More precisely, taking the nearest integer to $\frac{\pi}{4}\sqrt{N}$ gives success probability $1 - O(1/N)$.

General case with known M.

- If $M < \frac{3}{4}N$, then $\sin\theta_0 < \frac{\sqrt{3}}{2}$ and hence $\theta_0 < \frac{\pi}{3}$. Choose

$$k = \left\lfloor \frac{\pi}{4\theta_0} \right\rfloor.$$

  Writing $k = \frac{\pi}{4\theta_0} - \frac{1}{2} + \delta$ with $|\delta| < \frac{1}{2}$, we have

$$(2k+1)\theta_0 = \frac{\pi}{2} + 2\delta\theta_0.$$

  Because $2|\delta|\theta_0 < \frac{\pi}{3}$, the success probability satisfies

$$\sin^2((2k+1)\theta_0) > \sin^2\left(\frac{\pi}{6}\right) = \frac{1}{4}.$$

  Thus the algorithm succeeds with a constant probability, which can be amplified by independent repetition.
- If $M \geq \frac{3}{4}N$, a single uniformly random classical query already succeeds with probability at least $3/4$.

General case with unknown M.

If M is unknown, the optimal number of Grover iterations is not known in advance: too few iterations give insufficient amplification, whereas too many rotate the state past the solution subspace. A simple randomized variant avoids this problem and still succeeds with probability at least $1/4$:

1 Choose an input x uniformly at random. If $f(x) = 1$, declare SUCCESS.
2 Otherwise, choose $R \in \{0, 1, \ldots, \lfloor \sqrt{N} \rfloor - 1\}$ uniformly at random, perform R Grover iterations, and measure the output.

If $M \geq \frac{3}{4}N$, step 1 alone succeeds with probability at least $3/4$. If $M < \frac{3}{4}N$, then

$$\mathbb{P}\left[\text{success}\right] \geq \mathbb{P}\left[\text{success in step 2}\right],$$

and

$$\begin{aligned}
\mathbb{P}\left[\text{success in step 2}\right] &= \sum_{R=0}^{\lfloor \sqrt{N} \rfloor - 1} \mathbb{P}\left[\text{success} \mid R\right]\mathbb{P}\left[R\right] \\
&\simeq \frac{1}{\sqrt{N}} \sum_{R=0}^{\sqrt{N}-1} \sin^2((2R+1)\theta_0) \\
&= \frac{1}{2} - \frac{\sin\left(4\theta_0\sqrt{N}\right)}{4\sqrt{N}\sin(2\theta_0)}.
\end{aligned}$$

Since $\left|\sin\left(4\theta_0\sqrt{N}\right)\right| \leq 1$ and, for $M < \frac{3}{4}N$,

$$\sin(2\theta_0) = 2\sin\theta_0\cos\theta_0 = 2\sqrt{\frac{M}{N}}\sqrt{1-\frac{M}{N}} > \frac{1}{\sqrt{N}},$$

we obtain $\mathbb{P}\left[\text{success in step 2}\right] \geq \frac{1}{4}$. As usual, this constant success probability can be amplified by repetition.

13 Distributed Computation - Distributed Deutsch-Jozsa Problem

Suppose Alice and Bob each have a computer and wish to carry out a joint task. For example, they may need to compute a function $f(\vec{x}, \vec{y})$, where Alice receives $\vec{x} \in \mathbf{F}_2^n$ and Bob receives $\vec{y} \in \mathbf{F}_2^n$. Depending on the computational model, they may communicate through a classical channel, through a quantum channel, or they may share entanglement in advance. Our focus is exclusively on the communication complexity: the number of classical bits, qubits, or entangled bits (e-bits) that must be exchanged or shared.

13.1 Models of Distributed Computation

We begin with the classical communication model shown in Figure **13.1**.

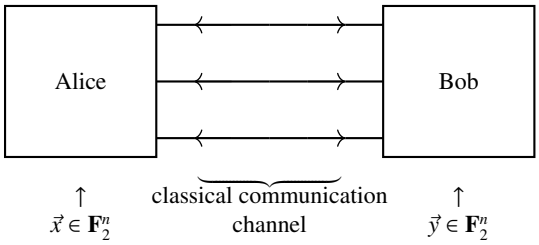


Figure 13.1 Classical model of distributed computation.

Alice and Bob must compute $f(\vec{x}, \vec{y})$ while exchanging at most T classical bits. We define the communication complexity as the minimum such T, ignoring the local computational cost of evaluating the function or any local oracle calls. A classical lower bound shows that, for the problem studied below, T must grow linearly with n; in particular $T \geq \alpha n$ for a positive constant α (one known bound gives $\alpha \simeq 0.007$).

We shall compare this classical setting with two quantum communication models, due respectively to Yao and to Cleve and Buhrman, for which the same task can be solved with $T = O(\log_2 n)$ communication.

Model of Yao:

Alice and Bob communicate through a quantum channel and exchange a total of T qubits, as illustrated in Figure 13.2. Each party may perform arbitrary local unitary operations and local measurements.

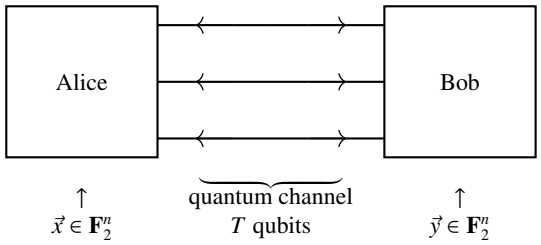


Figure 13.2 Yao's model of distributed quantum computation.

Model of Cleve-Buhrman:

Alice and Bob initially share entangled pairs (or, more generally, an entangled state) and may communicate through a classical channel, as in Figure 13.3. Their quantum operations and measurements are local.

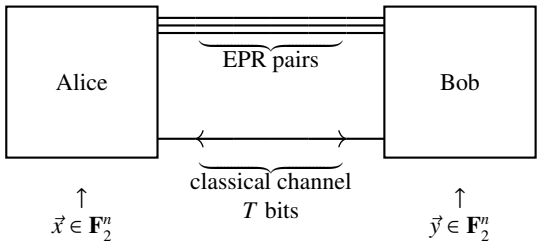


Figure 13.3 Cleve–Buhrman's model of distributed quantum computation.

The two models are closely related through quantum teleportation (Section 6.3). In the Cleve–Buhrman model, T shared EPR pairs together with $2T$ communicated classical bits can simulate the transmission of T qubits. We nevertheless analyze the two models separately, because the direct Cleve–Buhrman protocol below avoids this extra factor of two.

Distributed Deutsch-Jozsa Problem:

We focus on the following specific communication problem. Alice receives a vector $\vec{x} \in \mathbf{F}_2^n$ and Bob receives $\vec{y} \in \mathbf{F}_2^n$, where n is a power of two.[1] They are promised that either $\vec{x} = \vec{y}$, or the vectors differ in exactly half of their components. Equivalently, if d_H denotes Hamming distance,[2] then

$$d_H(\vec{x}, \vec{y}) = 0 \qquad \text{or} \qquad d_H(\vec{x}, \vec{y}) = \frac{n}{2}. \tag{13.1}$$

The promise can equivalently be expressed through the quantity

$$\frac{1}{n}\sum_{i=0}^{n-1}(-1)^{x_i+y_i} = \begin{cases} 1 & \text{if} \quad d_H(\vec{x}, \vec{y}) = 0 \\ 0 & \text{if} \quad d_H(\vec{x}, \vec{y}) = \frac{n}{2} \end{cases} \tag{13.2}$$

It is convenient to introduce the phase vector $\vec{f} : \mathbf{F}_2^n \times \mathbf{F}_2^n \to \{-1, 1\}^n$ defined by

$$\vec{f}(\vec{x}, \vec{y}) = \begin{pmatrix} f_0(\vec{x}, \vec{y}) \\ f_1(\vec{x}, \vec{y}) \\ \vdots \\ f_{n-1}(\vec{x}, \vec{y}) \end{pmatrix} \tag{13.3}$$

$$f_i(\vec{x}, \vec{y}) \equiv (-1)^{x_i+y_i} = (-1)^{x_i}(-1)^{y_i} \tag{13.4}$$

In other words, Alice can compute the phases $(-1)^{x_i}$ locally and Bob can compute $(-1)^{y_i}$ locally. Their task is to combine these phases so as to determine whether $\frac{1}{n}\sum_{i=0}^{n-1}(-1)^{x_i+y_i}$ equals 1 or 0, while communicating as little information as possible.

A purely classical protocol can solve the problem using $T = O(n)$ communicated bits. We shall see that both quantum models reduce the communication cost to $T = O(\log_2 n)$.

13.2 Analysis of Yao's Model

Alice's and Bob's circuits closely resemble the standard Deutsch–Jozsa circuit. For simplicity, let $n = 2^k$, so that $k = \log_2 n$. We begin with Alice's circuit, shown in Figure 13.4.

At time t_1, the state is

$$|\psi_1\rangle = |0\rangle^{\otimes k} \otimes |1\rangle \tag{13.5}$$

[1] In this chapter we index the components from 0 to $n-1$, so $\vec{x} = (x_0, \ldots, x_{n-1})$, rather than from 1 to n.

[2] The Hamming distance between two binary strings is the number of positions at which they differ: $d_H(\vec{x}, \vec{y}) = \#\{i \mid x_i \neq y_i\}$.

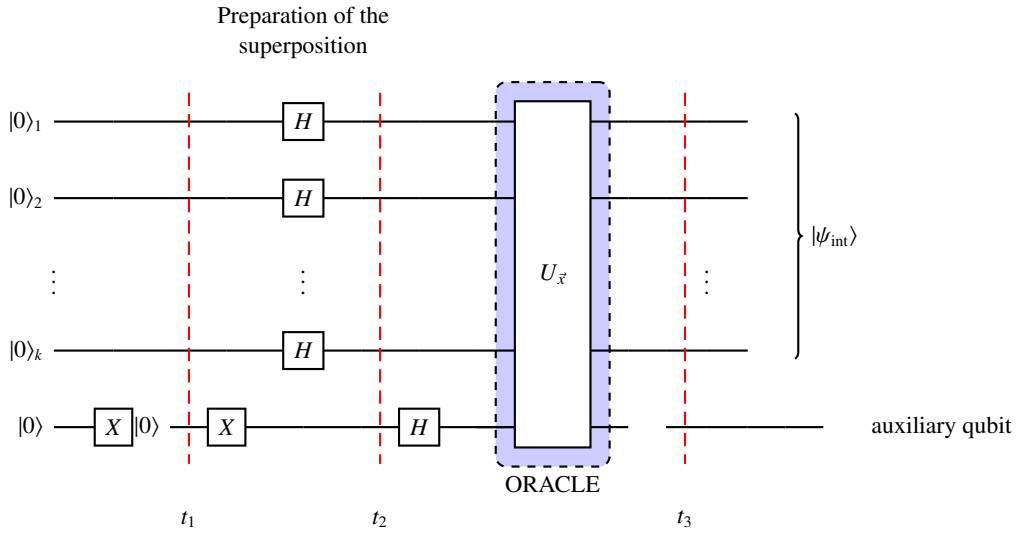


Figure 13.4 Alice's circuit in Yao's quantum communication model.

At time t_2, after the Hadamard gates, the state is

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2^{\frac{k}{2}}} \sum_{\substack{b_1 \dots b_k \\ \in \{0,1\}^k}} |b_1 \dots b_k\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned} \tag{13.6}$$

where $|i\rangle = |b_1 \dots b_k\rangle$ and $b_1 \dots b_k$ is the k-bit binary representation of the integer i.

Alice's oracle is defined by

$$U_{\vec{x}}(|i\rangle \otimes |z\rangle) = |i\rangle \otimes |x_i \oplus z\rangle \qquad z \in \{0,1\}, i = 0 \dots n-1 \tag{13.7}$$

After Alice applies her oracle, the state at time t_3 is

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle \otimes \left(\frac{|x_i\rangle - |1 \oplus x_i\rangle}{\sqrt{2}} \right) \\ &= \underbrace{\left\{ \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i} |i\rangle \right\}}_{|\psi_{\text{int}}\rangle} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned} \tag{13.8}$$

At this point Alice holds the intermediate state

$$|\psi_{\text{int}}\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i} |i\rangle,$$

encoded in $k = \log_2 n$ qubits. The phases of this state contain all of Alice's values $(-1)^{x_i}$ simultaneously. Alice sends these k qubits to Bob through a quantum channel. Physically, the register could be carried by photons, spins, or any other suitable qubit implementation. Bob then uses the received state as the input to the circuit shown in Figure **13.5**.

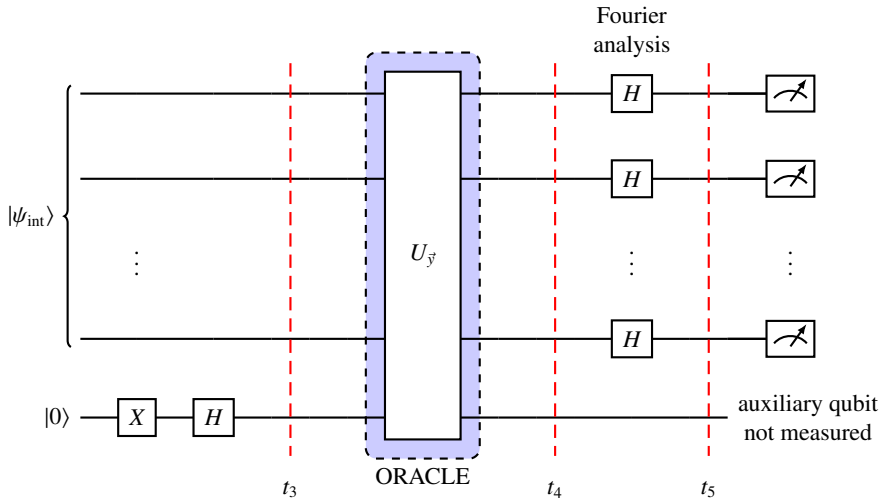


Figure 13.5 Bob's circuit in Yao's quantum communication model.

After receiving Alice's register and including the auxiliary qubit used in his own circuit, Bob's state at time t_3 is

$$|\psi_3\rangle = |\psi_{\text{int}}\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{13.9}$$

At time t_4, after Bob applies his oracle $U_{\vec{y}}$, the state is

$$\begin{aligned} |\psi_4\rangle &= U_{\vec{y}}\left(\left\{\frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}(-1)^{x_i}|i\rangle\right\} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}(-1)^{x_i} U_{\vec{y}}\left(|i\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \end{aligned} \tag{13.10}$$

Again, by definition, we have

$$U_{\vec{y}}(|i\rangle \otimes |z\rangle) = |i\rangle \otimes |y_i \oplus z\rangle \qquad z \in \{0,1\}, i = 0 \ldots n-1 \tag{13.11}$$

Using this definition, Bob obtains

$$\begin{aligned} |\psi_4\rangle &= \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \otimes \left(\frac{|y_i\rangle - |1 \oplus y_i\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i + y_i} |i\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned} \tag{13.12}$$

Bob must now extract the relevant information. As in the standard Deutsch–Jozsa algorithm, he applies a Hadamard transform to the first register and then measures it in the computational basis.

At time t_5, after the Hadamard transform, the state is

$$|\psi_5\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} H^{\otimes k} |i\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{13.13}$$

Using

$$\begin{aligned} H^{\otimes k} |i\rangle &= H^{\otimes k} |b_1 \dots b_k\rangle \\ &= H|b_1\rangle \otimes \dots \otimes H|b_k\rangle \\ &= \frac{1}{2^{\frac{k}{2}}} \sum_{\substack{c_1 \dots c_k \\ \in \{0,1\}^k}} (-1)^{b_1 c_1 + \dots + b_k c_k} |c_1 \dots c_k\rangle \end{aligned} \tag{13.14}$$

Therefore the state immediately before measurement is

$$\begin{aligned} |\psi_5\rangle &= \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} \left\{ \frac{1}{\sqrt{n}} \sum_{\substack{c_1 \dots c_k \\ \in \{0,1\}^k}} (-1)^{b_1 c_1 + \dots + b_k c_k} |c_1 \dots c_k\rangle \right\} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ &= \sum_{j=0}^{n-1} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} (-1)^{\langle i,j \rangle} \right\} |j\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned} \tag{13.15}$$

Here $\langle i, j \rangle$ denotes the binary inner product of the k-bit representations of the integers i and j. Thus Bob's register contains the Fourier transform of the phase pattern $(-1)^{x_i + y_i}$. Measuring in the computational basis gives outcome $|j\rangle$, $j = 0, \dots, n-1$, with probability

$$\mathbb{P}[j] = \left| \frac{1}{n} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} (-1)^{\langle i,j \rangle} \right|^2 \tag{13.16}$$

In particular, the probability of observing $j = 0$ is

$$\mathbb{P}[j = 0] = \frac{1}{n^2} \left| \sum_{i=0}^{n-1} (-1)^{x_i + y_i} \right|^2 = \begin{cases} 1 & \text{if} \quad \vec{x} = \vec{y} \\ 0 & \text{if} \quad d_H(\vec{x}, \vec{y}) = \frac{n}{2} \end{cases} \tag{13.17}$$

Therefore Bob can decide deterministically between the two promised cases by checking whether the measurement outcome is $j = 0$. The only quantum communication required by the protocol is the $k = \log_2 n$ qubits sent from Alice to Bob.

13.3 Analysis of the Cleve-Buhrman Model

Assume that Alice and Bob initially share the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle_A \otimes |i\rangle_B = \frac{1}{2^{\frac{k}{2}}} \sum_{\substack{b_1 \dots b_k \\ \in \{0,1\}^k}} |b_1 \dots b_k\rangle_A \otimes |b_1 \dots b_k\rangle_B \tag{13.18}$$

Alice and Bob each hold k qubits. The state above is simply the tensor product of k EPR pairs. Each party now applies the local circuit shown in Figure **13.6**.

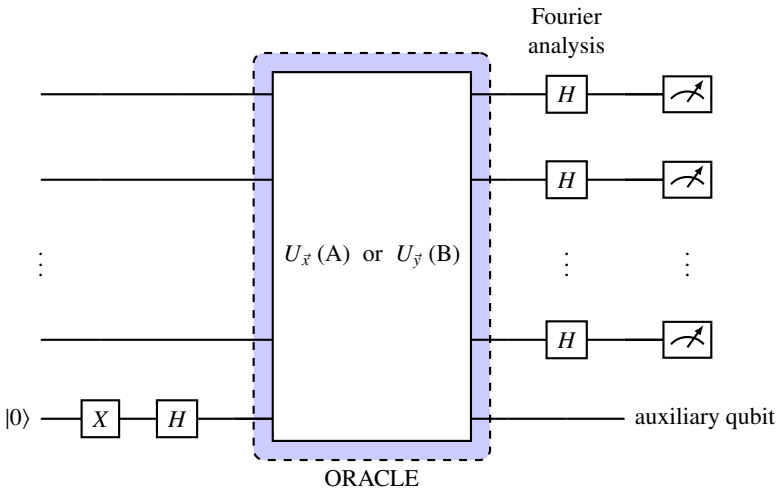


Figure 13.6 Local circuits used by Alice ($U_{\vec{x}}$) and Bob ($U_{\vec{y}}$) in the Cleve–Buhrman model.

Each party uses the appropriate half of the shared entangled state as input to the circuit. After the local oracle operations $U_{\vec{x}}$ and $U_{\vec{y}}$, the joint state is

$$|\psi'\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} |i\rangle_A \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \otimes |i\rangle_B \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{13.19}$$

The final step before measurement is a Hadamard transform on both sides. Dropping the two auxiliary factors $((|0\rangle - |1\rangle)/\sqrt{2})^{\otimes 2}$, which no longer play any role, we obtain

$$\begin{aligned} |\psi''\rangle &= \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} H^{\otimes k} |i\rangle_A \otimes H^{\otimes k} |i\rangle_B \\ &= \frac{1}{n^{\frac{3}{2}}} \sum_{i=0}^{n-1} (-1)^{x_i + y_i} \sum_{j_1=0}^{n-1} (-1)^{\langle i, j_1 \rangle} |j_1\rangle_A \otimes \sum_{j_2=0}^{n-1} (-1)^{\langle i, j_2 \rangle} |j_2\rangle_B \\ &= \frac{1}{n^{\frac{3}{2}}} \sum_{j_1=0}^{n-1} \sum_{j_2=0}^{n-1} \left\{ \sum_{i=0}^{n-1} (-1)^{x_i + y_i} (-1)^{\langle i, j_1 \rangle} (-1)^{\langle i, j_2 \rangle} \right\} |j_1\rangle_A \otimes |j_2\rangle_B \end{aligned} \tag{13.20}$$

As before, $\langle i, j_1 \rangle$ and $\langle i, j_2 \rangle$ denote the binary inner products of the k-bit representations of i, j_1, and j_2. A measurement produces an outcome $|j_1\rangle_A \otimes |j_2\rangle_B$ with probability

$$\mathbb{P}\left[j_1, j_2\right] = \frac{1}{n^3}\left|\sum_{i=0}^{n-1}(-1)^{x_i+y_i}(-1)^{\langle i,j_1\rangle+\langle i,j_2\rangle}\right|^2 \tag{13.21}$$

In particular:

$$\mathbb{P}\left[j_1 = j, j_2 = j\right] = \frac{1}{n^3}\left|\sum_{i=0}^{n-1}(-1)^{x_i+y_i}(-1)^{2\langle i,j\rangle}\right|^2 = \frac{1}{n^3}\left|\sum_{i=0}^{n-1}(-1)^{x_i+y_i}\right|^2 \tag{13.22}$$

Thus the probability that Alice and Bob obtain the same integer is

$$\mathbb{P}\left[j_1 = j_2\right] = \sum_{j=0}^{n-1}\mathbb{P}\left[j_1 = j, j_2 = j\right] = \frac{1}{n^2}\left|\sum_{i=0}^{n-1}(-1)^{x_i+y_i}\right|^2 = \begin{cases} 1 & \text{if} \quad d_H(\vec{x},\vec{y}) = 0 \\ 0 & \text{if} \quad d_H(\vec{x},\vec{y}) = \frac{n}{2} \end{cases} \tag{13.23}$$

In this protocol, Alice and Bob must finally exchange the k-bit strings j_1 and j_2 in order to determine whether they are equal. Since $k = \log_2 n$, the classical communication complexity is $T = \log_2 n$ bits.

14 Quantum Error Correction

In classical information theory, the standard way to protect stored or transmitted data against noise is to introduce redundancy in a sufficiently structured form. This is the basic idea of error correction. Digital information is particularly well suited to this strategy because errors can be classified discretely. At first sight, quantum error correction may appear impossible: quantum states form a continuum, and direct measurement generally disturbs the state one is trying to protect. Nevertheless, Shor and others showed that quantum error correction is possible. The key is that, although the state amplitudes are continuous, the relevant error operators can be decomposed into a discrete operator basis, allowing error syndromes to be extracted without learning the encoded quantum information itself.

In this chapter we introduce several elementary quantum error-correcting codes. We begin with the simplest examples, quantum repetition codes for bit-flip and phase-flip errors. Concatenating these two repetition codes leads to Shorś nine-qubit code. This construction already illustrates the main ideas behind more general stabilizer and Calderbank–Shor–Steane (CSS) codes.

14.1 Brief Review of Classical Linear Codes

The simplest classical error-correcting code is the repetition code. Suppose a bit 0 or 1 is transmitted through a binary symmetric channel (BSC), which flips each bit independently with probability $0 < p < \frac{1}{2}$. We encode

$$0 \longrightarrow 000$$
$$1 \longrightarrow 111$$

If at most one bit is flipped, the error can be detected and corrected by majority voting. For example, receiving 010 suggests that the second bit was flipped, so the decoder maps $010 \to 000$. This decision can of course be wrong: the transmitted word might have been 111 with flips on the first and third bits. For small p, however, such multiple-error events are unlikely. Without coding, the decoding error probability is p; with the three-bit repetition code it becomes $p^3+3p^2(1-p) = 3p^2-2p^3 < p$ for every $0 < p < \frac{1}{2}$.

Definition. A binary linear code is a k-dimensional vector subspace $C \subset \mathbf{F}_2^n$. It contains 2^k codewords of length n and carries k information bits. Its rate is $R = k/n$, and we say that the code has parameters (n, k). Two fundamental descriptions of a linear code are provided by a generator matrix and a parity-check matrix.

Generator matrix. A binary linear code can be specified by a linear map

$$\begin{aligned} \mathbf{F}_2^k &\to \mathbf{F}_2^n \\ \vec{u} &\mapsto \vec{x} = G\vec{u} \end{aligned}$$

where $\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$ is a column vector containing k information bits, and G is an $n \times k$ binary matrix. The vector $G\vec{u}$ is the corresponding length-n codeword, with all arithmetic performed modulo 2. To obtain a k-dimensional image, G must have rank k; equivalently, its k columns are linearly independent. The matrix G is called the *generator matrix*.

For example, the $(3, 1)$ repetition code has generator matrix

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Parity-check matrix. Since a linear code is a vector subspace of $\mathbf{F}_2^n$, it can also be represented as the kernel of a matrix H, namely the set of vectors satisfying

$$H\vec{x} = 0, \qquad H \text{ of dimension } (n-k) \times n$$

To obtain $\dim \ker H = k$, the rank of H must be $n - k$. We therefore usually choose H to be an $(n-k) \times n$ matrix of rank $n-k$, although the parity-check matrix is not unique.

Relation between the two matrices. For a given code, $HG = 0$: every generated codeword satisfies all parity checks. If $G = [\vec{g}_1 \cdots \vec{g}_k]$, choose $n - k$ independent vectors $\vec{h}_1, \ldots, \vec{h}_{n-k}$ spanning the orthogonal complement of the column space of G; these vectors form the rows of H.

$$H = \begin{bmatrix} \vec{h}_1^{\,T} \\ \vdots \\ \vec{h}_{n-k}^{\,T} \end{bmatrix}$$

Conversely, starting from H, one may choose a basis of $\ker H$ and use those basis vectors as the columns of a generator matrix G.

For example, one parity-check matrix for the $(3, 1)$ repetition code is

$$H = \begin{bmatrix} 1 & -1 & 0 \\ 0 & -1 & 1 \end{bmatrix}$$

Error detection, correction, and minimum distance. The parity-check matrix detects many transmission errors. Suppose a codeword $\vec{x}$ is transmitted and $\vec{x}' = \vec{x} + \vec{e}$ is received, where $\vec{e}$ has a 1 in each corrupted position and 0 elsewhere. Then

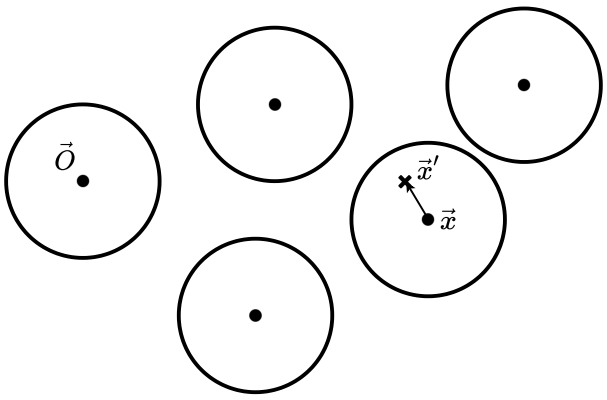
$$H\vec{x}' = H\vec{x} + H\vec{e} = H\vec{e}$$

The vector $H\vec{e}$ is called the *syndrome*. A nonzero syndrome certifies that an error has occurred; a zero syndrome may correspond either to no error or to an undetectable error. For a BSC, an error vector $\vec{e}$ of Hamming weight $|\vec{e}|$ occurs with probability $p^{|\vec{e}|}(1-p)^{n-|\vec{e}|}$. For $p < 1/2$, maximum-likelihood decoding is therefore equivalent to choosing the codeword $\vec{x}$ that minimizes the Hamming distance $d(\vec{x}, \vec{x}') = |\vec{e}|$. This is the *minimum-distance decoder*.

An important code parameter is the minimum distance $d = \min_{\vec{x} \neq \vec{x}' \in C} d(\vec{x}, \vec{x}')$. For a linear code this is equivalently the minimum Hamming weight of a nonzero codeword. We then write the parameters as (n, k, d).

Theorem. *An (n, k, d) code can correct every error pattern affecting at most t bits whenever $d \geq 2t + 1$, using minimum-distance decoding.*

Indeed, Hamming balls of radius $t \leq (d-1)/2$ centered on distinct codewords are disjoint. If at most t errors occur, the received word lies in exactly one such ball, whose center is therefore the unique nearest codeword.



Case (h!)

Theorem. *For a linear code, the minimum distance d is the smallest number of columns of the parity-check matrix H that are linearly dependent. Equivalently, every set of fewer than d columns is linearly independent.*

To see this, note that a nonzero codeword $\vec{x}$ satisfies $H\vec{x} = 0$. The nonzero entries of $\vec{x}$ therefore select a linearly dependent set of columns of H, and the Hamming weight of the smallest nonzero codeword is exactly the size of the smallest such dependent set.

Review of Hamming codes. Hamming codes are conveniently described by their parity-check matrix. Let $r \geq 2$, and let the columns of H be all $2^r - 1$ nonzero binary vectors of length r. Then $n = 2^r - 1$ and $n - k = r$, so $k = 2^r - r - 1$. The matrix has rank r because its columns include a basis of $\mathbf{F}_2^r$. The minimum distance is $d = 3$: no two columns are identical, whereas some three columns are linearly dependent. Hence Hamming codes correct one error. For example, the $(7, 4, 3)$ Hamming code has parity-check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Suppose an error occurs in the third bit. Then $\vec{e} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}^T$ and the syndrome $H\vec{e}$ equals the third column of H. The syndrome therefore identifies the corrupted bit directly, and flipping that bit corrects the error. This correction is guaranteed only when at most one error has occurred.

14.2 Quantum Repetition Codes

By analogy with the classical repetition code, consider the three-qubit encoding

$$|0\rangle \to |000\rangle$$
$$|1\rangle \to |111\rangle.$$

We shall use this code to protect against a *bit-flip channel*.

What is the corresponding detection and correction procedure for quantum information? The measurement basis must be chosen so that syndrome extraction does not reveal, and hence does not destroy, the encoded amplitudes. Here the output Hilbert space has dimension $2^3 = 8$. We use four orthogonal two-dimensional syndrome subspaces, represented by the following projectors:

$$
\begin{aligned}
P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \\
P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\
P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\
P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|.
\end{aligned}
$$

P_0 projects onto the no-error subspace, while P_1, P_2, and P_3 project onto the subspaces corresponding to a bit flip on the first, second, and third physical qubits, respectively. The input state $\alpha|0\rangle + \beta|1\rangle$ is encoded as

$$\alpha\,|000\rangle + \beta\,|111\rangle$$

Note that the quantum repetition code does not violate the no-cloning theorem: only the orthogonal computational-basis states are copied by the encoding circuit. The unknown state $\alpha|0\rangle + \beta|1\rangle$ is not cloned into three independent copies. If a single error occurs, say on the second qubit, the output state is

$$\alpha\,|010\rangle + \beta\,|101\rangle$$

A measurement in the basis $\{P_0, P_1, P_2, P_3\}$ preserves the state with probability 1 because

$$
\begin{aligned}
P_2\Big(\alpha\,|010\rangle + \beta\,|101\rangle\Big) &= \alpha\,|010\rangle + \beta\,|101\rangle \\
P_i\Big(\alpha\,|010\rangle + \beta\,|101\rangle\Big) &= 0, \qquad \text{for } i \neq 2.
\end{aligned}
$$

The syndrome measurement identifies an error on the second qubit without revealing the logical amplitudes. Correction is then performed by applying the unitary $\mathbb{1} \otimes X \otimes \mathbb{1}$.

$$\mathbb{1} \otimes X \otimes \mathbb{1}\Big(\alpha\,|010\rangle + \beta\,|101\rangle\Big) = \alpha\,|000\rangle + \beta\,|111\rangle.$$

As in the classical repetition code, this procedure does not reliably correct two or three simultaneous bit flips.

It is useful to describe the same error-correction procedure in terms of observables. Consider a syndrome measurement of

$$Z_1 \otimes Z_2 \otimes \mathbb{1} \qquad \text{and} \qquad \mathbb{1} \otimes Z_2 \otimes Z_3.$$

Because the two syndrome observables commute, they can be measured simultaneously. Each measurement yields an eigenvalue ± 1, and the pair of outcomes forms the

quantum analogue of a classical syndrome:

$$\begin{array}{llll} +1 & \text{and} & +1 & \longrightarrow \quad \text{no error} \\ -1 & \text{and} & +1 & \longrightarrow \quad \text{error on the first bit} \\ -1 & \text{and} & -1 & \longrightarrow \quad \text{error on the second bit} \\ +1 & \text{and} & -1 & \longrightarrow \quad \text{error on the third bit.} \end{array}$$

Once the error has been identified, it is corrected by applying the corresponding unitary operator:

$$\begin{array}{rcl} \text{no error} & \longrightarrow & \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \\ \text{first bit} & \longrightarrow & X_1 \otimes \mathbb{1} \otimes \mathbb{1} \\ \text{second bit} & \longrightarrow & \mathbb{1} \otimes X_2 \otimes \mathbb{1} \\ \text{third bit} & \longrightarrow & \mathbb{1} \otimes \mathbb{1} \otimes X_3. \end{array}$$

All stages—encoding, transmission, syndrome measurement, and correction—are legitimate quantum operations, consisting of unitary transformations and projective measurements.

The three-qubit repetition code does not protect against a phase-flip error. A phase flip on any one of the qubits changes the encoded state according to

$$\alpha\,|000\rangle - \beta\,|111\rangle$$

The syndrome of this phase-flipped state is still $(+1, +1)$, so the bit-flip code fails to detect the error. A repetition code adapted to phase-flip noise is obtained by working in the X basis, $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Encoding:

$$\begin{aligned} |0\rangle &\to |+\rangle \to |+\,+\,+\rangle \\ |1\rangle &\to |-\rangle \to |-\,-\,-\rangle. \end{aligned}$$

Error detection. Measure the commuting observables

$$X_1 \otimes X_2 \otimes \mathbb{1} \quad \text{and} \quad \mathbb{1} \otimes X_2 \otimes X_3$$

The measurement gives the syndromes:

$$\begin{array}{llll} +1 & \text{and} & +1 & \longrightarrow \quad \text{no error} \\ -1 & \text{and} & +1 & \longrightarrow \quad \text{error on the first qubit} \\ -1 & \text{and} & -1 & \longrightarrow \quad \text{error on the second qubit} \\ +1 & \text{and} & -1 & \longrightarrow \quad \text{error on the third qubit.} \end{array}$$

Error Correction

$$\begin{aligned} \text{no error} &\longrightarrow \mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1} \\ \text{first qubit} &\longrightarrow Z_1\otimes\mathbb{1}\otimes\mathbb{1} \\ \text{second qubit} &\longrightarrow \mathbb{1}\otimes Z_2\otimes\mathbb{1} \\ \text{third qubit} &\longrightarrow \mathbb{1}\otimes\mathbb{1}\otimes Z_3. \end{aligned}$$

For example, logical $|0\rangle$ is encoded as $|+++\rangle$. If a phase flip produces $|++-\rangle$, the syndrome is $(+1,-1)$, identifying an error on the third qubit. We then apply

$$\mathbb{1}\otimes\mathbb{1}\otimes Z_3|++-\rangle = |+++\rangle \to |0\rangle.$$

14.3 Shorś Code

The preceding construction is still incomplete because a realistic quantum channel may produce bit flips and phase flips simultaneously. We therefore seek a code that corrects both types of error. Shor introduced the first such quantum code, and the central ideas of his construction underlie many more general error-correcting codes.

If a code can correct both bit flips and phase flips, it can in fact correct an arbitrary single-qubit error. Any single-qubit noise operator can be decomposed in the Pauli basis $\{\mathbb{1}, X, Y, Z\}$, so it is sufficient to correct the corresponding discrete error components. In particular, this covers channels of the form

$$\mathcal{E}(\varrho) = p_0\varrho + p_1 X\varrho X + p_2 Y\varrho Y + p_3 Z\varrho Z$$

with $p_0 + p_1 + p_2 + p_3 = 1$. This includes bit-flip, phase-flip, bit-phase-flip, and depolarizing Pauli channels. More general noise processes may also change amplitudes coherently; after syndrome measurement, however, arbitrary single-qubit errors can be analyzed through their Pauli components.

The central idea of Shorś code is to *concatenate* the two repetition codes. Concatenation is a standard construction in classical coding theory: a codeword of one code is itself encoded using another code. Here the logical basis states are constructed as follows:

$$
\begin{aligned}
|0\rangle \to |+\rangle \longrightarrow |+++\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
&\longrightarrow \frac{|000\rangle+|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle+|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle+|111\rangle}{\sqrt{2}} \equiv |0\rangle_S \\
|1\rangle \to |-\rangle \longrightarrow |---\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\longrightarrow \frac{|000\rangle-|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle-|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle-|111\rangle}{\sqrt{2}} \equiv |1\rangle_S
\end{aligned}
$$

Each logical qubit is therefore encoded into nine physical qubits, giving rate $1/9$. Denote the two logical basis states by $|0\rangle_S$ and $|1\rangle_S$. A general encoded state is

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \to |\psi_S\rangle = \alpha\,|0\rangle_S + \beta\,|1\rangle_S.$$

The circuit in Figure **14.1** implements this encoding unitarily.

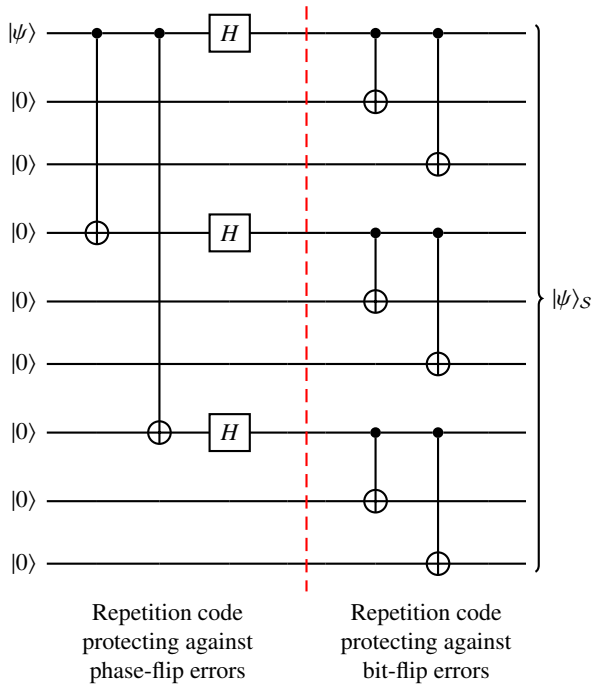


Figure 14.1 Encoding circuit for Shors nine-qubit code.

We now show that this code protects against any single-qubit Pauli error generated by $\mathbb{1}$ (no error), X (bit flip), Z (phase flip), or Y (bit and phase flip). Equivalently, if one physical qubit is affected, the corrupted state can be distinguished by syndrome

measurements and corrected without learning the logical amplitudes, thereby recovering $|\psi\rangle_S$ and hence the original logical state $|\psi\rangle$.

Bit-flip errors. Consider first an X error on one of the first three qubits. Measuring Z_1Z_2 and Z_2Z_3 identifies which qubit, if any, has flipped, exactly as in the three-qubit repetition code. Applying the corresponding X_i corrects the error. Repeating the same syndrome measurements on all three blocks amounts to measuring

$$Z_1Z_2 \text{ and } Z_2Z_3, \qquad Z_4Z_5 \text{ and } Z_5Z_6, \qquad Z_7Z_8 \text{ and } Z_8Z_9.$$

All these operators commute and the simultaneous measurement is possible.

Phase-flip errors. Consider now a Z error on one of the first three qubits. A phase flip on the second qubit changes the encoded state to $Z_2|\psi\rangle_S$ at the output of the channel:

$$Z_2|0\rangle_S = \frac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

and

$$Z_2|1\rangle_S = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

This error can be detected without revealing the logical amplitudes by measuring the two commuting stabilizers

$$(X_1X_2X_3)(X_4X_5X_6) \qquad \text{and} \qquad (X_4X_5X_6)(X_7X_8X_9)$$

For the error above, for example,

$$(X_1X_2X_3)(X_4X_5X_6)(Z_2|\psi_S\rangle) = -(Z_2|\psi_S\rangle)$$

and

$$(X_4X_5X_6)(X_7X_8X_9)(Z_2|\psi_S\rangle) = +(Z_2|\psi_S\rangle)$$

We conclude that a phase-flip error has occurred somewhere in the first block of three qubits. It is not necessary to determine which qubit within that block was affected: applying $Z_1Z_2Z_3$ corrects the logical phase error.

$$Z_1Z_2Z_3(Z_2|\psi_S\rangle) = |\psi_S\rangle.$$

Bit-and-phase-flip errors. As an illustration, consider a Y-type error on the fourth physical qubit. The channel output is

$$X_4Z_4|\psi_S\rangle.$$

First detect the bit-flip component by measuring the Z-type stabilizers:

$$\begin{aligned}
Z_1Z_2(X_4Z_4|\psi_S\rangle) &= X_4Z_4|\psi_S\rangle \\
Z_2Z_3(X_4Z_4|\psi_S\rangle) &= X_4Z_4|\psi_S\rangle \\
Z_4Z_5(X_4Z_4|\psi_S\rangle) &= -(X_4Z_4|\psi_S\rangle) \qquad (\text{since } Z_4X_4 = -X_4Z_4) \\
Z_5Z_6(X_4Z_4|\psi_S\rangle) &= X_4Z_4|\psi_S\rangle \\
Z_7Z_8(X_4Z_4|\psi_S\rangle) &= X_4Z_4|\psi_S\rangle \\
Z_8Z_9(X_4Z_4|\psi_S\rangle) &= X_4Z_4|\psi_S\rangle
\end{aligned}$$

we conclude that a bit flip has occurred on the fourth physical qubit. We then diagnose phase flips using

$$\begin{aligned}
X_1X_2X_3\,X_4X_5X_6(X_4Z_4|\psi_S\rangle) &= -X_4Z_4|\psi_S\rangle \qquad (\text{since } Z_4X_4 = -X_4Z_4) \\
X_4X_5X_6\,X_7X_8X_9(X_4Z_4|\psi_S\rangle) &= -X_4Z_4|\psi_S\rangle
\end{aligned}$$

which shows that a phase flip has also occurred on the fourth qubit. The state is corrected by applying X_4Z_4: $X_4Z_4\,(X_4Z_4)|\psi_S\rangle = |\psi_S\rangle$.

General single-qubit error correction. The preceding examples can be summarized in a unified way. Consider an arbitrary channel acting on the encoded density matrix:

$$|\psi_S\rangle\langle\psi_S| \to \mathcal{E}(|\psi_S\rangle\langle\psi_S|)$$

A measurement of the observables Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9 and Measuring the stabilizer observables projects the noisy state onto a joint eigenspace labeled by eigenvalues ± 1. When the dominant errors affect at most one physical qubit, the resulting syndrome identifies one of the discrete Pauli error patterns discussed above—bit flip, phase flip, or both—and the corresponding unitary correction can be applied. If multiple physical qubits are corrupted, the same decoder need not return the correct logical state; the probability of such events is small only when the physical noise is sufficiently weak.

In summary, Shorś code encodes one logical qubit into nine physical qubits and corrects an arbitrary single-qubit error. Its code space is the two-dimensional subspace spanned by $|0\rangle_S$ and $|1\rangle_S$ inside the 2^9-dimensional nine-qubit Hilbert space. In standard notation Shorś code is a $[[9, 1, 3]]$ quantum code.

14.4 Stabilizer Formalism

This section may be skipped on a first reading.

Shorś construction reveals an algebraic structure that underlies much more general quantum error-correcting codes. In the preceding discussion we found that

1. Every codeword $|\Psi\rangle$ of Shorś code is a simultaneous $+1$ eigenstate of the stabilizer observables $Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9$, and $X_1X_2X_3\,X_4X_5X_6, X_4X_5X_6\,X_7X_8X_9$. These commuting Pauli operators are the *stabilizer generators* of the code.
2. These operators commute with one another, so they can be measured simultaneously.
3. If $|\Psi\rangle$ is corrupted by a single-qubit Pauli error, the corrupted state is still a simultaneous eigenvector of the stabilizer generators, but some eigenvalues change sign.[1]
4. The syndrome is the list of stabilizer eigenvalues measured on the corrupted state.

Remark. Stabilizer generators are the quantum analogue of parity-check equations. Each condition $O_j|\Psi\rangle = |\Psi\rangle$ defines a parity-like constraint on the code space, while the measured eigenvalues ± 1 form the syndrome. For CSS-type codes one can naturally separate Z-type checks, which diagnose bit flips, from X-type checks, which diagnose phase flips.

To generalize this construction, introduce the n-qubit Pauli group $\mathcal{P}^n$, consisting of all tensor products of the single-qubit Pauli operators X_j, Y_j, and Z_j, multiplied by phases ± 1 or $\pm i$. Any two Pauli operators either commute or anticommute. A subgroup $\mathcal{S} \subset \mathcal{P}^n$ whose elements commute is called a *stabilizer group*. It can be generated by an independent set $\{O_1, \ldots, O_m\}$. The Hilbert subspace $\mathcal{H} \subset (\mathbb{C}^2)^{\otimes n}$ consisting of states $|\Psi\rangle$ satisfying

$$O_j|\Psi\rangle = 1 \cdot |\Psi\rangle, \qquad j = 1, \ldots, m$$

defines a quantum code of length n and dimension 2^{n-m}. Every code state is stabilized by the group $\mathcal{S}$ generated by the commuting observables $O_1, \ldots, O_m$. These observables can be measured simultaneously. A Pauli error, or a coherent linear combination of Pauli errors followed by syndrome measurement, projects the state into a syndrome subspace of the form

$$E_k|\Psi\rangle = |\Psi'\rangle$$

where $E_k \in \mathcal{P}^n$. The corrupted state remains a simultaneous eigenstate of the stabilizer generators, so measuring them does not reveal the encoded logical amplitudes. The measurement outcomes are eigenvalues $\lambda_1, \ldots, \lambda_m \in \{\pm 1\}$; their list is the *syndrome*. If the error E_k anticommutes with a generator O_j, then

$$O_j|\Psi'\rangle = O_jE_k|\Psi\rangle = -E_kO_j|\Psi\rangle = -E_k|\Psi\rangle = -|\Psi'\rangle$$

i.e. some stabilizer eigenvalues are -1. For a given code, one can tabulate the syndrome associated with each correctable error. Once an error has been diagnosed, it is corrected by applying an appropriate unitary operator.

$$|\Psi'\rangle \mapsto E_k|\Psi'\rangle = E_k^2|\Psi\rangle = |\Psi\rangle$$

Every Pauli operator can be written, up to an overall phase, as a product of X operators

[1] For a linear combination of Pauli errors, stabilizer measurement projects the state onto one of the corresponding discrete syndrome subspaces.

times a product of Z operators, since $Y = iXZ$. For example,

$$X_1\mathbb{1}_2Y_3Z_4Y_5\mathbb{1}_6 = -(X_1\mathbb{1}_2X_3\mathbb{1}_4X_5\mathbb{1}_6)(\mathbb{1}_1\mathbb{1}_2Z_3Z_4Z_5\mathbb{1}_6)$$

It is useful to introduce a binary, "semiclassical representation of this formalism. The Pauli product on the previous line can be encoded by the binary row vector

$$\begin{pmatrix}1 & 0 & 1 & 0 & 1 & 0 & | & 0 & 0 & 1 & 1 & 1 & 0\end{pmatrix}$$

Applying this representation to all stabilizer generators O_j yields a matrix of the form

$$(A_1 \mid A_2)$$

is sometimes called a *quantum parity-check matrix*. Each row encodes one stabilizer constraint $O_j|\Psi\rangle = |\Psi\rangle$. The requirement that all stabilizer generators commute is equivalent to

$$A_1A_2^T + A_2A_1^T = 0$$

This condition expresses orthogonality of the rows with respect to the binary symplectic inner product. An error operator E can similarly be represented by an error vector $(\vec{e}_1 \mid \vec{e}_2)$. The syndrome is then

$$A_1\vec{e}_1 + A_2\vec{e}_2 = \vec{s}$$

Quantum error correction can therefore be reduced, for this class of codes, to classical syndrome decoding—that is, solving binary linear equations. This connection is particularly useful because classical coding theory provides a large collection of efficient constructions and decoding algorithms.

Shorś code has a particularly transparent block structure:

$$(A_1 \mid A_2) = \left[\begin{array}{ccccccccc|ccccccccc}
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1
\end{array}\right]$$

Codes whose quantum parity-check matrix has this block form are Calderbank–Shor–Steane (CSS) codes. In general, such a code is represented by

$$(A_1 \mid A_2) = \begin{bmatrix}H_1 & | & 0\\ 0 & | & G_2^T\end{bmatrix}$$

with the orthogonality constraint

$$H_1 G_2 = 0$$

One may interpret H_1 as the parity-check matrix of a classical code C_1 and G_2 as a generator matrix of a second classical code C_2. Equivalently, G_2^T is a parity-check matrix for $C_2^\perp$. The orthogonality condition is precisely $C_2^\perp \subseteq C_1$. Decoding then reduces to solving classical syndrome equations for the two component codes.

We study this construction in detail in Section **14.5**. The code C_1 protects against bit-flip errors, whereas $C_2^\perp$ protects against phase-flip errors. Using the two codes simultaneously protects against arbitrary combinations of the two error types.

14.5 Calderbank-Shor-Steane Codes

This paragraph can be lu independently of the previous.

Calderbank–Shor–Steane codes form an important subclass of stabilizer codes whose structure is especially easy to analyze. A CSS code combines two classical linear codes: one is used to correct bit flips and the other to correct phase flips.

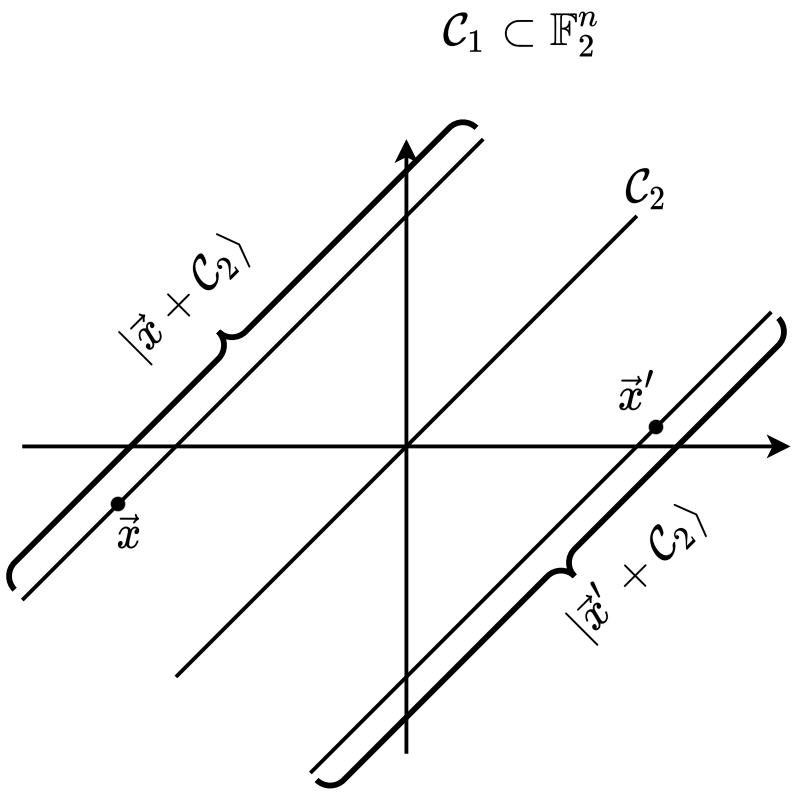
Let C_1 and C_2 be binary linear codes with $C_2 \subseteq C_1$, of parameters (n, k_1) and (n, k_2). Thus $C_1 \subseteq \mathbf{F}_2^n$ has dimension k_1 and C_2 has dimension $k_2 \leq k_1$. Assume that both C_1 and $C_2^\perp$ correct up to t errors, for example because their minimum distances are at least $2t + 1$. The dual code $C_2^\perp$ has dimension $n - k_2$.

Because C_2 is a subgroup of C_1, we may consider the quotient C_1/C_2. For $\vec{x} \in C_1$, the coset of $\vec{x}$ is $\{\vec{x} + \vec{y} : \vec{y} \in C_2\}$. Define

$$|\vec{x} + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} |\vec{x} + \vec{y}\rangle$$

This ket not depends that of the class of equivalence associated to $\vec{x}$ and no not of the representative special chosen.

Case (h!)



The ket $|\vec{x} + C_2\rangle$ is the superposition coherent of all the states in the class of equivalence $\vec{x}+C_2$. For two classes of equivalence different $\vec{x}+C_2$ and $\vec{x}'+C_2$ (that is that $\vec{x}-\vec{x}' \notin C_2$) the kets associated are perpendiculaires :

$$\langle \vec{x} + C_2 | \vec{x}' + C_2 \rangle = 0$$

It y a $\frac{|C_1|}{|C_2|} = 2^{k_1-k_2}$ classes of equivalence and therefore $2^{k_1-k_2}$ vectors orthogonal.

The CSS code CSS(C_1, C_2) is the Hilbert subspace spanned by these $2^{k_1-k_2}$ orthonormal vectors. It is a subspace of the 2^n-dimensional Hilbert space of n qubits. The code encodes $k_1 - k_2$ logical qubits into n physical qubits. We now show that if C_1 and $C_2^\perp$ each correct t classical errors, then CSS(C_1, C_2) corrects up to t bit flips and up to t phase flips.

It is enough to prove the correction procedure on the logical basis states, since linearity then extends it to arbitrary superpositions. Let $\vec{e}_1$ and $\vec{e}_2$ denote the binary error patterns for bit flips and phase flips, respectively, each of Hamming weight at most t. The corrupted state is

$$|\psi\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}+\vec{e}_1\rangle$$

To correct the state, we must extract the bit-flip and phase-flip syndromes without measuring the logical information. We therefore append ancillary registers and start from

$$|\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$$

Correction of bit flips. The syndrome of the first classical code is $H_1(\vec{x}+\vec{y}+\vec{e}_1) = H_1\vec{e}_1$, because $\vec{x}+\vec{y} \in C_1$. It can be computed coherently by a unitary transformation:

$$U_1|\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0\rangle^{\otimes n}$$

so that

$$U_1|\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0\rangle^{\otimes n}$$

Measuring the second register yields $|H_1\vec{e}_1\rangle$ with probability one. Thus the syndrome $H_1\vec{e}_1$ becomes known classically. If $|\vec{e}_1| \le t$, a decoder for C_1 recovers the bit-flip pattern, and we apply the corresponding unitary

$$\prod_{\substack{\text{components of} \\ \vec{e}_1 \text{ equal to 1}}} X_i \equiv U_{1,\text{corr}}$$

to correct the bit flips. This gives

$$U_{1,\text{corr}}U_1|\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0\rangle^{\otimes n}$$

Correction of phase flips. We first apply $H^{\otimes n}$, which exchanges the roles of X- and Z-type errors and moves to a basis in which phase errors can be decoded as bit errors:

$$\begin{aligned}
&H^{\otimes n}U_{1,\text{corr}}U_1|\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} \\
=&\frac{1}{2^{n/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} \sum_{\vec{z}} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{z}\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0\rangle^{\otimes n} \\
=&\frac{1}{2^{n/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{z}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{z}+\vec{e}_2)\cdot(\vec{x}+\vec{y})} |\vec{z}\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0\rangle^{\otimes n} \\
=&\frac{1}{2^{n/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{z}} \sum_{\vec{y}\in C_2} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{z}+\vec{e}_2\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0\rangle^{\otimes n} = \ldots
\end{aligned}$$

Note that

$$\sum_{\vec{y}\in C_2} (-1)^{\vec{z}\cdot\vec{y}} = \begin{cases} |C_2| & \text{if } \vec{z} \in C_2^{\perp} \\ 0 & \text{otherwise} \end{cases}$$

and therefore the state becomes

$$\ldots = \frac{1}{|C_2^\perp|} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}} |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0\rangle^{\otimes n}.$$

We now compute the syndrome of $C_2^\perp$ coherently and store it in the final register:

$$\begin{aligned} U_2 |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0\rangle^{\otimes n} \\ &= |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp (\vec{z} + \vec{e}_2)\rangle \\ &= |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

where $H_2^\perp$ is a parity-check matrix of $C_2^\perp$. The resulting state is

$$\begin{aligned} &U_2 H^{\otimes n} U_{1,\mathrm{corr}} U_1 |\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} \\ =&\frac{1}{\sqrt{|C_2^\perp|}} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}} |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

Measuring the last register yields $|H_2^\perp \vec{e}_2\rangle$ with probability one. If $|\vec{e}_2| \leq t$, a decoder for $C_2^\perp$ recovers the phase-error pattern, allowing us to apply the unitary

$$\prod_{\substack{\text{components of} \\ \vec{e}_2 \text{ equal to 1}}} X_i \equiv U_{2,\mathrm{corr}}$$

to remove the phase-error syndrome. We obtain

$$\begin{aligned} &U_{2,\mathrm{corr}} U_2 H^{\otimes n} U_{1,\mathrm{corr}} U_1 |\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} \\ =&\frac{1}{\sqrt{|C_2^\perp|}} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}} |\vec{z}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

Finally, apply $H^{\otimes n}$ once more to return to the original computational basis:

$$\begin{aligned} &H^{\otimes n} U_{2,\mathrm{corr}} U_2 H^{\otimes n} U_{1,\mathrm{corr}} U_1 |\psi\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} \\ =&\frac{1}{\sqrt{|C_2^\perp|}} \frac{1}{2^{n/2}} \sum_{\vec{z} \in C_2^\perp} \sum_{\vec{y}} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{y}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle \\ =&\frac{1}{\sqrt{|C_2^\perp|}} \frac{1}{2^{n/2}} \sum_{\vec{z} \in C_2^\perp} \sum_{\vec{y}} (-1)^{\vec{z}\cdot\vec{y}} |\vec{y} + \vec{x}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

As before,

$$\sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{y}} = \begin{cases} |C_2^\perp| & \text{if } \vec{y} \in (C_2^\perp)^\perp = C_2 \\ 0 & \text{otherwise} \end{cases}$$

The final state is therefore

$$\left(\frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} |\vec{x} + \vec{y}\rangle \right) \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle.$$

The original logical codeword has been recovered in the first register.

Part III

Physical realizations

15 Spin Dynamics

A spin-1/2 degree of freedom, such as the magnetic moment of certain atomic nuclei, provides one of the most important physical realizations of a qubit. Spins can be manipulated accurately with time-dependent magnetic fields; this is the basis of nuclear magnetic resonance (NMR) and also provides a natural mechanism for implementing quantum gates. In this chapter we show how resonant magnetic fields generate single-qubit operations, including NOT and Hadamard gates. Two-qubit gates require an interaction between two magnetic moments. Their implementation will be discussed in Chapter **16**.

15.1 The Bloch Sphere

We begin with a brief review of the Bloch sphere introduced in Section **2.10**. Any pure qubit state can be parametrized as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|\downarrow\rangle \tag{15.1}$$

The two complex amplitudes can be represented geometrically by a point on the Bloch sphere: θ is the polar angle from the z axis and ϕ is the azimuthal angle in the xy plane measured from the x axis; see Figure **15.1**.

It is useful to recall the three standard measurement bases introduced in Chapter **2**. The Z basis $\{|\uparrow\rangle, |\downarrow\rangle\}$ corresponds to antipodal points on the z axis, the X basis $\{|+\rangle, |-\rangle\}$ to antipodal points on the x axis, and the Y basis $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$ to antipodal points on the y axis.

Consider the matrix

$$\vec{\sigma}\cdot\vec{n} = \sigma_x n_x + \sigma_y n_y + \sigma_z n_z \tag{15.2}$$

where $(\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices and $\vec{n} = (n_x, n_y, n_z)$ is a unit vector. Writing $n_x = \sin\theta\cos\phi$, $n_y = \sin\theta\sin\phi$, and $n_z = \cos\theta$, the vector $\vec{n}$ is precisely the point on the Bloch sphere associated with $|\psi\rangle$. One verifies that

$$\vec{\sigma}\cdot\vec{n}|\psi\rangle = (+1)|\psi\rangle \tag{15.3}$$

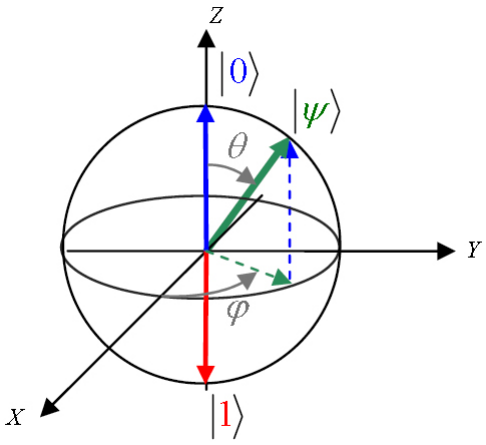


Figure 15.1 The Bloch sphere.

Thus $|\psi\rangle$ is the $+1$ eigenstate of $\vec{\sigma}\cdot\vec{n}$. Geometrically, the Bloch vector $\vec{n}$ identifies the spin direction associated with the state.

The exponential of $\vec{\sigma}\cdot\vec{n}$ obeys the useful generalized Euler identity

$$\exp\left(i\frac{\alpha}{2}\vec{\sigma}\cdot\vec{n}\right) = \cos\left(\frac{\alpha}{2}\right)\mathbb{1} + i(\vec{\sigma}\cdot\vec{n})\sin\left(\frac{\alpha}{2}\right). \tag{15.4}$$

To see the meaning of this 2×2 unitary, take the special case $\vec{n} = (0,0,1)$ and apply it to $|\psi\rangle$.

$$\exp\left(i\frac{\alpha}{2}\sigma_z\right) = \exp\left(i\frac{\alpha}{2}\sigma_z\right)\left\{\cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle\right\} \tag{15.5}$$

$$= e^{i\frac{\alpha}{2}}\cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + e^{i\phi}e^{-i\frac{\alpha}{2}}\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle \tag{15.6}$$

$$= e^{i\frac{\alpha}{2}}\left\{\cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + e^{i(\phi-\alpha)}\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle\right\} \tag{15.7}$$

The prefactor $e^{i\alpha/2}$ is a global phase and has no physical effect. The polar angle θ is unchanged, while the azimuthal angle changes from ϕ to $\phi-\alpha$. Thus $\exp(i\alpha\sigma_z/2)$ represents a rotation by $-\alpha$ about the z axis, whereas $\exp(-i\alpha\sigma_z/2)$ represents a rotation by $+\alpha$.

More generally, $\exp(-i\alpha\,\vec{\sigma}\cdot\vec{n}/2)$ represents a rotation by angle α about the axis $\vec{n}$ on the Bloch sphere.

The dynamics of a spin in a static magnetic field will lead directly to this type of rotation, with the field direction defining the rotation axis.

15.2 Spin Hamiltonian in a Magnetic Field

As recalled in Section 2.7, the interaction energy of a magnetic moment $\vec{M}$ with a magnetic field $\vec{B}$ is

$$E = -\vec{M} \cdot \vec{B} \tag{15.8}$$

In quantum mechanics the magnetic moment becomes an observable. For a spin-1/2 particle, such as an electron, proton, or suitable atomic nucleus,

$$\vec{M} = \frac{g\hbar}{2}\vec{\sigma} \tag{15.9}$$

where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli matrices. The interaction Hamiltonian of a spin-1/2 magnetic moment with the field is therefore the Hermitian 2×2 matrix

$$H = -\frac{g\hbar}{2}\vec{B} \cdot \vec{\sigma} \tag{15.10}$$

In matrix form,

$$H = -\frac{g\hbar}{2}\begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix} \tag{15.11}$$

For a static magnetic field we may choose the z axis along $\vec{B} = (0, 0, B)$, so that

$$H = -\frac{g\hbar}{2}B\sigma_z \equiv -\frac{\hbar\omega_0}{2}\sigma_z = -\frac{\hbar\omega_0}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{15.12}$$

where $\omega_0 = gB$ is the Larmor angular frequency. The eigenvalues are $-\hbar\omega_0/2$ and $+\hbar\omega_0/2$, with eigenvectors $|\uparrow\rangle$ and $|\downarrow\rangle$ respectively. These two levels are shown schematically in Figure 15.2.

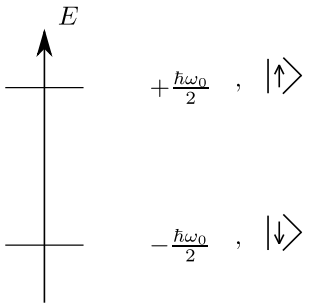


Figure 15.2 Energy levels of a spin-1/2 particle in a static magnetic field.

Any two-level quantum system has a Hamiltonian of this general form, at least after a suitable choice of basis and energy scale. The analysis below therefore applies much more broadly than to magnetic moments alone.

We shall also need a time-dependent magnetic field of the form

$$\vec{B} = (0, 0, B_0) + (B_1 \cos(\omega t), -B_1 \sin(\omega t), 0) \tag{15.13}$$

This field consists of a static component along z and a transverse component rotating in the xy plane. The corresponding Hamiltonian is

$$H = -\frac{g\hbar}{2}\begin{pmatrix} B_0 & B_1\Big(\cos(\omega t) + i\sin(\omega t)\Big) \\ B_1\Big(\cos(\omega t) - i\sin(\omega t)\Big) & B_0 \end{pmatrix} \tag{15.14}$$

Introduce the raising and lowering operators

$$\sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \sigma_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{15.15}$$

In terms of these operators, the Hamiltonian can be written as

$$H = -\frac{\hbar\omega_0}{2}\sigma_z - \frac{\hbar\omega_1}{2}\Big(\sigma_+ e^{i\omega t} + \sigma_- e^{-i\omega t}\Big) \tag{15.16}$$

Because of the time-dependent transverse term, $|\uparrow\rangle$ and $|\downarrow\rangle$ are no longer stationary eigenstates of the full Hamiltonian. The operators σ_+ and σ_- generate transitions between them:

$$\sigma_+|\downarrow\rangle = |\uparrow\rangle \quad \text{and} \quad \sigma_+|\uparrow\rangle = 0 \tag{15.17}$$

$$\sigma_-|\uparrow\rangle = |\downarrow\rangle \quad \text{and} \quad \sigma_-|\downarrow\rangle = 0 \tag{15.18}$$

These raising and lowering terms induce transitions between the two energy levels of the static Hamiltonian. Such transitions are the basis of NMR control and of the single-qubit gates discussed below.

15.3 Larmor Precession

We first study a state $|\psi\rangle = \cos(\theta/2)|\uparrow\rangle + e^{i\phi}\sin(\theta/2)|\downarrow\rangle$ in a constant magnetic field $\vec{B} = (0, 0, B_0)$ directed along z.

According to the postulates of quantum mechanics, the time evolution is unitary:

$$U(t,0)|\psi\rangle \equiv |\psi(t)\rangle \tag{15.19}$$

with the composition law $U(t_3,t_2)U(t_2,t_1) = U(t_3,t_1)$. Here $U(t,s)$ denotes evolution from time s to time t. The evolution operator satisfies the Schrödinger equation

$$i\hbar\frac{d}{dt}U(t,0) = HU(t,0) \tag{15.20}$$

The task is therefore to solve this Schrödinger equation for the relevant Hamiltonian.

When H is time independent, the solution is simply

$$U(t,0) = \exp\left(-i\frac{t}{\hbar}H\right) \tag{15.21}$$

If H depends explicitly on time, this simple exponential form is generally no longer valid because Hamiltonians at different times need not commute.

For the constant field $\vec{B} = (0,0,B_0)$, the Hamiltonian $H = -\frac{\hbar\omega_0}{2}\sigma_z$ is time independent, and therefore

$$U(t,0) = \exp\left(it\frac{\omega_0}{2}\sigma_z\right) \tag{15.22}$$

This is precisely a rotation about the z axis with angular velocity ω_0. Therefore

$$|\psi(t)\rangle = \exp\left(i\frac{t\omega_0}{2}\sigma_z\right)|\psi(0)\rangle \tag{15.23}$$

$$= \exp\left(i\frac{t\omega_0}{2}\sigma_z\right)\left\{\cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle\right\} \tag{15.24}$$

$$= \exp\left(i\frac{t\omega_0}{2}\right)\cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + e^{i\phi}\exp\left(-i\frac{t\omega_0}{2}\right)\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle \tag{15.25}$$

$$= \exp\left(i\frac{t\omega_0}{2}\right)\left\{\cos\left(\frac{\theta}{2}\right)|\uparrow\rangle + \exp\left(i(\phi - t\omega_0)\right)\sin\left(\frac{\theta}{2}\right)|\downarrow\rangle\right\} \tag{15.26}$$

The polar angle θ remains fixed while the azimuthal angle evolves as $\phi(t) = \phi - \omega_0 t$. On the Bloch sphere this is a uniform precession about the magnetic-field direction, known as Larmor precession, with angular frequency ω_0 and period $T_0 = 2\pi/\omega_0$.

15.4 Rabi oscillations

We now consider a spin in the rotating magnetic field $\vec{B} = (0,0,B_0)+B_1(\cos\omega t, -\sin\omega t, 0)$.

The evolution operator still satisfies the Schrödinger equation

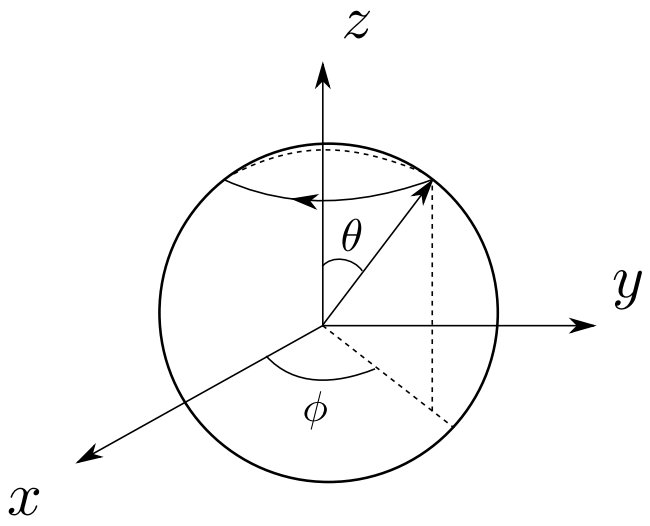


Figure 15.3 Larmor precession on the Bloch sphere. The Bloch vector, specified by θ and ϕ, precesses about the z axis at angular frequency ω_0.

$$i\hbar\frac{d}{dt}U(t,0) = H(t)U(t,0) \tag{15.27}$$

with

$$H(t) = -\frac{\hbar\omega_0}{2}\sigma_z - \frac{\hbar\omega_1}{2}\left(\sigma_+ e^{i\omega t} + \sigma_- e^{-i\omega t}\right) \tag{15.28}$$

Because $H(t)$ is time dependent, the Schrödinger equation is less convenient to solve directly. We remove this explicit time dependence by moving to a frame rotating about the z axis. Define

$$|\tilde{\psi}(t)\rangle = \exp\left(i\frac{t}{\hbar}K\right)|\psi(t)\rangle \tag{15.29}$$

with $K = \begin{pmatrix} -\frac{\hbar\omega}{2} & 0 \\ 0 & \frac{\hbar\omega}{2} \end{pmatrix}$.

The matrix $e^{itK/\hbar}$ represents a rotation of the reference frame about z at angular frequency ω. Since $|\psi(t)\rangle = U(t,0)|\psi(0)\rangle$, we obtain

$$|\tilde{\psi}(t)\rangle = \exp\left(i\frac{t}{\hbar}K\right)U(t,0)|\psi(0)\rangle \tag{15.30}$$

$$\equiv \tilde{U}(t,0)|\psi(0)\rangle \tag{15.31}$$

The corresponding evolution operator in the rotating frame is $\tilde{U}(t,0) = e^{itK/\hbar}U(t,0)$. Differentiating gives

$$i\hbar\frac{d}{dt}\tilde{U} = i\hbar\frac{i}{\hbar}Ke^{i\frac{t}{\hbar}K}U + e^{i\frac{t}{\hbar}K}H(t)U \tag{15.32}$$

$$= \left\{-K + e^{i\frac{tK}{\hbar}}H(t)e^{-i\frac{tK}{\hbar}}\right\}\tilde{U} \tag{15.33}$$

$$\equiv \tilde{H}(t)\tilde{U} \tag{15.34}$$

The rotating-frame Hamiltonian is thus $\tilde{H}$. It is straightforward to evaluate because

$$e^{i\frac{tK}{\hbar}} = \begin{pmatrix} e^{-i\frac{t\omega}{2}} & 0 \\ 0 & e^{i\frac{t\omega}{2}} \end{pmatrix} \tag{15.35}$$

Substituting into the expression above yields the time-independent Hamiltonian

$$\tilde{H} = \frac{\hbar\delta}{2}\sigma_z - \frac{\hbar\omega_1}{2}\sigma_x \tag{15.36}$$

where $\delta = \omega - \omega_0$ is the detuning. The rotating-frame evolution operator is therefore

$$\tilde{U} = \exp\left(-\frac{it}{\hbar}\tilde{H}\right) = \exp\left\{-i\frac{t}{2}(\delta\sigma_z - \omega_1\sigma_x)\right\} \tag{15.37}$$

This exponential is evaluated directly using the generalized Euler identity (15.4). Transforming back to the laboratory frame,

$$U = e^{-i\frac{t}{\hbar}K}\tilde{U} \tag{15.38}$$

Transforming back to the laboratory frame gives the exact evolution operator

$$U(t,0) = \begin{pmatrix} u_{\uparrow\uparrow} & u_{\uparrow\downarrow} \\ u_{\downarrow\uparrow} & u_{\downarrow\downarrow} \end{pmatrix} \tag{15.39}$$

with matrix elements

$$u_{\uparrow\uparrow} = e^{i\frac{t\omega}{2}}\left\{\cos\left(\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right) + i\frac{\delta}{\sqrt{\delta^2+\omega_1^2}}\sin\left(\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right)\right\} \tag{15.40}$$

$$u_{\uparrow\downarrow} = -i\frac{i\omega_1}{\sqrt{\delta^2+\omega_1^2}}e^{i\frac{t\omega}{2}}\sin\left(\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right) \tag{15.41}$$

$$u_{\downarrow\uparrow} = -i\frac{i\omega_1}{\sqrt{\delta^2+\omega_1^2}}e^{-i\frac{t\omega}{2}}\sin\left(\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right) \tag{15.42}$$

$$u_{\downarrow\downarrow} = e^{-i\frac{t\omega}{2}}\left\{\cos\left(\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right) - i\frac{\delta}{\sqrt{\delta^2+\omega_1^2}}\sin\left(\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right)\right\} \tag{15.43}$$

We have therefore solved the dynamics exactly for a spin driven by a rotating field of the form $(B_1 \cos \omega t, -B_1 \sin \omega t, B_0)$. From the evolution operator we can compute the transition probabilities

$$P_{|\uparrow\rangle \to |\downarrow\rangle}(t) = |\langle\downarrow|U(t)|\uparrow\rangle|^2 = |u_{\uparrow\downarrow}|^2 \tag{15.44}$$

$$P_{|\uparrow\rangle \to |\uparrow\rangle}(t) = |\langle\uparrow|U(t)|\uparrow\rangle|^2 = |u_{\uparrow\uparrow}|^2 \tag{15.45}$$

The first quantity is the probability that a spin initially in $|\uparrow\rangle$ is found in $|\downarrow\rangle$ at time t; the second is the probability that it remains in $|\uparrow\rangle$. This gives

$$\begin{cases} P_{|\uparrow\rangle \to |\downarrow\rangle}(t) & = \dfrac{\omega_1^2}{\delta^2 + \omega_1^2}\left(\sin\left(\dfrac{t}{2}\sqrt{\delta^2 + \omega_1^2}\right)\right)^2 \\ P_{|\uparrow\rangle \to |\uparrow\rangle}(t) & \end{cases} \tag{15.46}$$

As required by unitarity, these two probabilities sum to one.

Figure Figure **15.4** shows $P_{\uparrow\to\downarrow}(t)$. It oscillates with Rabi period $T_{\text{Rabi}} = 2\pi/\sqrt{\delta^2 + \omega_1^2}$ and maximum amplitude $\omega_1^2/(\delta^2 + \omega_1^2)$. The amplitude is maximal at resonance, $\delta = 0$ or $\omega = \omega_0$. Far from resonance, $|\delta| \gg \omega_1$, transitions are strongly suppressed; δ is called the detuning.

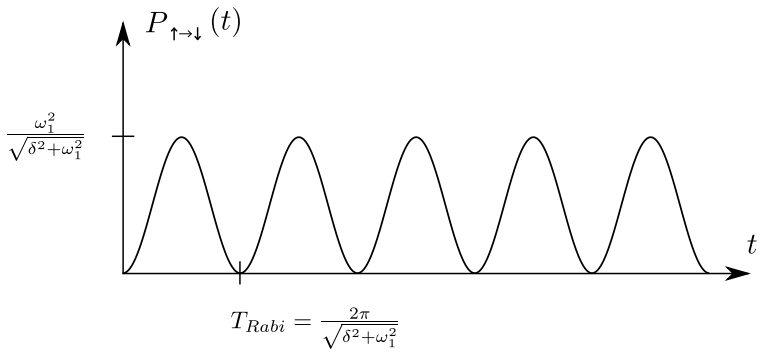


Figure 15.4 Transition probability as a function of time.

15.5 Implementation of Quantum Gates

At exact resonance, Rabi oscillations provide a direct way to implement single-qubit gates. We illustrate this with the NOT and Hadamard gates.

The NOT Gate

At exact resonance, $\delta = 0$, choosing $t = T_{\text{Rabi}}/2 = \pi/\omega_1$ gives $P_{\uparrow\to\downarrow} = 1$. Thus a resonant rotating field applied for this duration flips the spin with unit probability. In NMR terminology this is a π pulse.

To identify the corresponding unitary explicitly, it is convenient to work in the rotating frame.

$$\tilde{U} = \exp\Big(- i\frac{t}{2}(\delta\sigma_z - \omega_1\sigma_x)\Big). \tag{15.47}$$

For $\delta = 0$ and $t = \pi/\omega_1$, this becomes

$$\tilde{U} = \exp\Big(i\frac{\pi}{2}\sigma_x\Big) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{15.48}$$

This is a rotation by π about the x axis. It exchanges $|\uparrow\rangle$ and $|\downarrow\rangle$, and therefore implements a NOT gate up to an irrelevant global phase.

The Hadamard Gate

Now set $\delta = 0$ and apply the resonant rotating field for a quarter of a Rabi period, $t = T_{\text{Rabi}}/4 = \pi/(2\omega_1)$. The transition probabilities are then both $1/2$. In the rotating frame,

$$\tilde{U} = \exp\Big(- i\frac{t}{2}(\delta\sigma_z - \omega_1\sigma_x)\Big) \tag{15.49}$$

$$= \exp\Big(i\frac{\pi}{4}\sigma_x\Big) \tag{15.50}$$

$$= \cos\Big(\frac{\pi}{4}\Big)\mathbb{1} + i\sin\Big(\frac{\pi}{4}\Big)\sigma_x \tag{15.51}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{15.52}$$

This unitary maps $|\uparrow\rangle$ to $\frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle)$ and $|\downarrow\rangle$ to $\frac{1}{\sqrt{2}}(i|\uparrow\rangle + |\downarrow\rangle)$. Up to simple phase rotations, this is physically equivalent to a Hadamard operation, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

16 Heisenberg Hamiltonian and Two-Qubit Gates

In Chapter **15**, we studied the dynamics of a spin in a time-dependent magnetic field and showed how such control can be used to implement single-qubit gates, including the NOT and Hadamard gates (Section **15.5**). Universal quantum computation also requires an entangling two-qubit gate, such as CNOT. Any nontrivial two-qubit gate must rely on an interaction between the two physical qubits. We therefore begin by studying the interaction between two magnetic moments, and then show how several common forms of magnetic coupling can be used to implement useful two-qubit gates. Such interactions occur naturally in many physical systems and will be discussed further in Chapter **17**.

16.1 Heisenberg Hamiltonian

We have seen that the interaction energy of a magnetic moment $\vec{M}$ with an external magnetic field $\vec{B}$ is $-\vec{B}\cdot\vec{M}$ (Section **2.7**). Consider now two magnetic moments $\vec{M}_1$ and $\vec{M}_2$. They may be pictured as two small magnetic dipoles. Depending on their relative orientation, their mutual interaction can raise or lower the total energy, as illustrated in Figure **16.1**.

The curves represent magnetic field lines. If the interaction energy is required to be independent of the overall orientation of the system, so that no spatial direction is preferred, the simplest rotationally invariant bilinear interaction is proportional to

$$H \approx \vec{M}_1 \cdot \vec{M}_2 \tag{16.1}$$

At first order in $\vec{M}_1$ and $\vec{M}_2$, this scalar product is the unique bilinear form that is invariant under a simultaneous rotation of the two moments.

For intrinsic spin-$1/2$ magnetic moments, such as those associated with protons or suitable atomic nuclei, we may write $\vec{M}_1 = g_1\frac{\hbar}{2}\vec{\sigma_1}$ and $\vec{M}_2 = g_2\frac{\hbar}{2}\vec{\sigma_2}$, where $\vec{\sigma_1}$ and $\vec{\sigma_2}$ denote vectors of Pauli matrices and the constants g_1 and g_2 depend on the physical species. A rotationally invariant interaction between two spin-$1/2$ moments therefore has the form

$$H = \hbar J\vec{\sigma_1}\cdot\vec{\sigma_2} \tag{16.2}$$

where $\hbar J$ has units of energy and J has units of angular frequency.

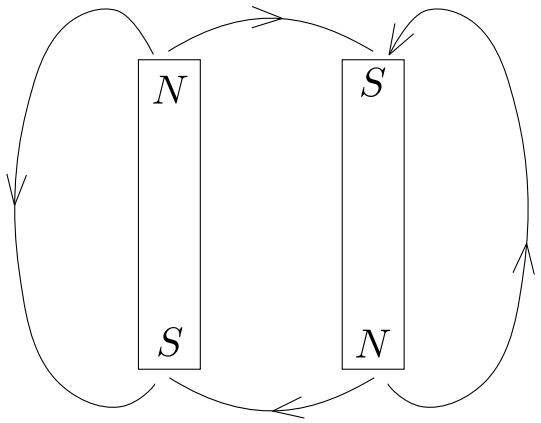


Figure 16.1 Magnetic field lines produced by two dipoles.

A few remarks are useful concerning the scalar product above. Since the Hamiltonian acts on two qubits, $\vec{\sigma_1}\cdot\vec{\sigma_2}$ is a 4×4 Hermitian matrix acting on the Hilbert space $\mathbb{C}^2\otimes\mathbb{C}^2$. Explicitly,

$$\vec{\sigma_1}\cdot\vec{\sigma_2} = \sigma_1^x\otimes\sigma_2^x + \sigma_1^y\otimes\sigma_2^y + \sigma_1^z\otimes\sigma_2^z. \tag{16.3}$$

Explicitly, in the computational basis,

$$\sigma_1^x\otimes\sigma_2^x = \begin{pmatrix}0&1\\1&0\end{pmatrix}\otimes\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix} \tag{16.4}$$

$$\sigma_1^y\otimes\sigma_2^y = \begin{pmatrix}0&-i\\i&0\end{pmatrix}\otimes\begin{pmatrix}0&-i\\i&0\end{pmatrix} = \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix} \tag{16.5}$$

$$\sigma_1^z\otimes\sigma_2^z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&-1\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix} \tag{16.6}$$

And therefore

$$H = \hbar J \vec{\sigma_1} \cdot \vec{\sigma_2} = \hbar J \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{16.7}$$

The eigenvalues and eigenvectors can be obtained directly from this matrix, but it is more instructive to use the algebra of the Pauli operators.

Introduce the raising and lowering operators

$$\sigma^+ = \frac{1}{2}(\sigma^x + i\sigma^y) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{16.8}$$

$$\sigma^- = \frac{1}{2}(\sigma^x - i\sigma^y) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{16.9}$$

One readily verifies that $\sigma^+|\uparrow\rangle = 0$, $\sigma^+|\downarrow\rangle = |\uparrow\rangle$, $\sigma^-|\downarrow\rangle = 0$, and $\sigma^-|\uparrow\rangle = |\downarrow\rangle$. Expressing σ^x and σ^y in terms of σ^+ and σ^- gives

$$H = \hbar J \left\{ \sigma_1^z \otimes \sigma_2^z + 2(\sigma_1^+ \otimes \sigma_2^- + \sigma_1^- \otimes \sigma_2^+) \right\} \tag{16.10}$$

The matrix elements $\langle s_1' s_2' | H | s_1 s_2 \rangle$, with each spin label equal to $\uparrow$ or $\downarrow$, reproduce the matrix written above. For example,

$$H|\uparrow\downarrow\rangle = 2\hbar J(\sigma_1^- \otimes \sigma_2^+)|\uparrow\downarrow\rangle \tag{16.11}$$

$$= 2\hbar J|\downarrow\uparrow\rangle \tag{16.12}$$

and therefore $\langle\downarrow\uparrow|H|\uparrow\downarrow\rangle = 2\hbar J$.

Consider now the action of H on the Bell state $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$.

$$\sigma_1^z \otimes \sigma_2^z(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{16.13}$$

$$\sigma_1^+ \otimes \sigma_2^-(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -|\uparrow\downarrow\rangle \tag{16.14}$$

$$\sigma_1^- \otimes \sigma_2^+(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = |\downarrow\uparrow\rangle. \tag{16.15}$$

These three relations imply

$$H(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -3\hbar J(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle). \tag{16.16}$$

Thus $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ is an eigenstate of H with energy $-3\hbar J$.

Consider next the three states $|\uparrow\uparrow\rangle$, $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$, and $|\downarrow\downarrow\rangle$. The exchange term $\sigma_1^+ \otimes \sigma_2^- + \sigma_1^- \otimes \sigma_2^+$ acts in such a way that the following eigenvalue equations are obtained:

$$H|\uparrow\uparrow\rangle = \hbar J|\uparrow\uparrow\rangle \tag{16.17}$$
$$H(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) = \hbar J(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{16.18}$$
$$H|\downarrow\downarrow\rangle = \hbar J|\downarrow\downarrow\rangle \tag{16.19}$$

These three states are therefore eigenstates of H with the common energy $+\hbar J$.

In summary, the antisymmetric state is the singlet, with energy $-3\hbar J$, whereas the three symmetric states form the triplet manifold, each with energy $+\hbar J$.

As an instructive extension, consider the effect of an external magnetic field $\vec{B}$ on the energy levels. The Hamiltonian becomes

$$H = -\frac{\hbar g_1}{2}\vec{B}\cdot\vec{\sigma_1} - \frac{\hbar g_2}{2}\vec{B}\cdot\vec{\sigma_2} + \hbar J\vec{\sigma_1}\cdot\vec{\sigma_2} \tag{16.20}$$

The term $\vec{B}\cdot\vec{\sigma_1}$ is understood as $(\vec{B}\cdot\vec{\sigma_1})\otimes\mathbb{1}_2$, and similarly $\vec{B}\cdot\vec{\sigma_2}$ means $\mathbb{1}_1\otimes(\vec{B}\cdot\vec{\sigma_2})$. We may choose the z axis along $\vec{B}$. Because the Heisenberg interaction $\hbar J\vec{\sigma_1}\cdot\vec{\sigma_2}$ is rotationally invariant, this choice does not affect its spectrum.

For two identical nuclei, $g_1 = g_2 = g$. Defining $gB = \omega_0$, where ω_0 is the Larmor angular frequency (Section **15.3**), the Hamiltonian becomes

$$H = -\frac{\hbar\omega_0}{2}(\sigma_1^z\otimes\mathbb{1}_2 + \mathbb{1}_1\otimes\sigma_2^z) + \hbar J\vec{\sigma_1}\cdot\vec{\sigma_2} \tag{16.21}$$

We have

$$H|\uparrow\uparrow\rangle = (-\hbar\omega_0 + \hbar J)|\uparrow\uparrow\rangle \tag{16.22}$$
$$H|\downarrow\downarrow\rangle = (+\hbar\omega_0 + \hbar J)|\downarrow\downarrow\rangle \tag{16.23}$$
$$H(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) = \hbar J(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{16.24}$$
$$H(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -3\hbar J(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{16.25}$$

The singlet energy is unchanged because the two z components are opposite. The $m = 0$ triplet state $|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle$ is likewise unaffected by the Zeeman term. By contrast, the energies of $|\uparrow\uparrow\rangle$ and $|\downarrow\downarrow\rangle$ shift in opposite directions. The external field therefore lifts the degeneracy of the triplet manifold, a generic effect of a perturbation that breaks a symmetry. The resulting energy levels are shown in Figure **16.2**.

Above a critical field B_c, the state $|\uparrow\uparrow\rangle$ becomes the lowest-energy state of the system.

16.2 SWAP Gate and Heisenberg Hamiltonian

The SWAP gate is defined on computational-basis states by

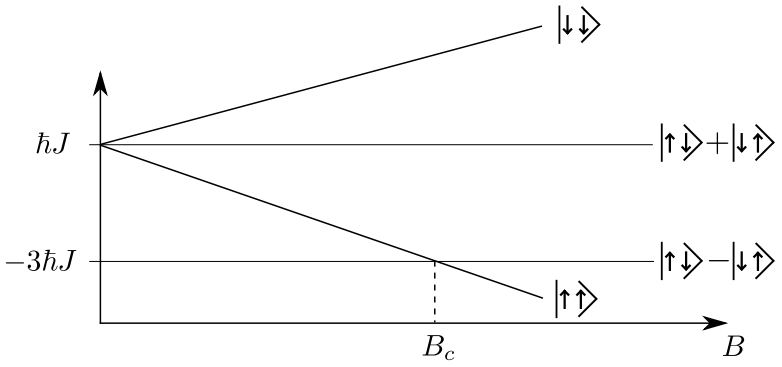


Figure 16.2 Energies of the singlet and triplet states as a function of the external magnetic-field strength.

$$\text{SWAP}\,|x, y\rangle = |y, x\rangle \tag{16.26}$$

By linearity, this definition extends to the entire two-qubit Hilbert space. The gate exchanges the states carried by two qubits and can be implemented using three CNOT gates, as shown in Figure **16.3**.

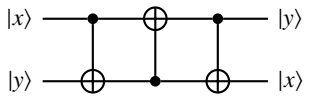


Figure 16.3 Circuit for the realization of the SWAP.

Conversely, a CNOT gate can be synthesized from $\sqrt{\text{SWAP}}$ together with single-qubit gates. Thus $\sqrt{\text{SWAP}}$ provides an entangling primitive that is universal when combined with arbitrary single-qubit operations.

We now show that the isotropic Heisenberg Hamiltonian directly generates both SWAP and $\sqrt{\text{SWAP}}$.

The time-evolution operator generated by the Heisenberg Hamiltonian is

$$U_{Heis}(t) = \exp\Big(-\frac{it}{\hbar}H_{Heis}\Big). \tag{16.27}$$

It is convenient to work in the eigenbasis introduced above. The spectral decomposition of the Hamiltonian is

$$H = -3\hbar J\left\{\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| - \langle\downarrow\uparrow|}{\sqrt{2}}\right\} \tag{16.28}$$

$$+ \hbar J\left\{|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| + \langle\downarrow\uparrow|}{\sqrt{2}} + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|\right\} \tag{16.29}$$

Exponentiating the corresponding eigenvalues gives

$$U_{Heis}(t) = e^{i3Jt}\left\{\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| - \langle\downarrow\uparrow|}{\sqrt{2}}\right\} \tag{16.30}$$

$$+ e^{-itJ}\left\{|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| + \langle\downarrow\uparrow|}{\sqrt{2}} + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|\right\} \tag{16.31}$$

As an exercise, one may write this operator explicitly as a matrix in the computational basis $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$.

Now choose $t = \frac{\pi}{4J}$. Formally, this corresponds to allowing the Heisenberg interaction to act for precisely this duration. In an experiment one cannot usually switch microscopic magnetic couplings on and off at will. As discussed in Chapter **17**, refocusing techniques (Section **17.4**) can be used to engineer the required effective interaction time.

For $t = \frac{\pi}{4J}$, we have $e^{i3Jt} = e^{i3\pi/4} = -e^{-i\pi/4}$ and $e^{-iJt} = e^{-i\pi/4}$. Hence

$$U_{Heis}(\frac{\pi}{4J}) = e^{-i\frac{\pi}{4}}\left\{-\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| - \langle\downarrow\uparrow|}{\sqrt{2}}\right. \tag{16.32}$$

$$\left. + |\uparrow\uparrow\rangle\langle\uparrow\uparrow| + \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| + \langle\downarrow\uparrow|}{\sqrt{2}} + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|\right\} \tag{16.33}$$

From this expression one immediately obtains

$$U_{Heis}(\frac{\pi}{4J})|\uparrow\uparrow\rangle = e^{-i\frac{\pi}{4}}|\uparrow\uparrow\rangle \tag{16.34}$$

$$U_{Heis}(\frac{\pi}{4J})|\downarrow\downarrow\rangle = e^{-i\frac{\pi}{4}}|\downarrow\downarrow\rangle \tag{16.35}$$

$$U_{Heis}(\frac{\pi}{4J})(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) = e^{-i\frac{\pi}{4}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{16.36}$$

$$U_{Heis}(\frac{\pi}{4J})(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -e^{-i\frac{\pi}{4}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{16.37}$$

$$= e^{-i\frac{\pi}{4}}(|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle) \tag{16.38}$$

Up to the global phase $e^{-i\pi/4}$, the evolution therefore exchanges the two qubits. The triplet subspace is invariant under this exchange, whereas the singlet acquires a minus sign. Adding and subtracting the last two relations gives

$$U_{Heis}(\frac{\pi}{4J})|\uparrow\downarrow\rangle = e^{-i\frac{\pi}{4}}|\downarrow\uparrow\rangle \tag{16.39}$$

$$U_{Heis}(\frac{\pi}{4J})|\downarrow\uparrow\rangle = e^{-i\frac{\pi}{4}}|\uparrow\downarrow\rangle \tag{16.40}$$

which is precisely the action of SWAP, up to the same global phase.

To obtain $\sqrt{\text{SWAP}}$, it is sufficient to let the interaction act for half as long, namely $t = \frac{\pi}{8J}$.

16.3 CNOT Gate and Anisotropic Magnetic Interaction

In an anisotropic environment, the spin–spin interaction need not have the same strength along all spatial directions. An important limiting case, which provides a good approximation in several NMR settings (Chapter **17**), is a coupling dominated by the z direction. This situation can arise, for example, in the presence of a strong static field $\vec{B_0} = (0, 0, B_0)$. The interaction is then well approximated by the Ising Hamiltonian

$$H = \hbar J \sigma_1^z \otimes \sigma_2^z. \tag{16.41}$$

This Hamiltonian is diagonal in the computational basis:

$$H = \hbar J \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \hbar J \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{16.42}$$

$$= \hbar J \Big\{ |\uparrow\uparrow\rangle\langle\uparrow\uparrow| - |\uparrow\downarrow\rangle\langle\uparrow\downarrow| - |\downarrow\uparrow\rangle\langle\downarrow\uparrow| + |\downarrow\downarrow\rangle\langle\downarrow\downarrow| \Big\} \tag{16.43}$$

The corresponding time-evolution operator is therefore

$$e^{-i\frac{t}{\hbar}H} = e^{-itJ}|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + e^{itJ}|\uparrow\downarrow\rangle\langle\uparrow\downarrow| + e^{itJ}|\downarrow\uparrow\rangle\langle\downarrow\uparrow| + e^{-itJ}|\downarrow\downarrow\rangle\langle\downarrow\downarrow| \tag{16.44}$$

$$= \begin{pmatrix} e^{-itJ} & 0 & 0 & 0 \\ 0 & e^{itJ} & 0 & 0 \\ 0 & 0 & e^{itJ} & 0 \\ 0 & 0 & 0 & e^{-itJ} \end{pmatrix} \tag{16.45}$$

One may verify the following identity:

$$CNOT = (\mathbb{1}_1 \otimes H_2)(R_1 \otimes R_2) e^{-\frac{i}{\hbar}\frac{\pi}{4J}H} (\mathbb{1}_1 \otimes H_2) \tag{16.46}$$

where $R_1 = \exp\left(-i\frac{\pi}{4}\sigma_1^z\right)$ and $R_2 = \exp\left(-i\frac{\pi}{4}\sigma_2^z\right) = \begin{pmatrix} e^{-i\frac{\pi}{4}} & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$.

Thus CNOT can be implemented by allowing the anisotropic interaction to act for a time $\frac{\pi}{4J}$ and combining this evolution with suitable single-qubit gates. In practice, refocusing techniques (Section **17.4**) are used to control the effective duration of the coupling.

The circuit corresponding to (16.46) is shown below:

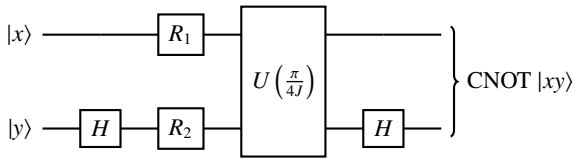


Figure 16.4 Implementation of the CNOT gate using an anisotropic spin–spin interaction and single-qubit rotations.

17 Experimental implementations

In this chapter we present the basic principles underlying experimental implementations of quantum algorithms. The principles will be illustrated in the framework of nuclear magnetic resonance (NMR), which, as we shall see, has made it possible to implement several algorithms, including Shor's algorithm, in the laboratory. Although it is probably not possible to go much beyond about ten qubits with NMR, this technology has the advantage of illustrating in a concrete and simple way universal principles that also apply to other, more promising technologies. Indeed, whatever the underlying technology used to fabricate and manipulate effective qubits, the Hamiltonians governing their dynamics can only be "polynomials" built from Pauli matrices, containing linear and quadratic terms at lowest order.

17.1 The physical systems involved

In the NMR setting, the qubits are the magnetic moments of spin-$1/2$ atomic nuclei in suitable molecules. These molecules may be natural or synthetic and form a macroscopic fluid or solid. Figure **17.1** shows two naturally occurring molecules—chloroform and trichloroethylene—that have already been used for quantum computation. As we shall see, each molecule can in some sense be regarded as a quantum circuit. In these molecules, the relevant qubits are the spin-$1/2$ nuclei of hydrogen ^1H, carbon ^{13}C, and fluorine ^{19}F. The hydrogen nucleus is a proton with spin $1/2$. The ^{13}C nucleus contains 6 protons and 7 neutrons[1]. In the nuclear ground state, the proton and neutron spins compensate one another so that the total spin is $1/2$. The situation is similar for the fluorine isotope ^{19}F, which contains 9 protons and 10 neutrons.

The fluid (or solid), at room temperature, is placed in a region with a static magnetic field $\vec{B}_0 = (0, 0, B_0)$ directed along z, with magnitude $B_0 \approx 1 - 10$T. This is a very strong field: 1T $= 10^5$ Gauss, whereas one Gauss is roughly the order of magnitude of the Earth's magnetic field. The Larmor frequencies of the nuclear magnetic moments ^1H, ^{13}C, and ^{19}F are typically $\omega_L \approx 10 - 100$MHz (1MHz $= 10^6$Hz).

Single-qubit gates are implemented using radio-frequency pulses $\vec{B}_1 e^{i\omega t}$ with an intensity corresponding to $\omega_1 \approx 0.1 - 1$MHz. These pulses are generated by one or more

[1] It is an isotope of ^{12}C, which contains 6 protons and 6 neutrons and has total spin zero. The ^{14}C isotope, well known for radiocarbon dating, contains 6 protons and 8 neutrons and also has total spin zero. Carbon atoms are electrically neutral and all contain 6 electrons; their chemical properties are governed by the electron cloud and are therefore essentially identical for the different isotopes.

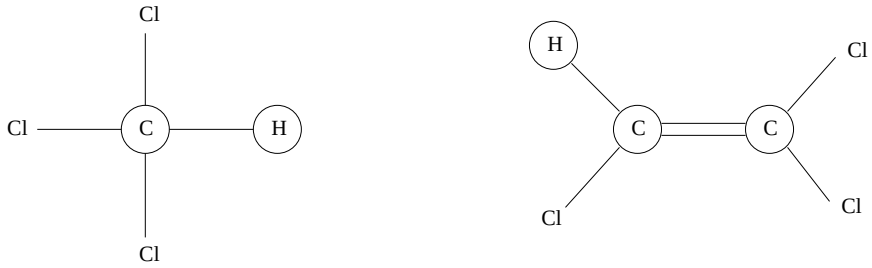


Figure 17.1 Chloroform (left) and trichloroethylene (right) molecules. The hydrogen ^1H, carbon ^{13}C, and fluorine ^{19}F atoms whose spin-1/2 nuclei serve as qubits are circled. The chlorine nuclei have zero spin and are not qubits.

coils carrying an alternating current at radio frequency ω. A given nuclear-spin species can be selectively addressed ^1H, ^{13}C, or ^{19}F by tuning ω to the Larmor frequency of that qubit (the resonant case). The influence on other qubits with a different, non-resonant Larmor frequency can then be neglected. We shall see that the chemical environment of a qubit in the molecule produces a correction to its Larmor frequency. This is important both because the resonance frequencies must be tuned sufficiently accurately and because these shifts make it possible to selectively address and distinguish qubits associated with identical nuclei. The scale ω_1 sets the gate duration, $\tau_1 \approx \frac{2\pi}{\omega_1} \approx 10^{-6}$ s.

Two-qubit gates are provided by nature itself. As we shall see, the Heisenberg-type spin–spin interaction can be exploited to implement two-qubit gates. Their duration is determined by the strength of the spin–spin coupling and is approximately 10^{-3} s. It is therefore about a thousand times longer than the duration of a single-qubit gate. To first approximation, the duration of the latter may be neglected.

At this point it is useful to develop an intuition for the various energy scales involved. The "molecular quantum circuit" is controlled using radio-frequency pulses. The energy involved in these radio-frequency pulses is $\hbar\omega_1 \approx 10^{-6}$ eV. This is at least a thousand times smaller than all the other relevant energy scales, so these pulses do not disturb the molecular structure. Indeed, the excitation energies of the electron cloud are of order eV[2]; the Zeeman splitting energy of electron spins is of order 10^{-3} eV[3].

NMR quantum computation operates simultaneously on a macroscopic number of molecules, and the final collective measurement directly produces a statistical result. In order to manipulate the magnetic moments of the active nuclei in the molecule, their Larmor frequencies must be characterized and separated with sufficient precision. This is only possible for relatively small molecules containing at most about ten qubits. Even if it were possible to synthesize molecules with hundreds or thousands of nuclei representing active qubits, the Larmor frequencies would form a quasi-continuum and it would become difficult to manipulate them and/or maintain the coherence of the quantum states. In that regime, both thermal excitation energies and the frequency width of the radio-frequency pulses are larger than the differences between neighboring Lar-

[2] 1 eV = $1.6\,10^{-19}$ Joule, J = kg m^2/s^2, and $\hbar = 6.58211928(15).10^{-16}$ eV.

[3] The internal excitation energy of nuclei is $\sim 10^6$ eV, while for nucleons it is $\sim 10^9$ eV, the scale of quantum chromodynamics.

mor frequencies. This is one reason why NMR has not been used to build a quantum computer operating with substantially more than about ten qubits. Another important limitation is that the spins in the initial state are not sufficiently polarized and their state is far from a pure state. Instead, the system is in thermal equilibrium. One of the innovations of NMR experiments was to transform the thermal state into a "pseudo-pure" state. This point lies beyond the scope of this course and will not be discussed here[4].

17.2 Rabi oscillations and single-qubit gates

This section summarizes the essential theory of Rabi oscillations, which underlies the implementation of single-qubit gates such as Hadamard gates, rotations about the x, y, or z axes, and $\pi/2^k$ phase shifts.

The Hamiltonian of a magnetic moment in a field $\vec{B}_0 = (0, 0, B_0)$ is

$$H = -\frac{g\hbar}{2m}\vec{B}_0 \cdot \vec{\sigma} = -\frac{\hbar\omega_L}{2}\sigma_z.$$

For the hydrogen nucleus ${}^1H$, $g \approx 5.59$, $m = 10^{-27}$ kg and $q = 1.6\,10^{-19}$ C, which gives a Larmor frequency $\omega_L \approx 100$ MHz. The time evolution of a state is given by[5]

$$|\psi\rangle = e^{i\frac{\varphi+\omega_L t}{2}} \cos\frac{\theta}{2}|\uparrow\rangle + e^{-i\frac{\varphi+\omega_L t}{2}} \sin\frac{\theta}{2}|\downarrow\rangle.$$

This dynamics can be visualized by representing the state as a vector on the Bloch sphere. The vector makes a constant angle θ with the z axis and precesses around z at frequency ω_L.

In an NMR experiment, the field $B_0 \approx 1 - 10$ Tesla is fixed once and for all, and all magnetic moments precess around z at their respective Larmor frequencies.

To manipulate the magnetic moments, one uses a radio-frequency field of frequency ω and amplitude $B_1 \approx 10^{-2}$ Tesla. For this field to significantly affect a given magnetic moment, its frequency must be tuned close to the resonance frequency $\omega \approx \omega_L$. In that case, the spin can absorb or emit a quantum of energy $\hbar\omega$ exactly matching the energy difference between the magnetic-moment levels in the field $\vec{B}_0$. A rotation of the spin about the x and/or y axes is produced by switching on the radio-frequency field $\vec{B}_1(t) = (B_1 \cos\omega t, B_1 \sin\omega t, 0)$. The Hamiltonian is

$$H = -\frac{\hbar\omega_L}{2}\sigma_z - \frac{\hbar\omega_1}{2}(\sigma_x \cos\omega t + \sigma_y \sin\omega t).$$

The evolution operator then gives (for $\omega = \omega_L$)

$$\text{prob}(|\uparrow\rangle \to |\downarrow\rangle) = |\langle\downarrow|U(t)|\uparrow\rangle|^2 = \sin^2\frac{\omega_1 t}{2}.$$

[4] For information, a pseudo-pure state is a density matrix of the form $\rho = \alpha\mathbb{1} + \delta|\Psi\rangle\langle\Psi|$. The expectation value of any traceless observable A satisfies $\text{Tr}\rho A = \delta\langle\Psi|A|\Psi\rangle$. When a thermal state is transformed into a pseudo-pure state, δ decreases with the number of qubits and the resulting measurement signal eventually becomes too weak.

[5] The initial state is obtained by setting $t = 0$.

Thus the transition probability oscillates between 0 and 1 with period $\frac{2\pi}{\omega_1} \approx 10^{-6}$ s. These are the so-called Rabi oscillations.

NOT gate. If we set $t = \frac{\pi}{\omega_1}$ (half a Rabi period), we obtain

$$U(\frac{\pi}{\omega_1}) = \sigma_x = \text{NOT}.$$

Thus, to implement a NOT gate it is sufficient to switch on the radio-frequency field for a duration $\frac{\pi}{\omega_1}$. This operation is also called a π pulse and flips the spin, $|\uparrow\rangle \to |\downarrow\rangle$ and $|\downarrow\rangle \to |\uparrow\rangle$.

Hadamard gate. For $t = \frac{\pi}{2\omega_1}$ (one quarter of a Rabi period), one obtains

$$U(\frac{\pi}{2\omega_1}) = H.$$

To implement an H gate it is therefore sufficient to switch on the radio-frequency field for a duration $\frac{\pi}{2\omega_1}$. This operation is also called a $\pi/2$ pulse and tips a spin initially aligned with z into the xy plane: $|\uparrow\rangle \to \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle)$ and $|\downarrow\rangle \to \frac{1}{\sqrt{2}}(|\downarrow\rangle - |\uparrow\rangle)$.

Other gates. In principle one can proceed similarly to implement other single-qubit operations, for example rotations about z. In practice, however, because of the coil geometry, radio-frequency pulses cannot be generated along z. A rotation of a qubit about z is instead implemented by introducing an appropriate phase shift in subsequent signals applied to that qubit, which is equivalent to rotating the reference frame about z. This phase shift depends on the Larmor frequency of the qubit in question.

Finally, it is important to note that radio-frequency pulses selectively act on qubits associated with the nuclei ^1H, ^{13}C, and ^{19}F because their Larmor frequencies are well separated. We shall see that selective addressing is also possible for identical nuclei because their chemical environment within the molecule slightly shifts their Larmor frequencies.

17.3 Spin–spin coupling and two-qubit gates

Two-qubit gates exploit the natural interaction between magnetic moments. The time evolution associated with this interaction is a unitary operator that cannot be reduced to a tensor product of two single-qubit unitaries. In other words, this interaction creates entanglement and makes it possible, in particular, to implement the $CNOT$ gate. Note immediately that this does not come without difficulties, because this interaction cannot simply be switched on and off at will: it is a *natural* interaction. This problem can be overcome using the technique of *refocusing* (Section **17.4**).

For two nuclear magnetic moments in a molecule connected by an axis $\vec{n}$, the magnetic dipole interaction has the form

$$\hbar J_{\text{dip}}(3(\vec{\sigma}_1 \cdot \vec{n})(\vec{\sigma}_2 \cdot \vec{n}) - \vec{\sigma}_1 \cdot \vec{\sigma}_2).$$

The coupling constant decreases as the inverse cube of the distance between the magnetic moments. Note that two different algebraic structures appear in this expression: the scalar product in Euclidean space and the tensor product between Pauli matrices in the Hilbert space of the spins. The first term does not play a role in a fluid because thermal molecular rotations average over the vector $\vec{n}$. Indeed, $\langle n_i \rangle = 0$ and $\langle n_i^2 \rangle = \frac{1}{3}$ $(i = x, y, z)$ imply

$$\langle (\vec{\sigma}_1 \cdot \vec{n})(\vec{\sigma}_2 \cdot \vec{n}) \rangle = \frac{1}{3} \langle \vec{\sigma}_1 \cdot \vec{\sigma}_2 \rangle$$

and therefore the magnetic dipole interaction averages to zero in a fluid at thermal equilibrium. The magnetic moments also interact with the surrounding electron cloud, which induces an effective interaction between nuclear spins through the chemical bonds. The analysis[6] of these effects is nontrivial and leads to a Heisenberg-type (anisotropic) Hamiltonian

$$\sum_{i,j=x,y,z} \hbar J_{ij} \sigma_{1i} \otimes \sigma_{2j}.$$

In fact $J_{ij} \ll \hbar\omega_L$, so this Hamiltonian can be regarded as a small perturbation of the original Hamiltonian governing Larmor precession, which is diagonal in the computational basis. A lowest-order perturbative calculation then shows that it is sufficient to retain only the z component of this interaction.

Altogether, the spin coupling will therefore be modeled by (setting $J_{zz} = J$)

$$\mathcal{H}_{int} = \hbar J \sigma_{1z} \otimes \sigma_{2z}.$$

The unitary evolution associated with this interaction is

$$U_{int}(t) = \exp\left(-\frac{it}{\hbar}\mathcal{H}_{int}\right) = \exp(-itJ\sigma_{1z} \otimes \sigma_{2z}).$$

This is a 4×4 matrix diagonal in the computational basis. Its diagonal entries are $e^{-itJ}; e^{itJ}; e^{itJ}; e^{-itJ}$. Moreover $\hbar J \ll \hbar\omega_1$ $(\ll \hbar\omega_L)$. This separation of energy scales is extremely important because it means that *the interaction time scale is roughly a thousand times longer than the duration of a single-qubit gate*. Indeed, $\tau_{\text{int}} \approx \frac{2\pi}{J} \approx 10^{-2} - 10^{-3}$ s, whereas $\tau_{\text{pulse}} \approx \frac{2\pi}{\omega_1} \approx 10^{-6}$ s. Thus the elementary time step in NMR quantum computation is of order one millisecond. This time scale is not especially short compared with the time scales of classical computers; the potential advantage of quantum computation instead comes from the potentially polynomial complexity of quantum algorithms, compared with potentially exponential complexity in the classical case.

The following identity, together with its corresponding circuit (Figure **17.3**), underlies the implementation of the *CNOT* gate:

$$CNOT = (\mathbb{1} \otimes H)(R_1 \otimes R_2) U_{int}(t = \frac{\pi}{4J_z})(\mathbb{1} \otimes H)$$

where

$$R_1 = \exp\left(i\frac{\pi}{2}\frac{\sigma_{1z}}{2}\right), \qquad R_2 = \exp\left(i\frac{\pi}{2}\frac{\sigma_{2z}}{2}\right).$$

[6] This involves the Fermi contact interaction between the electron cloud and the nucleus, the Pauli principle, and Hund's rule.

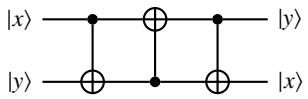


Figure 17.2 Circuit corresponding to the identity for the $CNOT$ gate. Here U_{int} is the unitary evolution due to spin–spin coupling. The single-qubit gates are implemented using radio-frequency pulses.

Consider the chloroform molecule, where the qubits are the magnetic moments of the ^1H and ^{13}C nuclei. Suppose that ^1H is qubit 1 and ^{13}C is qubit 2. The experimental protocol for implementing the $CNOT$ gate is as follows:

- At the initial time, apply a $\frac{\pi}{2}$ pulse of frequency $\omega = \omega_L^C$ in the xy plane. This implements the Hadamard gate on the second qubit. The corresponding Hamiltonian is
$$-\frac{\hbar\omega_1}{2}(\sigma_x \cos\omega_L^C t + \sigma_y \sin\omega_L^C t).$$
- Then apply two $\frac{\pi}{2}$ pulses of frequencies $\omega = \omega_L^H$ and $\omega = \omega_L^C$ along the z direction. These implement the two rotations R_1 and R_2 by an angle $\pi/2$ about z. The corresponding Hamiltonian is
$$-\frac{\hbar\omega_1}{2}\sigma_z(\cos\omega_L^H t + \cos\omega_L^C t).$$
- Wait for a time $\tau = \frac{\pi}{4J}$. During this interval, the two qubits evolve according to their natural interaction Hamiltonian
$$\hbar J\sigma_{1z} \otimes \sigma_{2z}.$$
- At the final time, apply a $\frac{\pi}{2}$ pulse in the xy plane at frequency $\omega = \omega_L^C$. This implements the last Hadamard gate on the second qubit. The corresponding Hamiltonian is the same as above.

Of course, the natural interaction $\hbar J\sigma_{1z}\otimes\sigma_{2z}$ also acts during the individual-qubit operations (the $\pi/2$ pulses). Therefore this experimental protocol implements the $CNOT$ gate only approximately. The important point, however, is that the approximation is excellent because the duration of the $\pi/2$ pulses is negligible—and the pulses can therefore be regarded as instantaneous—compared with $\tau_{\text{int}} = \frac{\pi}{4J}$. Finally, throughout all these operations, the spins continue their Larmor precession about the direction of $\vec{B}_0$.

17.4 Refocusing

To fix ideas, consider the state obtained after carrying out the protocol of the previous section for the $CNOT$ gate. A priori, this state continues to evolve under the natural interaction between the magnetic moments. How can we preserve it for an appreciable time, say of order a millisecond? Another relevant situation is one in which we want to

perform operations on certain qubits while keeping other qubits in a prescribed state for a time of order a millisecond. At first sight this may seem difficult, since the natural interactions cannot be switched on and off at will. The technique of *refocusing* overcomes this problem. It plays a central role in experimental implementations of algorithms: as we shall illustrate in the final section, most of the operations actually performed are related to refocusing.

Let $t_{\text{in}} < t_{\text{fin}}$ be initial and final times such that $t_{\text{fin}} - t_{\text{in}}$ is of order a few milliseconds. Let $|\psi_{\text{in}}\rangle$ be the initial state of a two-qubit system that we wish to preserve. Its natural evolution would lead to

$$|\psi_{\text{fin}}\rangle = \exp(-i(t_{\text{fin}} - t_{\text{in}})J\sigma_{1z} \otimes \sigma_{2z})|\psi_{\text{in}}\rangle.$$

Now suppose that at times $\frac{t_{\text{fin}}+t_{\text{in}}}{2}$ and t_{fin} we apply a π pulse corresponding to the rotation

$$R_{1x} = \exp\left(i\pi\frac{\sigma_{1x}}{2}\right) \otimes \mathbb{1}_2$$

by an angle π about the x axis, acting on the first qubit (for example ${}^1H$). Since these pulses have negligible duration compared with the total evolution time, the new final state—call it $|\psi_{\text{refoc}}\rangle$—is approximately

$$|\psi_{\text{refoc}}\rangle \approx R_{1x}\exp(-\frac{i(t_{\text{fin}} - t_{\text{in}})}{2}J\sigma_{1z} \otimes \sigma_{2z})R_{1x}\exp(-\frac{i(t_{\text{fin}} - t_{\text{in}})}{2}J\sigma_{1z} \otimes \sigma_{2z})|\psi_{\text{in}}\rangle.$$

It is straightforward to verify the exact mathematical identity

$$\mathbb{1}_1 \otimes \mathbb{1}_2 = R_{1x}\exp(-i\frac{t}{2}J\sigma_{1z} \otimes \sigma_{2z})R_{1x}\exp(-i\frac{t}{2}J\sigma_{1z} \otimes \sigma_{2z}),$$

valid for all t and J. Hence

$$|\psi_{\text{refoc}}\rangle \approx |\psi_{\text{in}}\rangle,$$

so the state obtained after the refocusing operation is a very good approximation to the desired initial state.

The general principle described above can be applied to more complicated situations. In short, the basic idea is to "correct" the natural dynamics by applying short pulses to individual qubits.

17.5 Chemical shifts and coupling effects

There is an important effect that we have not yet taken into account: the chemical shift. Within a molecule, the bare Larmor frequency of a nucleus is modified by its chemical environment. Indeed, the local magnetic field experienced by a nucleus is equal to B_0 plus diamagnetic and paramagnetic corrections produced by the electron cloud. This is important because identical nuclei can then have slightly different Larmor frequencies, making it possible to address them individually with radio-frequency pulses. This shift of the Larmor frequencies is called the *chemical shift*.

There is yet another important effect on the Larmor frequencies that must be taken into account, originating from spin–spin coupling. It causes each Larmor frequency to

"split" into several satellite frequencies. To fix ideas, consider again the chloroform molecule. Suppose that the state of the ^{13}C nucleus is $|\phi\rangle$. In this case the effective Hamiltonian of ^{1}H is

$$\mathcal{H}_{\text{eff}} = -\frac{\hbar\omega_L^H}{2}\sigma_z^H + \hbar J_{HC}\sigma_z^H\langle\phi|\sigma_z^C|\phi\rangle.$$

Depending on whether $|\phi\rangle = |\uparrow\rangle$ or $|\downarrow\rangle$, we obtain

$$\mathcal{H}_{\text{eff}} = -\frac{\hbar(\omega_L^H \pm 2J_{HC})}{2}\sigma_z^H$$

and therefore two effective Larmor frequencies for ^{1}H. The precession frequency is $\omega_L^H - 2J_{HC}$ when ^{13}C is in the state $|\uparrow\rangle$, and $\omega_L^H + 2J_{HC}$ when ^{13}C is in the state $|\downarrow\rangle$. Similarly, the ^{13}C nucleus has two Larmor frequencies $\omega_L^C - 2J_{HC}$ and $\omega_L^C + 2J_{HC}$ depending on whether ^{1}H is in the state $|\uparrow\rangle$ or $|\downarrow\rangle$.

Now consider the trichloroethylene molecule (Figure **17.1**). The two ^{13}C atoms do not have identical chemical environments, so the chemical shifts of their Larmor frequencies are different. This is useful because it allows us to distinguish the two qubits. In addition, each of these frequencies is split by spin–spin coupling. It is not difficult to see that for trichloroethylene there are *three groups of four frequencies*. Indeed, ω_L^H is split into four satellite frequencies corresponding to the four possible states of the two C^{13} nuclei, $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, and $|\downarrow\downarrow\rangle$. Likewise, ω_L^C is split into two groups (one for each carbon atom), each containing four frequencies corresponding to the four possible states of the neighboring nuclei. Figure **17.5** shows the spectrum of the two ^{13}C nuclei. The four ^{1}H frequencies are higher and do not appear on this scale.

The discussion is easily generalized. For a molecule with N spin-1/2 nuclei (or N qubits), there are in principle N Larmor frequencies (because of chemical shifts, this is true even if the nuclei are identical). Because of spin–spin coupling, there are in fact N groups of 2^{N-1} satellite frequencies[7]. These effects are extremely important in NMR spectroscopy. Molecular spectra provide a signature of molecular structure, which can often be inferred from the different groups of frequencies. The number, position, and intensity of the peaks provide valuable information about the molecule. For experimental implementations of quantum algorithms, this effect must be taken into account in order to tune pulse frequencies with sufficient accuracy. As noted above, it also allows one to distinguish qubits associated with identical nuclei. We shall see in Section **17.6** that it also allows us to read out computational-basis states.

17.6 Reading out the qubits

In NMR experiments, the molecular state is observed through a measurement performed on a statistical ensemble of qubits. The resulting signal is therefore directly an average value. Thus this is not quite a projective measurement of an individual quantum state,

[7] This is true if all chemical shifts are different. Otherwise some of these satellite frequencies coincide.

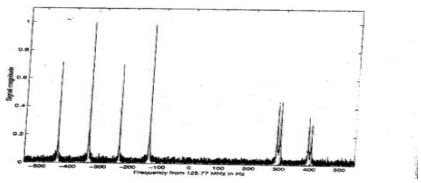


Figure 17.3 Spectrum of the two ^{13}C nuclei in the trichloroethylene molecule. The frequency origin is set at 125.77 MHz and the horizontal scale is in Hz. [Source: Nielsen and Chuang, Quantum Computation and Information, CUP].

but rather a collective measurement. Of course, the measured average is fully consistent with the measurement postulate.

Imagine an NMR experiment in which a molecular solution is acted upon by a sequence of pulses generated by a coil carrying an alternating current. The same coil can then be used for measurement. The final state of the qubits $|\Psi_{\text{fin}}\rangle$ has a total magnetic moment (in this section we omit proportionality factors and constants)

$$\vec{M}_{\text{fin}} \sim \langle \Psi_{\text{fin}} | \sum_{i=1}^{N} \vec{\sigma}_i \, | \Psi_{\text{fin}} \rangle .$$

This macroscopic magnetization precesses in the field $\vec{B}_0$ (around z), thereby inducing, according to Faraday's law, a voltage and current in the coil (we assume here that the coil is oriented along x and has resistance R):

$$i(t) = RV(t) \sim -\frac{d}{dt} M_x(t).$$

This signal is a linear combination of sinusoidal signals whose frequencies are the different Larmor frequencies involved in the precession of the magnetization. Fourier analysis gives a spectrum of Larmor frequencies, corrected by chemical shifts. Note that in the time domain the signal decays exponentially on a scale $O(T)$ because of relaxation of the magnetization toward its equilibrium value (decoherence). In the frequency domain this produces a broadening $O(\frac{1}{T})$ of the spectral lines. If this broadening is too large—equivalently, if the exponential decay is too fast—the measurement loses precision.

For a single frequency,

$$i(t) \sim e^{-t/T} \cos \omega_L t.$$

The corresponding spectral line is a Lorentzian function,

$$\hat{i}(\omega) \sim \frac{T}{1 + (\omega - \omega_L)^2 T^2}.$$

Let us apply these principles to reading computational-basis states. We shall neglect relaxation effects, whose description goes beyond the elementary formalism used here. Begin with the simplest case of an N-qubit state in which all qubits have the same Larmor frequency and the state is

$$|\uparrow\uparrow \cdots \uparrow\rangle.$$

A $\pi/2$ pulse tips this state into the xy plane,

$$|\Psi_{\text{fin}}\rangle = (|\uparrow\rangle + e^{-it\omega_L}|\downarrow\rangle) \otimes \cdots (|\uparrow\rangle + e^{-it\omega_L}|\downarrow\rangle)$$

(up to a global phase). This state has a macroscopic magnetization $(M_x(t), M_y(t), 0)$ precessing about z. A simple calculation gives

$$M_x(t) \sim N \sin \omega_L t,$$

which implies a sinusoidal current through the coil,

$$i(t) \sim N\omega \cos \omega_L t, \qquad \text{and} \qquad \hat{i}(\omega) \sim N\delta(\omega - \omega_L), \omega > 0.$$

Starting instead from the initial state $|\downarrow\downarrow \cdots \downarrow\rangle$, the $\pi/2$ pulse gives $|\Psi_{\text{fin}}\rangle = (|\uparrow\rangle - e^{-it\omega_L}|\downarrow\rangle) \otimes \cdots (|\uparrow\rangle - e^{-it\omega_L}|\downarrow\rangle)$, and hence

$$M_x(t) \sim -N \sin \omega_L t$$

and

$$i(t) \sim -N\omega \cos \omega_L t, \qquad \text{and} \qquad \hat{i}(\omega) \sim -N\delta(\omega - \omega_L), \omega > 0.$$

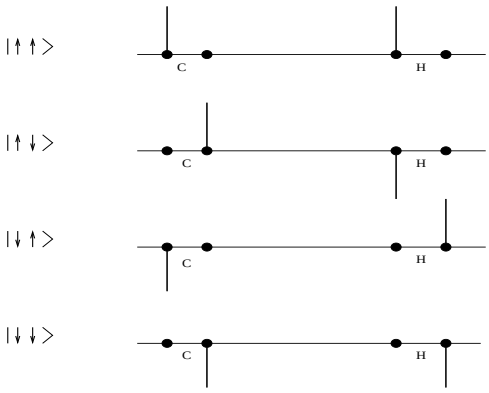


Figure 17.4 Schematic representation of the NMR spectra corresponding to the computational-basis states of chloroform (horizontal axis = Larmor frequencies).

These simple calculations lead to an important observation.

- A qubit in the state $|\uparrow\rangle$ produces *positive* peaks[8].
- A qubit in the state $|\downarrow\rangle$ produces *negative* peaks.
- A qubit in a superposition state $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ produces a spectrum with both *positive and negative* peaks.

Figure **17.6** gives a schematic representation of the peaks associated with computational-basis states for the chloroform molecule.

17.7 Experimental implementation of Shor's algorithm

We now outline a remarkable experiment by Vandersypen, Steffen, Breyta, Yannoni, Sherwood, and Chuang, *"Experimental realization of quantum factoring using nuclear magnetic resonance"*, Nature vol. 414, pp. 883–887 (2001). In this experiment the number 15 was factored experimentally following the principles of Shor's algorithm. More precisely, the aim is to determine the period of the function $f(x) = a^x \bmod 15$ for an integer a coprime with 15. The authors carried out the experiment for both $a = 11$ and $a = 7$. Here we illustrate the experiment for $a = 7$. Although mathematically this is of course a very small factoring problem, the experiment is important because it demonstrates that the principles of quantum computation can be implemented in the laboratory. It is also an impressive experimental achievement.

We first summarize the theory of Shor's algorithm in the concrete case of interest here.

The function $f(x) = 7^x \bmod 15$ is shown in the figure for integers $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, \dots\}$. Its period is $r = 4$. In other words, the order of 7 modulo 15 is 4, which is even. The factorization is therefore obtained by calculating $\gcd(7^{4/2} \pm 1, 15) = 3$ and 5.

To observe the periodicity of this function it is sufficient to work with the integers $\{0, \dots, 7\}$. Three qubits are needed to represent the corresponding kets $|x\rangle$, so we take $M = 2^3 = 8$. We also need to store the values $7^x \bmod 15$, which requires at most four qubits. Thus seven qubits in total are sufficient. Note also that if $x = x_0 + 2x_1 + 4x_2 + 8x_3$,

$$a^x = a^{x_0} a^{2x_1} a^{4x_2} a^{8x_3}$$

and therefore for $a = 7$ (since $7^4 = 1$),

$$7^x = 7^{x_0} 7^{2x_1}.$$

The modular exponentiation is therefore controlled only by the bits x_0 and x_1. Shor's circuit is shown in Figure 17.5. The figure also illustrates the two controlled multiplications by 7^{x_0} and 7^{x_1}. These require only *CNOT* gates; we leave it to the reader to verify that the circuits have the desired action.

We distinguish four stages in the unitary evolution of the quantum circuit. This is convenient for discussing the experiment. In stage (0), the algorithm is initialized in the

[8] In practice several peaks are observed because of coupling to the other qubits.

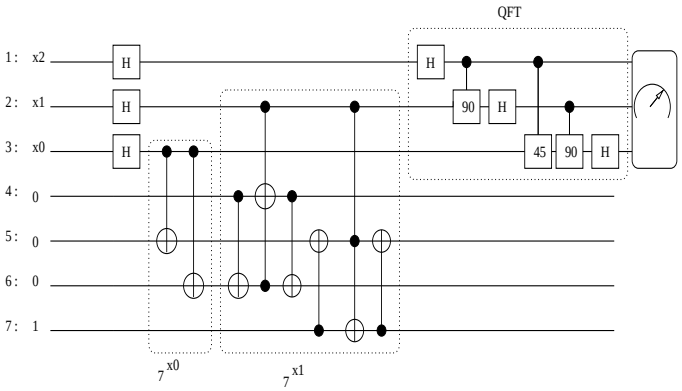


Figure 17.5 Circuit for Shor's algorithm with $N = 15$ and $a = 7$. Qubits numbered 1 to 7 correspond to the nuclear spins in the molecule shown in Figure **17.6**. The bits $x_2x_1x_0$ represent the integers $x \in \{0, 1, \cdots, 7\}$. The input state is $|000\rangle \otimes |0001\rangle = |0\rangle \otimes |1\rangle$.

Figure 17.6 Perfluorobutadienyl molecule used in the experimental implementation of Shor's algorithm. The magnetic moments of nuclei numbered 1 to 7 correspond to the qubits of the circuit in Figure **17.5**. For a magnetic field of 11.7 T, the shifted Larmor frequencies $\omega_i/2\pi$ (measured around 470 MHz for F^{19} and 125 MHz for C^{13}), as well as the couplings J_{ij}, are given in Hz. Relaxation times T_{i1} and T_{i2} are given in seconds. [Source: [VSBYSC] Nature vol. 414, pp. 883–887 (2001)].

state $|0000001\rangle$, corresponding to the tensor product of the "integers" $|0\rangle \otimes |1\rangle$. Stage (1) corresponds to the action of the Hadamard gates, which prepare the coherent superposition

$$\frac{1}{2^4} \sum_{x=0}^{7} |x\rangle \otimes |1\rangle.$$

The third stage, (2), performs modular exponentiation. The state becomes

$$(|0\rangle + |4\rangle) \otimes |1\rangle + (|1\rangle + |5\rangle) \otimes |7\rangle + (|2\rangle + |6\rangle) \otimes |4\rangle + (|3\rangle + |7\rangle) \otimes |3\rangle.$$

Finally, in stage (3), the quantum Fourier transform is applied and gives an output state that is

$$\textit{a superposition of the states } |0\rangle, |2\rangle, |4\rangle, |6\rangle \textit{ (check the calculation!)}$$

Applying the measurement postulate, we find $\text{Prob}(y) = 1/4$ for $y = 0, 2, 4, 6$ and $\text{Prob}(y) = 0$ for $y = 1, 3, 5, 7$. We observe that $M/r = 2$. Since $M = 2^3 = 8$, this gives $r = 4$, which is the correct result.

These remarks show that when reading out the final state using the techniques of the previous section, we should observe spectral lines corresponding to the states $|0\rangle = |000\rangle$, $|2\rangle = |010\rangle$, $|4\rangle = |100\rangle$, and $|6\rangle = |110\rangle$. Let us now discuss the experimental implementation itself.

The experiment uses a solution containing synthetic molecules with, among other nuclei, seven active spin-1/2 nuclei. More precisely, there are two C^{13} nuclei and five F^{19}

nuclei. A schematic representation of the molecule is shown in Figure **17.6**, together with the numbering used for the qubits. The shifted Larmor frequencies and the couplings of the seven active nuclei can be determined experimentally and are indicated in the table. Each molecule may be thought of as a "quantum circuit", or at least as the physical substrate on which the circuit is implemented.

Figure **17.7** shows the pulse sequence used to implement the single-qubit gates, while the two-qubit gates are generated naturally through spin–spin couplings.

Figure 17.7 Time sequence of radio-frequency pulses acting on qubits 1 through 7 of the molecule. [Source: [VSBYSC] Nature vol. 414, pp. 883–887 (2001)].

In this figure, lines 1 through 7 represent the seven qubits (nuclei), the horizontal axis represents time, and the vertical bars indicate the times at which the pulses act. As explained above, the duration of each pulse is negligible (of order 10^{-6} s) compared with the intervals between pulses (of order 10^{-3} s), during which the system undergoes its natural evolution. Four stages are separated by vertical dashed lines: initialization stage (0), which prepares the initial state; stage (1), which prepares the coherent superposition; stage (2), the longest stage (with total duration $\sim$ 400 ms), which computes the modular exponentiation; and stage (3), which performs the QFT (duration $\sim$ 120 ms). The total duration of the experiment is 720 ms. Note that the technique used to prepare the initial state is nontrivial and was one of the innovations of this experiment. Indeed, the state of the seven qubits is not initially the pure state $|0000001\rangle$, but rather a thermal mixed state that is transformed into a "pseudo-pure" state by appropriate operations. This preparation step is in fact an important limitation when the number of qubits increases. We will not discuss it further here.

A few additional details about the different pulse types are useful. The tall red bars are $\pi/2$ pulses corresponding to rotations about the positive x axis (no cross), negative x axis (lower cross), and positive y axis (upper cross). When these bars appear in isolation they represent Hadamard gates; when they occur in pairs, they are separated by an interval of evolution corresponding to a two-qubit gate. The blue bars represent pulses used for refocusing. They are rotations by an angle π about the x axis (positive $\rightarrow$ dark blue; negative $\rightarrow$ light blue). The short green bars represent rotations about z.

It is worth noting that the great majority of the pulses are related to refocusing rather than directly to gates in Shor's quantum circuit. The pulse sequence required for refocusing was determined by numerical simulations before being implemented in the NMR experiment. In addition, a decoherence model was used to simulate the dynamics. All these aspects lie far beyond the scope of this introduction.

We finally come to the last stage, which consists in reading out the *output state* of the qubits. Readout $\pi/2$ pulses are tuned to the resonance frequencies of the first three

Figure 17.8 Experimental spectrum of the first three qubits after preparation of the initial state. It is a mixed state that closely approximates the pure state $|\uparrow\uparrow\uparrow\rangle$. [Source: [VSBYSC] Nature vol. 414, pp. 883–887 (2001)].

qubits. Their spins are tipped into the xy plane and precess about z, thereby inducing a signal in the coil according to Faraday's law. The Fourier spectrum of this signal is shown in Figure **17.9**.

Figure 17.9 Ideal theoretical (first row), experimental (second row), and decoherence-model simulation (third row) spectra of the three qubits at the output of the circuit. [Source: [VSBYSC] Nature vol. 414, pp. 883–887 (2001)].

This spectrum contains several frequencies because of the many chemical-shift effects. Nevertheless, it immediately shows that in the output state qubit 0 was in the state $|\uparrow\rangle$ (i.e. $|0\rangle$). Qubits 1 and 2, on the other hand, are in superposition states of $|\uparrow\rangle$ and $|\downarrow\rangle$ (i.e. $|0\rangle$ and $|1\rangle$). We can therefore conclude that the output state was a superposition of

$$|000\rangle,\ |010\rangle,\ |100\rangle,\ |110\rangle.$$

The integers appearing in this superposition are $|0\rangle$, $|2\rangle$, $|4\rangle$, and $|6\rangle$, exactly as predicted by the theory. This implies $M/r = 2$ and hence $r = 4$, since $M = 2^3 = 8$.

Notes