Chapter 1

Qubits and Quantum Measurement

1.1 The Double Slit Experiment

A great deal of insight into the quantum theory can be gleaned by addressing the question, *is light transmitted by particles or waves?* Until quite recently, the evidence strongly favored wave-like propagation. Diffraction of light, a wave interference phenomenon, was observed as long ago as 1655 by Grimaldi. In fact, a rather successful theory of wave-like light propagation, due to Huygens, was developed in 1678. Perhaps the most striking confirmation of the wave nature of light was the double-slit interference experiment performed by Young in 1802. However, a dilemma began in the late 19th century when theoreticians such as Wien calculated how might light should be emitted by hot objects (*i.e.,* blackbody radiation). Their wave-based calculation differed dramatically from what was observed experimentally. At about the same time, the 1890's, it was noticed that the behavior of electrons kicked out of metals by light, the photoelectric effect, was strikingly inconsistent with any existing wave theory. In the first decade of the 20th century, blackbody radiation and the photoelectric effect were explained by treating light not as a wave phenomenon, but as particles containing discrete packets of energy, which we now call *photons*.

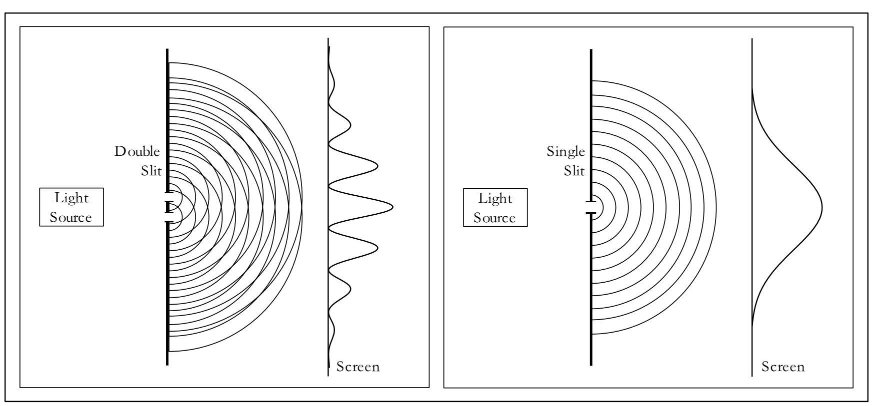


Figure 1.1: Double- and single-slit diffraction. Notice that in the double-slit experiment the two paths interfere with one another. This experiment gives evidence that light propagates as a wave.

To illustrate this seeming paradox, let us recall Young's double-slit experiment, which consists of a source of light, an intermediate screen with two very thin identical slits, and a viewing screen; see Figure 1.1. If only one slit is open then intensity of light on the viewing screen is maximum on the straight line path and falls off in either direction. However, if both slits are open, then the intensity oscillates according to the familiar interference pattern predicted by wave theory. These facts can be very convincingly explained, both qualitatively and quantitatively, by positing that light travels in waves.

Suppose, however, that you were to place photodetectors at the viewing screen, and turn down the intensity of the light source until the photodetectors only occasionally record the arrival of a photon, then you would make a very surprising discovery. To begin with, you would notice that as you turn down the intensity of the source, the magnitude of each click remains constant, but the time between successive clicks increases. You could infer that light is emitted from the source as discrete particles (photons) — the intensity of light is proportional to the rate at which photons are emitted by the source. And since you turned the intensity of the light source down sufficiently, it only emits a photon once every few seconds. You might now ask the question, once a photon is emitted from the light source, where will it hit the viewing screen. The answer is no longer deterministic, but probabilistic. You can only speak about the probability that a photodetector placed at point x detects the photon. So what is the probability that the photon is detected at point x in the setup of the double slit experiment with the light intensity turned way down? If only a single slit is open, then plotting this probability of detection as a function of x gives the same curve as the intensity as a function of x in the classical Young experiment. So far this should agree with your intuition, since the photon should randomly scatter as it goes through the slit. What happens when both slits are open? Our intuition would strongly suggest that the probability we detect the photon at x should simply be the sum of the probability of detecting it at x if only slit 1 were open and the probability if only slit 2 were open. In other words the outcome should no longer be consistent with the interference pattern. If you were to actually carry out the experiment, you would make the very surprising discovery that the probability of detection does still follow the interference pattern. Reconciling this outcome with the particle nature of light appears impossible, and this is the basic dilemma we face.

Before proceeding further, let us try to better understand in what sense the outcome of the experiment is inconsistent with the particle nature of light. Clearly, for the photon to be detected at x, either it went through slit 1 and ended up at x or it went through slit 2 and ended up at x. And the probability of seeing the photon at x should then be the sum of the probabilities of the two cases. The nature of the contradiction can be seen even more clearly at "dark" points x, where the probability of detection is 0 when both slits are open, even though it is non-zero if either slit is open. This truly defies reason! After all, if the photon has non-zero probability of going through slit 1 and ending up at x, how can the existence of an additional trajectory for getting to x possibly decrease the probability that it arrives at x?

Quantum mechanics provides a way to reconcile both the wave and particle nature of light. Let us sketch how it might address the situation described above. Quantum mechanics introduces the notion of the complex amplitude $\psi_1(x) \in \mathbb{C}$ with which the photon goes through slit 1 and hits point x on the viewing screen. The probability that the photon is actually detected at x is the square of the magnitude of this complex number: $P_1(x) = |\psi_1(x)|^2$. Similarly, let $\psi_2(x)$ be the amplitude if only slit 2 is open. $P_2(x) = |\psi_2(x)|^2$.

Now when both slits are open, the amplitude with which the photon hits point x on the screen is just the sum of the amplitudes over the two ways of getting there: $\psi_{12}(x) = \psi_1(x) + \psi_2(x)$. As before the probability that the photon is detected at x is the squared magnitude of this amplitude: $P_{12}(x) = |\psi_1(x) + \psi_2(x)|^2$. The two complex numbers $\psi_1(x)$ and $\psi_2(x)$ can cancel each other out to produce destructive interference, or reinforce each other to produce constructive interference or anything in between.

Some of you might find this "explanation" quite dissatisfying. You might say it is not an explanation at all. Well, if you wish to understand how Nature behaves you have to reconcile yourselves to this type of explanation — this wierd way of thinking has been successful at describing (and understanding) a vast range of physical phenomena. But you might persist and (quite reasonably) ask "but how does a particle that went through the first slit know that the other slit is open"? In quantum mechanics, this question is not well-posed. Particles do not have trajectories, but rather take all paths simultaneously (in superposition). As we shall see, this is one of the key features of quantum mechanics that gives rise to its paradoxical properties as well as provides the basis for the power of quantum computation. To quote Feynman, 1985, "The more you see how strangely Nature behaves, the harder it is to make a model that explains how even the simplest phenomena actually work. So theoretical physics has given up on that."

1.2 Basic Quantum Mechanics

Feynman also said, "I think I can safely say that nobody understands quantum mechanics." Paradoxically, quantum mechanics is a very simple theory, whose fundamental principles can be stated very concisely and are enshrined in the three basic postulates of quantum mechanics - indeed we will go through these postulates over the course of the next two chapters. The challenge lies in understanding and applying these principles, which is the goal of the rest of the book (and will continue through more advanced courses and research if you choose to pursue the subject further):

- The superpostion principle: this axiom tells us what are the allowable (possible) states of a given quantum system. An addendum to this axiom tells us given two subsystems, what the allowable states of the composte system are.

- The measurement principle: this axiom governs how much information about the state we can access.

- Unitary evolution: this axoim governs how the state of the quantum system evolves in time.

In keeping with the philosophy of the book, we will introduce the basic axioms gradually, starting with simple finite systems, and simplified basis state measurements, and building our way up to the more general formulations. This should allow the reader a chance to develop some intuition about these topics.

1.3 The Superposition Principle

Consider a system with k distinguishable (classical) states. For example, the electron in a hydrogen atom is only allowed to be in one of a discrete set of energy levels, starting with the ground state, the first excited state, the second excited state, and so on. If we assume a suitable upper bound on the total energy, then the electron is restricted to being in one of k different energy levels — the ground state or one of $k-1$ excited states. As a classical system, we might use the state of this system to store a number between 0 and $k-1$. The superposition principle says that if a quantum system can be in one of two states then it can also be placed in a linear superposition of these states with complex coefficients.

Let us introduce some notation. We denote the ground state of our k-state system by $|0\rangle$, and the succesive excited states by $|1\rangle, \ldots, |k-1\rangle$. These are the k possible classical states of the electron. The superposition principle tells us that, in general, the quantum state of the electron is $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{k-1} |k-1\rangle$, where $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ are complex numbers normalized so that $\sum_j |\alpha_j|^2 = 1$. α_j is called the *amplitude of the state* $|j\rangle$. For instance, if $k = 3$, the state of the electron could be

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{2} |1\rangle + \frac{1}{2} |2\rangle$$

or

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{2} |1\rangle + \frac{i}{2} |2\rangle$$

or

$$|\psi\rangle = \frac{1+i}{3} |0\rangle - \frac{1-i}{3} |1\rangle + \frac{1+2i}{3} |2\rangle .$$

The superposition principle is one of the most mysterious aspects about quantum physics — it flies in the face of our intuitions about the physical world. One way to think about a superposition is that the electron does not make up its mind about whether it is in the ground state or each of the $k-1$ excited states, and the amplitude α_0 is a measure of its inclination towards the ground state. Of course we cannot think of α_0 as the probability that an electron is in the ground state — remember that α_0 can be negative or imaginary. The measurement priniciple, which we will see shortly, will make this interpretation of α_0 more precise.

1.4 The Geometry of Hilbert Space

We saw above that the quantum state of the k-state system is described by a sequence of k complex numbers $\alpha_0, \ldots, \alpha_{k-1} \in \mathbb{C}$, normalized so that $\sum_j |\alpha_j|^2 = 1$. So it is natural to write the state of the system as a k dimensional vector:

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \end{pmatrix}$$

The normalization on the complex amplitudes means that the state of the system is a unit vector in a k dimensional complex vector space — called a Hilbert space.

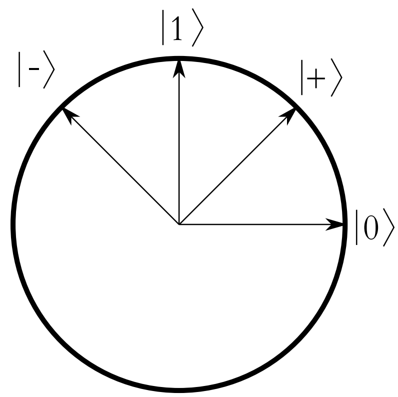


Figure 1.2: Representation of qubit states as vectors in a Hilbert space.

But hold on! Earlier we wrote the quantum state in a very different (and simpler) way as: $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{k-1} |k-1\rangle$. Actually this notation, called Dirac's ket notation, is just another way of writing a vector. Thus

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |k-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

So we have an underlying geometry to the possible states of a quantum system: the k distinguishable (classical) states $|0\rangle, \ldots, |k-1\rangle$ are represented by mutually orthogonal unit vectors in a k-dimensional complex vector space. i.e. they form an orthonormal basis for that space (called the standard basis). Moreover, given any two states, $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{k-1} |k-1\rangle$, and $\beta |0\rangle + \beta |1\rangle + \cdots + \beta |k-1\rangle$, we can compute the inner product of these two vectors, which is $\sum_{j=0}^{k-1} \alpha_j^* \beta_j$. The absolute value of the inner product is the cosine of the angle between these two vectors in Hilbert space. You should verify that the inner product of any two basis vectors in the standard basis is 0, showing that they are orthogonal.

The advantage of the ket notation is that the it labels the basis vectors explicitly. This is very convenient because the notation expresses both that the state of the quantum system is a vector, while at the same time explicitly writing out the physical quantity of interest (energy level, position, spin, polarization, etc).

1.5 Bra-ket Notation

In this section we detail the notation that we will use to describe a quantum state, $|\psi\rangle$. This notation is due to Dirac and, while it takes some time to get used to, is incredibly convenient.

Inner Products

We saw earlier that all of our quantum states live inside a Hilbert space. A Hilbert space is a special kind of vector space that, in addition to all the usual rules with vector spaces, is also endowed with an inner product. And an inner product is a way of taking two states (vectors in the Hilbert space) and getting a number out. For instance, define

$$|\psi\rangle = \sum_k a_k |k\rangle ,$$

where the kets $|k\rangle$ form a basis, so are orthogonal. If we instead write this state as a column vector,

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix}$$

Then the inner product of $|\psi\rangle$ with itself is

$$\langle \psi, \psi \rangle = \begin{pmatrix} a_0^* & a_1^* & \cdots & a_{N_1}^* \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} = \sum_{k=0}^{N-1} a_k^* a_k = \sum_{k=0}^{N-1} |a_k|^2$$

The complex conjugation step is important so that when we take the inner product of a vector with itself we get a real number which we can associate with a length. Dirac noticed that there could be an easier way to write this by defining an object, called a “bra,” that is the conjugate-transpose of a ket,

$$\langle \psi| = |\psi\rangle^\dagger = \sum_k a_k^* \langle k| .$$

This object acts on a ket to give a number, as long as we remember the rule,

$$\langle j| \, |k\rangle \equiv \langle j|k\rangle = \delta_{jk}$$

Now we can write the inner product of $|\psi\rangle$ with itself as

$$\begin{aligned} \langle \psi|\psi\rangle &= \left(\sum_j a_j^* \langle j| \right) \left(\sum_k a_k |k\rangle \right) \\ &= \sum_{j,k} a_j^* a_k \langle j|k\rangle \\ &= \sum_{j,k} a_j^* a_k \delta_{jk} \\ &= \sum_k |a_k|^2 \end{aligned}$$

Now we can use the same tools to write the inner product of any two states, $|\psi\rangle$ and $|\phi\rangle$, where

$$|\phi\rangle = \sum_k b_k |k\rangle .$$

Their inner product is,

$$\langle\psi|\phi\rangle = \sum_{j,k} a_j^* b_k \langle j|k\rangle = \sum_k a_k^* b_k$$

Notice that there is no reason for the inner product of two states to be real (unless they are the same state), and that

$$\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^* \in \mathbb{C}$$

In this way, a bra vector may be considered as a "functional." We feed it a ket, and it spits out a complex number.

The Dual Space

We mentioned above that a bra vector is a *functional* on the Hilbert space. In fact, the set of all bra vectors forms what is known as the *dual space*. This space is the set of *all* linear functionals that can act on the Hilbert space.

1.6 The Measurement Principle

This linear superposition $|\psi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle$ is part of the private world of the electron. Access to the information describing this state is severely limited — in particular, we cannot actually measure the complex amplitudes α_j. This is not just a practical limitation; it is enshrined in the measurement postulate of quantum physics.

A measurement on this k state system yields one of at most k possible outcomes: i.e. an integer between 0 and $k-1$. Measuring $|\psi\rangle$ in the standard basis yields j with probability $|\alpha_j|^2$.

One important aspect of the measurement process is that it alters the state of the quantum system: the effect of the measurement is that the new state is exactly the outcome of the measurement. I.e., if the outcome of the measurement is j, then following the measurement, the qubit is in state $|j\rangle$. This implies that you cannot collect any additional information about the amplitudes α_j by repeating the measurement.

Intuitively, a measurement provides the only way of reaching into the Hilbert space to probe the quantum state vector. In general this is done by selecting an orthonormal basis $|e_0\rangle, \ldots, |e_{k-1}\rangle$. The outcome of the measurement is $|e_j\rangle$ with probability equal to the square of the length of the projection of the state vector ψ on $|e_j\rangle$. A consequence of performing the measurement is that the new state vector is $|e_j\rangle$. Thus measurement may be regarded as a probabilistic rule for projecting the state vector onto one of the vectors of the orthonormal measurement basis.

Some of you might be puzzled about how a measurement is carried out physically? We will get to that soon when we give more explicit examples of quantum systems.

1.7 Qubits

Qubits (pronounced "cue-bit") or quantum bits are basic building blocks that encompass all fundamental quantum phenomena. They provide a mathematically simple framework in which to introduce the basic concepts of quantum physics. Qubits are 2-state quantum systems. For example, if we set $k = 2$, the electron in the Hydrogen atom can be in the ground state or the first excited state, or any superposition of the two. We shall see more examples of qubits soon.

The state of a qubit can be written as a unit (column) vector $\binom{\alpha}{\beta} \in \mathbb{C}^2$. In Dirac notation, this may be written as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{with} \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1.$$

This linear superposition $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is part of the private world of the electron. For us to know the electron's state, we must make a measurement. Making a measurement gives us a single classical bit of information — 0 or 1. The simplest measurement is in the standard basis, and measuring $|\psi\rangle$ in this $\{|0\rangle, |1\rangle\}$ basis yields 0 with probability $|\alpha|^2$, and 1 with probability $|\beta|^2$.

One important aspect of the measurement process is that it alters the state of the qubit: the effect of the measurement is that the new state is exactly the outcome of the measurement. *I.e.*, if the outcome of the measurement of $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ yields 0, then following the measurement, the qubit is in state $|0\rangle$. This implies that you cannot collect any additional information about α, β by repeating the measurement.

More generally, we may choose any orthogonal basis $\{|v\rangle, |w\rangle\}$ and measure the qubit in that basis. To do this, we rewrite our state in that basis: $|\psi\rangle = \alpha'\,|v\rangle + \beta'\,|w\rangle$. The outcome is v with probability $|\alpha'|^2$, and $|w\rangle$ with probability $|\beta'|^2$. If the outcome of the measurement on $|\psi\rangle$ yields $|v\rangle$, then as before, the the qubit is then in state $|v\rangle$.

Examples of Qubits

Atomic Orbitals

The electrons within an atom exist in quantized energy levels. Qualitatively these electronic orbits (or "orbitals" as we like to call them) can be thought of as resonating standing waves, in close analogy to the vibrating waves one observes on a tightly held piece of string. Two such individual levels can be isolated to configure the basis states for a qubit.

Photon Polarization

Classically, a photon may be described as a traveling electromagnetic wave. This description can be fleshed out using Maxwell's equations, but for our purposes we will focus simply on the fact that an electromagnetic wave has a *polarization* which describes the orientation of the electric field oscillations (see Fig. 1.4). So, for a given direction of photon motion, the photon's polarization axis might lie anywhere in a 2-d plane perpendicular to that motion. It is thus natural to pick an orthonormal 2-d basis (such as $\vec{x}$ and $\vec{y}$, or "vertical" and "horizontal") to describe the polarization state (i.e. polarization direction) of a photon. In a quantum mechanical description, this 2-d nature

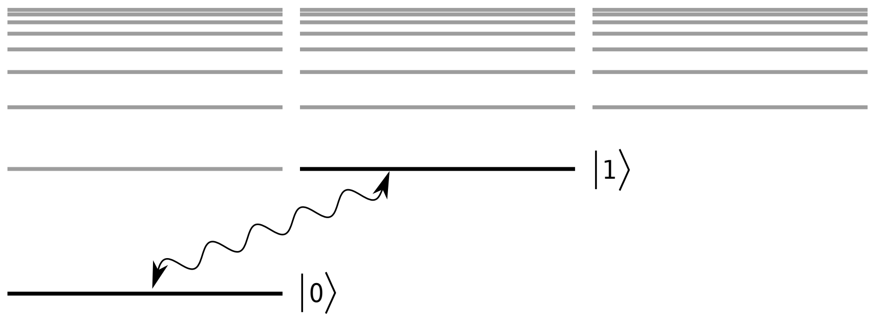


Figure 1.3: Energy level diagram of an atom. Ground state and first excited state correspond to qubit levels, $|0\rangle$ and $|1\rangle$, respectively.

of the photon polarization is represented by a qubit, where the amplitude of the overall polarization state in each basis vector is just the projection of the polarization in that direction.

The polarization of a photon can be measured by using a polaroid film or a calcite crystal. A suitably oriented polaroid sheet transmits x-polarized photons and absorbs y-polarized photons. Thus a photon that is in a superposition $|\phi\rangle = \alpha\,|\mathsf{x}\rangle + \beta\,|\mathsf{y}\rangle$ is transmitted with probability $|\alpha|^2$. If the photon now encounters another polariod sheet with the same orientation, then it is transmitted with probability 1. On the other hand, if the second polaroid sheet has its axes crossed at right angles to the first one, then if the photon is transmitted by the first polaroid, then it is definitely absorbed by the second sheet. This pair of polarized sheets at right angles thus blocks all the light. A somewhat counter-intuitive result is now obtained by interposing a third polariod sheet at a 45 degree angle between the first two. Now a photon that is transmitted by the first sheet makes it through the next two with probability 1/4.

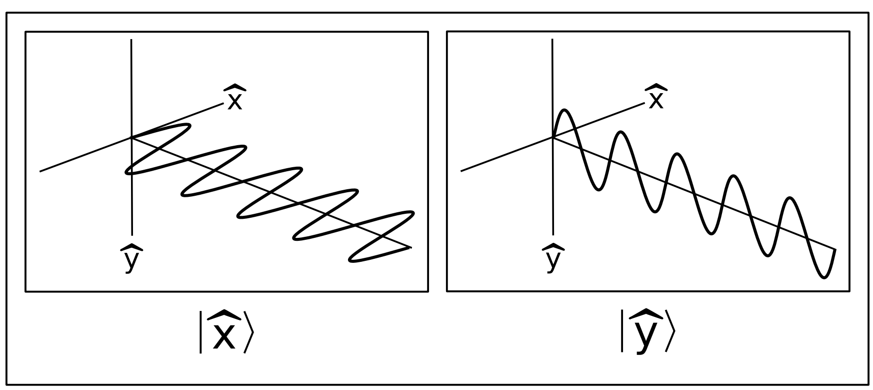


Figure 1.4: Using the polarization state of light as the qubit. Horizontal polarization corresponds to qubit state, $|\hat{\mathsf{x}}\rangle$, while vertical polarization corresponds to qubit state, $|\hat{\mathsf{y}}\rangle$.

To see this first observe that any photon transmitted through the first filter is in the state, $|0\rangle$. The probability this photon is transmitted through the second filter is 1/2 since it is exactly the probability that a qubit in the state $|0\rangle$ ends up in the state $|+\rangle$ when measured in the $|+\rangle, |-\rangle$ basis. We can repeat this reasoning for the third filter, except now we have a qubit in state $|+\rangle$ being measured in the $|0\rangle, |1\rangle$-basis — the chance that the outcome is $|0\rangle$ is once again 1/2.

Spins

Like photon polarization, the spin of a (spin-1/2) particle is a two-state system, and can be described by a qubit. Very roughly speaking, the spin is a quantum description of the magnetic moment of an electron which behaves like a spinning charge. The two allowed states can roughly be thought of as clockwise rotations ("spin-up") and counter clockwise rotations ("spin-down"). We will say much more about the spin of an elementary particle later in the course.

Measurement Example I: Phase Estimation

Now that we have discussed qubits in some detail, we can are prepared to look more closesly at the measurement principle. Consider the quantum state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle.$$

If we were to measure this qubit in the standard basis, the outcome would be 0 with probability 1/2 and 1 with probability 1/2. This measurement tells us only about the norms of the state amplitudes. Is there any measurement that yields information about the phase, θ?

To see if we can gather any phase information, let us consider a measurement in a basis other than the standard basis, namely

$$|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{and} \qquad |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

What does $|\phi\rangle$ look like in this new basis? This can be expressed by first writing,

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \qquad \text{and} \qquad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).$$

Now we are equipped to rewrite $|\psi\rangle$ in the $\{|+\rangle, |-\rangle\}$-basis,

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle) \\ &= \frac{1}{2}(|+\rangle + |-\rangle) + \frac{e^{i\theta}}{2}(|+\rangle - |-\rangle) \\ &= \frac{1+e^{i\theta}}{2}|+\rangle + \frac{1-e^{i\theta}}{2}|-\rangle \quad .\end{aligned}$$

Recalling the Euler relation, $e^{i\theta} = \cos\theta + i\sin\theta$, we see that the probability of measuring $|+\rangle$ is $\frac{1}{4}((1+\cos\theta)^2 + \sin^2\theta) = \cos^2(\theta/2)$. A similar calculation reveals that the probability of measuring $|-\rangle$ is $\sin^2(\theta/2)$. Measuring in the $(|+\rangle, |-\rangle)$-basis therefore reveals some information about the phase θ.

Later we shall show how to analyze the measurement of a qubit in a general basis.

Measurement example II: General Qubit Bases

What is the result of measuring a general qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, in a general orthonormal basis $|v\rangle, |v^\perp\rangle$, where $|v\rangle = a|0\rangle + b|1\rangle$ and $|v^\perp\rangle = b^*|0\rangle - a^*|1\rangle$? You should also check that $|v\rangle$ and $|v^\perp\rangle$ are orthogonal by showing that $\langle v^\perp|v\rangle = 0$.

To answer this question, let us make use of our recently acquired bra-ket notation. We first show that the states $|v\rangle$ and $|v^\perp\rangle$ are orthogonal, that is, that their inner product is zero:

$$\begin{aligned}
\left\langle v^\perp|v\right\rangle &= (b^*|0\rangle - a^*|1\rangle)^\dagger (a|0\rangle + b|1\rangle) \\
&= (b\langle 0| - a\langle 1|)^\dagger (a|0\rangle + b|1\rangle) \\
&= ba\langle 0|0\rangle - a^2\langle 1|0\rangle + b^2\langle 0|1\rangle - ab\langle 1|1\rangle \\
&= ba - 0 + 0 - ab \\
&= 0
\end{aligned}$$

Here we have used the fact that $\langle i|j\rangle = \delta_{ij}$.

Now, the probability of measuring the state $|\psi\rangle$ and getting $|v\rangle$ as a result is,

$$\begin{aligned}
P_\psi(v) &= |\langle v|\psi\rangle|^2 \\
&= |(a^*\langle 0| + b^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle)|^2 \\
&= |a^*\alpha + b^*\beta|^2
\end{aligned}$$

Similarly,

$$\begin{aligned}
P_\psi(v^\perp) &= \left|\left\langle v^\perp|\psi\right\rangle\right|^2 \\
&= |(b\langle 0| - a\langle 1|)(\alpha|0\rangle + \beta|1\rangle)|^2 \\
&= |b\alpha - a\beta|^2
\end{aligned}$$

Unitary Operators

The third postulate of quantum physics states that the evolution of a quantum system is necessarily unitary. Geometrically, a unitary transformation is a rigid body rotation of the Hilbert space, thus resulting in a transformation of the state vector that doesn't change its length.

Let us consider what this means for the evolution of a qubit. A unitary transformation on the Hilbert space $\mathbb{C}^2$ is specified by mapping the basis states $|0\rangle$ and $|1\rangle$ to orthonormal states $|v_0\rangle =$

$a|0\rangle + b|1\rangle$ and $|v_1\rangle = c|0\rangle + d|1\rangle$. It is specified by the linear transformation on $\mathbb{C}^2$:

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

If we denote by $U^\dagger$ the conjugate transpose of this matrix:

$$U^\dagger = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$$

then it is easily verified that $UU^\dagger = U^\dagger U = I$. Indeed, we can turn this around and say that a linear transformation U is unitary if and only if it satisfies this condition, that

$$UU^\dagger = U^\dagger U = I.$$

Let us now consider some examples of unitary transformations on single qubits or equivalently single qubit quantum gates:

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$ in the real plane. In the complex plane it is actually a π-rotation about the $\pi/8$ axis.

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

  The Hadamard Gate is one of the most important gates. Note that $H^\dagger = H$ – since H is real and symmetric – and $H^2 = I$.

- Rotation Gate. This rotates the plane by θ.

  $$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

- NOT Gate. This flips a bit from 0 to 1 and vice versa.

  $$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase Flip.

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

  The phase flip is a NOT gate acting in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis. Indeed, $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

How do we physically effect such a (unitary) transformation on a quantum system? To explain this we must first introduce the notion of the Hamiltonian acting on a system; you will have to wait for three to four lectures before we get to those concepts.

1.8 Problems

Problem 1

Show that

$$HZH = X$$

Problem 2

Verify that

$$U^\dagger U = UU^\dagger = I$$

for the general unitary operator,

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Chapter 2

Entanglement

What are the allowable quantum states of systems of several particles? The answer to this is enshrined in the addendum to the first postulate of quantum mechanics: the superposition principle. In this chapter we will consider a special case, systems of two qubits. In keeping with our philosophy, we will first approach this subject naively, without the formalism of the formal postulate. This will facilitate an intuitive understanding of the phenomenon of quantum entanglement — a phenomenon which is responsible for much of the ”quantum weirdness” that makes quantum mechanics so counter-intuitive and fascinating.

2.1 Two qubits

Now let us examine a system of two qubits. Consider the two electrons in two hydrogen atoms, each regarded as a 2-state quantum system:

Since each electron can be in either of the ground or excited state, classically the two electrons are in one of four states – 00, 01, 10, or 11 – and represent 2 bits of classical information. By the superposition principle, the quantum state of the two electrons can be any linear combination of these four classical states:

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

where $\alpha_{ij} \leq \mathbb{C}$, $\sum_{ij} |\alpha_{ij}|^2 = 1$. Of course, this is just Dirac notation for the unit vector in $\mathbb{C}^4$:

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

Measurement

As in the case of a single qubit, even though the state of two qubits is specified by four complex numbers, most of this information is not accessible by measurement. In fact, a measurement of a two qubit system can only reveal two bits of information. The probability that the outcome of the measurement is the two bit string $x \in \{0,1\}^2$ is $|\alpha_x|^2$. Moreover, following the measurement the state of the two qubits is $|x\rangle$. i.e. if the first bit of x is j and the second bit k, then following the measurement, the state of the first qubit is $|j\rangle$ and the state of the second is $|k\rangle$.

An interesting question comes up here: what if we measure just the first qubit? What is the probability that the outcome is 0? This is simple. It is exactly the same as it would have been if we had measured both qubits: $\Pr\{\text{1st bit } = 0\} = \Pr\{00\} + \Pr\{01\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. Ok, but how does this partial measurement disturb the state of the system?

The answer is obtained by an elegant generalization of our previous rule for obtaining the new state after a measurement. The new superposition is obtained by crossing out all those terms of $|\psi\rangle$ that are inconsistent with the outcome of the measurement (i.e. those whose first bit is 1). Of course, the sum of the squared amplitudes is no longer 1, so we must renormalize to obtain a unit vector:

$$|\phi_{\text{new}}\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Entanglement

Suppose the first qubit is in the state $3/5|0\rangle + 4/5|1\rangle$ and the second qubit is in the state $1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle$, then the joint state of the two qubits is $(3/5|0\rangle + 4/5|1\rangle)(1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle) = 3/5\sqrt{2}|00\rangle - 3/5\sqrt{2}|01\rangle + 4/5\sqrt{2}|10\rangle - 4/5\sqrt{2}|11\rangle$

Can every state of two qubits be decomposed in this way? Our classical intuition would suggest that the answer is obviously affirmative. After all each of the two qubits must be in some state $\alpha|0\rangle + \beta|1\rangle$, and so the state of the two qubits must be the product. In fact, there are states such as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which cannot be decomposed in this way as a state of the first qubit and that of the second qubit. Can you see why? Such a state is called an entangled state. When the two qubits are entangled, we cannot determine the state of each qubit separately. The state of the qubits has as much to do with the relationship of the two qubits as it does with their individual states.

If the first (resp. second) qubit of $|\Phi^+\rangle$ is measured then the outcome is 0 with probability 1/2 and 1 with probability 1/2. However if the outcome is 0, then a measurement of the second qubit results in 0 with certainty. This is true no matter how large the spatial separation between the two particles.

The state $|\Phi^+\rangle$, which is one of the Bell basis states, has a property which is even more strange and wonderful. The particular correlation between the measurement outcomes on the two qubits holds true no matter which rotated basis a rotated basis $|v\rangle, |v^\perp\rangle$ the two qubits are measured in, where $|0\rangle = \alpha|v\rangle + \beta\left|v^{\perp}\right\rangle$ and $|1\rangle = -\beta|v\rangle + \alpha\left|v^{\perp}\right\rangle$. This can bee seen as,

$$\begin{aligned}\left|\Phi^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\left(\alpha|v\rangle + \beta\left|v^{\perp}\right\rangle\right) \otimes \left(\alpha|v\rangle + \beta\left|v^{\perp}\right\rangle\right)\right) \\ &\quad - \frac{1}{\sqrt{2}}\left(\left(-\beta|v\rangle + \alpha\left|v^{\perp}\right\rangle\right) \otimes \left(-\beta|v\rangle + \alpha\left|v^{\perp}\right\rangle\right)\right) \\ &= \frac{1}{\sqrt{2}}\left(\left(\alpha^2 + \beta^2\right)|vv\rangle + \left(\alpha^2 + \beta^2\right)\left|v^{\perp}v^{\perp}\right\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|vv\rangle + |v^{\perp}v^{\perp}\rangle\right)\end{aligned}$$

Two Qubit Gates

Recall that the third axiom of quantum physics states that the evolution of a quantum system is necessarily unitary. Intuitively, a unitary transformation is a rigid body rotation of the Hilbert space. In particular it does not change the length of the state vector.

Let us consider what this means for the evolution of a two qubit system. A unitary transformation on the Hilbert space $\mathbb{C}^4$ is specified by a $4x4$ matrix U that satisfies the condition $UU^{\dagger} = U^{\dagger}U = I$. The four columns of U specify the four orthonormal vectors $|v_{00}\rangle$, $|v_{01}\rangle$, $|v_{10}\rangle$ and $|v_{11}\rangle$ that the basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are mapped to by U.

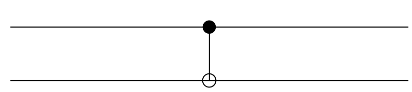
A very basic two qubit gate is the controlled-not gate or the CNOT:

Controlled Not (CNOT)

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The first bit of a CNOT gate is called the "control bit," and the second the "target bit." This is because (in the standard basis) the control bit does not change, while the target bit flips if and only if the control bit is 1.

The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



Though the CNOT gate looks very simple, any unitary transformation on two qubits can be closely approximated by a sequence of CNOT gates and single qubit gates. This brings us to an important point. What happens to the quantum state of two qubits when we apply a single qubit gate to one of them, say the first? Let's do an example. Suppose we apply a Hadamard gate to the superposition: $|\psi\rangle = 1/2\,|00\rangle - i/\sqrt{2}\,|01\rangle + 1/\sqrt{2}\,|11\rangle$. Then this maps the first qubit as follows:

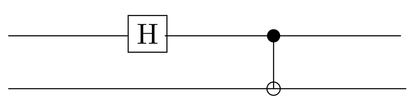
$$\begin{aligned}|0\rangle &\to 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle\\ |1\rangle &\to 1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle\,.\end{aligned}$$

So

$$\begin{aligned}|\psi\rangle &\to 1/2\sqrt{2}\,|00\rangle + 1/2\sqrt{2}\,|01\rangle - i/2\,|00\rangle + i/2\,|01\rangle + 1/2\,|10\rangle - 1/2\,|11\rangle\\ &= (1/2\sqrt{2} - i/2)\,|00\rangle + (1/2\sqrt{2} + i/2)\,|01\rangle + 1/2\,|10\rangle - 1/2\,|11\rangle\,.\end{aligned}$$

Bell states

We can generate the Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$ with the following simple quantum circuit consisting of a Hadamard and CNOT gate:



The first qubit is passed through a Hadamard gate and then both qubits are entangled by a CNOT gate.

If the input to the system is $|0\rangle \otimes |0\rangle$, then the Hadamard gate changes the state to

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \;\; ,$$

and after the CNOT gate the state becomes $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the Bell state $|\Phi^+\rangle$.

Notice that the action of the CNOT gate is not so much copying, as our classical intuition would suggest, but rather to entangle.

The state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$ is one of four Bell basis states:

$$\begin{aligned}\left|\Phi^\pm\right\rangle &= \tfrac{1}{\sqrt{2}}\,(|00\rangle \pm |11\rangle)\\ \left|\Psi^\pm\right\rangle &= \tfrac{1}{\sqrt{2}}\,(|01\rangle \pm |10\rangle) \quad .\end{aligned}$$

These maximally entangled states on two qubits form an orthonormal basis for $\mathbb{C}^4$. Exercise: give a simple quantum circuit for generating each of these states, and prove that the Bell basis states form an orthonormal basis for $\mathbb{C}^4$.

So far we have avoided a discussion of the addendum to the superposition axiom, which tells us the allowable states of a composite quantum system consisting of two subsystems. The basic question for our example of a two qubit system is this: how do the 2-dimensional Hilbert spaces corresponding to each of the two qubits relate to the 4-dimensional Hilbert space corresponding to the composite system? i.e. how do we glue two 2-dimensional Hilbert spaces to get a 4-dimensional Hilbert space? This is done by taking a tensor product of the two spaces.

Let us describe this operation of taking tensor products in a slightly more general setting. Suppose we have two quantum systems - a k-state system with associated k-dimensional Hilbert space V with orthonormal basis $|0\rangle, \ldots, |k-1\rangle$ and a l-state system with associated l-dimensional Hilbert space W with orthonormal basis $|0\rangle, \ldots, |l-1\rangle$. What is resulting Hilbert space obtained by gluing these two Hilbert spaces together? We can answer this question as follows: there are kl distinguishable states of the composite system — one for each choice of basis state $|i\rangle$ of the first system and basis state $|j\rangle$ of the second system. We denote the resulting of dimension kl Hilbert space by $V \otimes W$ (pronounced "V tensor W"). The orthonormal basis for this new Hilbert space is given by:

$$\{|i\rangle \otimes |j\rangle : 0 \leq i \leq k-1, 0 \leq j \leq l-1\},$$

So a typical element of $V \otimes W$ will be of the form $\sum_{ij} \alpha_{ij}(|i\rangle \otimes |j\rangle)$.

In our example of a two qubit system, the Hilbert space is $\mathbb{C}^2 \otimes \mathbb{C}^2$, which is isomorphic to the four dimensional Hilbert space $\mathbb{C}^4$. Here we are identifying $|0\rangle \otimes |0\rangle$ with $|00\rangle$.

EPR Paradox:

Everyone has heard Einstein's famous quote "God does not play dice with the Universe". The quote is a summary of the following passage from Einstein's 1926 letter to Max Born: "Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot, but does not really bring us any closer to the secret of the Old One. I, at any rate, am convinced that He does not throw dice." Even to the end of his life, Einstein held on to the view that quantum physics is an incomplete theory and that some day we would learn a more complete and satisfactory theory that describes nature.

In what sense did Einstein consider quantum mechanics to be incomplete? To understand this better, let us imagine that we were formulating a theory that would explain the act of flipping a coin. A simple model of a coin flip is that its outcome is random — heads 50% of the time, and tails 50% of the time. This model seems to be in perfect accordance with our experience with flipping a coin, but it is incomplete. A more complete theory would say that if we were able to determine the initial conditions of the coin with perfect accuracy (position, momentum), then we could solve Newton's equations to determine the eventual outcome of the coin flip with certainty. The coin flip amplifies our lack of knowledge about the initial conditions, and makes the outcome seem completely random. In the same way, Einstein believed that the randomness in the outcome of quantum measurements reflected our lack of knowledge about additional degrees of freedom of the quantum system.

Einstein sharpened this line of reasoning in a paper he wrote with Podolsky and Rosen in 1935, where they introduced the famous Bell states. Recall that for Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, when you measure first qubit, the second qubit is determined. However, if two qubits are far apart, then the second qubit must have had a determined state in some time interval before measurement, since the speed of light is finite. By the rotational symmetry of the Bell state, which we saw earlier, this fact holds in every basis. This appears analogous to the coin flipping example. EPR therefore suggested that there is a more complete theory where "God does not throw dice." Until his death in 1955, Einstein tried to formulate a more complete "local hidden variable theory" that would describe the predictions of quantum mechanics, but without resorting to probabilistic outcomes. But in 1964, almost three decades after the EPR paper, John Bell showed that properties of Bell (EPR) states were not merely fodder for a philosophical discussion, but had verifiable consequences: local hidden variables are not the answer. He showed that there is a particular experiment that could be performed on two qubits entangled in a Bell state such no local hidden variable theory [1] could possibly match the outcome predicted by quantum mechanics. The Bell experiment has been performed to increasing accuracy, originally by Aspect, and the results have always been consistent with the predictions of quantum mechanics and inconsistent with local hidden variable theories.

2.2 Bell's Thought Experiment

Bell considered the following experiment: let us assume that two particles are produced in the Bell state $|\Phi^+\rangle$ in a laboratory, and the fly in opposite directions to two distant laboratories. Upon arrival, each of the two qubits is subject to one of two measurements. The decision about which of the two experiments is to be performed at each lab is made randomly at the last moment, so that speed of light considerations rule out information about the choice at one lab being transmitted to the other. The measurements are cleverly chosen to distinguish between the predictions of quantum mechanics and any local hidden variable theory. Concretely, the experiment measures the correlation between the outcomes of the two experiments. The choice of measurements is such that any classical hidden variable theory predicts that the correlation between the two outcomes can be at most 0.75, whereas quantum mechanics predicts that the correlation is $\cos^2 \pi/8 \approx 0.8$. Thus the experiment allows us to distinguish between the predictions of quantum mechanics and any local hidden variable theory! We now describe the experiment in more detail.

The two experimenters A and B (for Alice and Bob) each receives one qubit of a Bell state $|\Phi^+\rangle$, and measures it in one of two bases depending upon the value of a random bit r_A and r_B respectively. Denote by a and b respectively the outcomes of the measurements. We are interested in the highest achievable correlation between the two quantities $r_A \times r_B$ and $a + b(mod2)$. We will see below that there is a particular choice of bases for the quantum measurements made by A and B such that $P[r_A \times r_B = a + b(mod2)] = \cos^2 \pi/8 \approx .8$. Before we do so, let us see why no classical hidden variable theory allows a correlation of over 0.75. i.e. $P[r_A \times r_B = a + b(mod2)] \leq 0.75$.

We can no longer postpone a discussion about what a local hidden variable theory is. Let us do so in the context of the Bell experiment. In a local hidden variable theory, when the Bell state was created, the two particles might share an arbitrary amount of classical information, x. This information could help them coordinate their responses to any measurements they are subjected to in the future. By design, the Bell experiment selects the random bits r_A an r_B only after the two particles are too far apart to exchange any further information before they are measured. Thus we are in the setting, where A and B share some arbitrary classical information x, and are given as input independent, random bits x_A an x_B as input, and must output bits a and b respectively

[1] We will describe what we mean by a local hidden variable theory below after we start describing the actual experiment

to maximize their chance of achieving $r_A \times r_B = a + b(mod 2)$. It can be shown that the shared information x is of no use in increasing this correlation, and indeed, the best they can do is to always output $a = b = 0$. This gives $P[r_A \times r_B = a + b(mod 2)] \leq .75$.

Let us now describe the quantum measurements that achieve greater correlation. They are remarkably simple to describe:

- if $r_A = 0$, then Alice measures in the $-\pi/16$ basis.
- if $r_A = 1$, then Alice measures in the $3\pi/16$ basis.
- if $r_B = 0$, then Bob measures in the $\pi/16$ basis.
- if $r_B = 1$, then Bob measures in the $-3\pi/16$ basis.

The analysis of the success probability of this experiment is also beautifully simple. We will show that in each of the four cases $r_A = r_B = 0$, etc, the success probability $P[r_A \times r_B = a + b(mod 2)] = \cos^2 \pi/8$.

We first note that if Alice and Bob measure in bases that make an angle θ with each other, then the chance that their measurement outcomes are the same (bit) is exactly $\cos^2 \theta$. This follows from the rotational invariance of $|\Phi^+\rangle$ and the following observation: if the first qubit is measured in the standard basis, then the outcome is outcome is an unbiased bit. Moreover the state of the second qubit is exactly equal to the outcome of the measurement — $|0\rangle$ if the measurement outcome is 0, say. But now if the second qubit is measured in a basis rotated by θ, then the probability that the outcome is also 0 is exactly $\cos^2 \theta$.

Now observe that in three of the four cases, where $x_A \cdot x_B = 0$, Alice and Bob measure in bases that make an angle of $\pi/8$ with each other. By our observation above, $P[a + b \equiv 0 \mod 2] = P[a = b] = \cos^2 \pi/8$.

In the last case $x_A \cdot x_B = 1$, and they measure in bases that make an angle of $3\pi/8$ with each other. Now, $P[a + b \equiv 1 \mod 2] = P[a \neq b] = \sin^2 3\pi/8 = \cos^2 5\pi/8$.

2.3 No Cloning Theorem and Quantum Teleportation

The axioms of quantum mechanics are deceptively simple. Our view is that to begin to understand and appreciate them you have to be exposed to some of their most counterintuitive consequences. Paradoxically, this will help you build a better intuition for quantum mechanics.

In this chapter we will study three very simple but counterintuitive consequences of the laws of quantum mechanics. The theme of all three vignettes is the copying or transmission of quantum information.

No Cloning Theorem

Given a quantum bit in an unknown state $|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, is it possible to make a copy of this quantum state? i.e. create the state $|\phi\rangle \otimes |\phi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle)$? The axioms of quantum mechanics forbid this very basic operation, and the proof of the no cloning theorem helps gain insight into this.

To be more precise, we are asking whether it is possible to start with two qubits in state $|\phi\rangle \otimes |0\rangle$ and transform them to the state $|\phi\rangle \otimes |\phi\rangle$? By the third axiom of quantum mechanics, for this to be possible there must be a unitary transformation U such that $U|\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle$. We will show that no unitary transformation can achieve this simultaneously for two orthogonal states $|\phi\rangle$ and $|\psi\rangle$.

Recall that a unitary transformation is a rotation of the Hilbert space, and therefore necessarily preserves angles. Let us make this more precise. Consider two quantum states (say on a single qubit): $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. The cosine of the angle between them is given by (the absolute value of) their inner product: $\alpha_0^*\beta_0 + \alpha_1^*\beta_1$.

Now consider the quantum states (on two qubits) $|\phi\rangle \otimes |\phi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle)$ and $|\psi\rangle \otimes |\phi\rangle = (\beta_0|0\rangle + \beta_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle)$. Their inner product is: $(\alpha_0^*\beta_0 + \alpha_1^*\beta_1)^2$. i.e. $\langle\phi|\,\psi\rangle^2 = \langle\phi\phi|\,\psi\psi\rangle$.

We are now ready to state and prove the no cloning theorem:

Assume we have a unitary operator U and two quantum states $|\phi\rangle$ and $|\psi\rangle$:

$$\begin{array}{ccc} |\phi\rangle \otimes |0\rangle & \xrightarrow{U} & |\phi\rangle \otimes |\phi\rangle \\ |\psi\rangle \otimes |0\rangle & \xrightarrow{U} & |\psi\rangle \otimes |\psi\rangle \end{array} .$$

Then $\langle\phi|\psi\rangle$ is 0 or 1.

$\langle\phi|\psi\rangle = (\langle\phi| \otimes \langle 0|)(|\psi\rangle \otimes |0\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle^2$. In the second equality we used the fact that U, being unitary, preserves inner products.

Superdense Coding

Suppose Alice and Bob are connected by a *quantum* communications channel. By this we mean, for example, that they can communicate qubits over an optical fibre using polarized photons. Is this much more powerful than a classical communication channel, over which only classical bits may be transmitted? The answer seems obvious, since a classical bit is a special case of a quantum bit. And a qubit appears to encode an infinite number of bits of information, since to specify its state we must specify two complex numbers. However, the truth is a little more subtle, since the axioms of quantum mechanics also severely restrict how we may access information about the quantum state by a measurement.

So the question we wish to ask is "how many classical bits can Alice transmit to Bob in a message consisting of a single qubit?" We will show that if Alice and Bob share entanglement in the form of a Bell state, then Alice can transmit two classical bits by transmitting just one qubit over the quantum channel.

The overall idea is this: say Alice and Bob share $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice can transform this shared state to any of the four Bell basis states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ by applying a suitable quantum gate just to her qubit. Now if she transmits her qubit to Bob, he holds both qubits of of a Bell basis state and can perform a measurement in the Bell basis to distinguish which of the four states he holds.

Let's now see the details of Alice's protocol: if Alice wishes to transmit the two bit message b_1b_2, she applies a bit flip X to her qubit if $_1 = 1$ and a phase flip Z to her qubit if $b_2 = 1$. You should verify that in the four cases 00, 01, 10, 11 this results in the two qubits being in the state $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ respectively.

After receiving Alice's qubit, Bob measures the two qubits in the Bell basis by running the circuit we saw in chapter 2 backwards (i.e., applying $(H \otimes I) \circ CNOT$), then measuring in the standard basis.

Note that Alice really did use two qubits total to transmit the two classical bits. After all, Alice and Bob somehow had to start with a shared Bell state. However, the first qubit – Bob's half of the Bell state – could have been sent well before Alice had decided what message she wished to send to Bob.

One can show that it is not possible to do any better. No more than two classical bits can be transmitted by sending just one qubit. To see why you will have to understand our next example.

Quantum Teleportation

After months of effort, Alice has managed to synthesize a special qubit, which she strongly suspects has some wonderful physical properties. Unfortunately, she doesn't explicitly know the state vector $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$. And she does not have the equipment in her lab to carry out a crucial next phase of her experiment. Luckily Bob's lab has the right equipment, though it is at the other end of town. Is there a way for Alice to safely transport her qubit to Bob's lab?

If Alice and Bob share a Bell state, then there is a remarkable method for Alice to transmit her qubit to Bob. The method requires her to make a certain measurement on her two qubits: the qubit she wishes to transmit and her share of the Bell state. She then calls up Bob on the phone and tells him the outcome of her measurement — just two classical bits. Depending upon which of four outcomes Alice announces to him on the phone, Bob performs one of four operations on his qubit, and voila, his qubit is in the state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$!

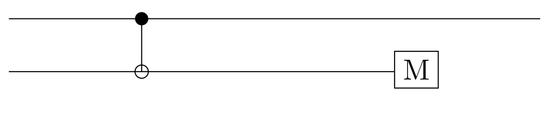
But hold on a moment, doesn't this violate the no cloning theorem?! No, because Alice's qubit was destroyed by measurement before Bob created his copy. Let us build our way to the teleportation protocol in a couple of simple stages:

Let us start with the following scenario. Alice and Bob share two qubits in the state $a\,|00\rangle + b\,|11\rangle$. Alice and Bob don't know the amplitudes a and b. How can Bob end up with the state $a\,|0\rangle + b\,|1\rangle$? An easy way to achieve this is to perform a CNOT gate on the two qubits with Bob's qubit as the control, and Alice's qubit as the target. But this requires an exchange of quantum information. What if Alice and Bob can only exchange classical information?

Here is a way. Alice performs a Hadamard on her qubit. The state of the two qubits is now $a/\sqrt{2}(|0\rangle + |1\rangle)\,|0\rangle + b/\sqrt{2}(|0\rangle - |1\rangle)\,|1\rangle = 1/\sqrt{2}\,|0\rangle\,(a\,|0\rangle + b\,|1\rangle) + 1/sqrt2\,|1\rangle\,(a\,|1\rangle - b\,|1\rangle)$. Now if Alice measures her qubit in the standard basis, if the measurement outcome is 0, then Bob's qubit is the desired $a\,|0\rangle + b\,|1\rangle$. If the measurement outcome is 1, then Bob's qubit is $a\,|0\rangle - b\,|1\rangle$. But in this case if Bob were to apply a phase flip gate (Z) to his qubit, it would end up in the desired state $a\,|0\rangle + b\,|1\rangle$.

Back to teleportation. Alice has a qubit in state $a\,|0\rangle + b\,|1\rangle$, and Alice and Bob share a Bell state. Is there any way for them to convert their joint state to $a\,|00\rangle + b\,|11\rangle$, without exchanging any quantum information? If they succeed, then by our previous discussion Alice can teleport her qubit to Bob.

Consider what happens if Alice applies a CNOT gate with her qubit $a\,|0\rangle + b\,|1\rangle$ as the control qubit, and her share of the Bell state as the target qubit.



$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=0,1} a_i|i\rangle \otimes \sum_{j=0,1} \frac{1}{\sqrt{2}}|j,j\rangle.$$

After passing through the CNOT gate this becomes

$$\sum_{i,j} a_i\big|i, i \oplus j, j\big\rangle.$$

Now A measures the middle qubit. Suppose it is measured as l; then $l = i \oplus j$. The state is now

$$\sum_{j} a_{j\oplus l}\big|j \oplus l, j\big\rangle.$$

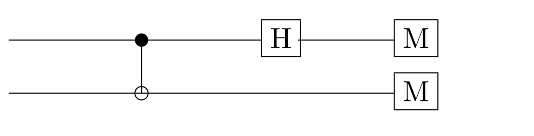
Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip on his qubit (the bottom qubit in the diagram.) A bit flip is just the transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we have

$$\sum_{j} a_{j\oplus l}\big|j, j\big\rangle.$$

Finally, B does a phase flip on his qubit, yielding

$$\sum_{j} a_{j}\big|j, j\big\rangle.$$

The correct solution is to go back and modify the original diagram, inserting a Hadamard gate and an additional measurement:



Now the algorithm proceeds exactly as before. However A's application of the Hadamard gate now induces the transformation

$$\sum_j a_j|j,j\rangle \longrightarrow \sum_{ij} a_j(-1)^{ij}|i,j\rangle.$$

Finally A measures i and sends the measurement to B. The state is now:

$$\sum_j a_j(-1)^{ij}|j\rangle.$$

If $i = 0$ then we are done; if $i = 1$ then B applies a phase flip. In either case the state is now $a_0|0\rangle + a_1|1\rangle$.

So A has transported the quantum state to B simply by sending two classical bits.