Quantum Computing as a High School Module

Anastasia Perry
aperry@imsa.edu

Ranbel Sun
rsun@andover.edu

Ciaran Hughes
chughes@fnal.gov

Joshua Isaacson
isaacson@fnal.gov

Jessica Turner
jturner@fnal.gov

Quantum computing is a growing field at the intersection of physics and computer science. This module introduces three of the key principles that govern how quantum computers work: superposition, quantum measurement, and entanglement. The goal of this module is to bridge the gap between popular science articles and advanced undergraduate texts by making some of the more technical aspects accessible to motivated high school students. Problem sets and simulation-based labs of various levels are included to reinforce the conceptual ideas described in the text.

This is intended as a one week course for high school students between the ages of 15-18 years. The course begins by introducing basic concepts in quantum mechanics which are needed to understand quantum computing.

Copyright

Disclaimer

The authors take no responsibility for broken links or if the web interface of referenced material changes. The views and opinions expressed here are those of the authors and do not necessarily reflect the official policy or position of any other agency, organization, employer, or company. The authors are not to be held responsible for misuse, reuse, recycled, cited and/or uncited copies of content.

Contents

Chapter 0

Course Description

0.1 About

Quantum computing is a growing field at the intersection of physics and computer science. This module introduces three key principles of quantum computing: superposition, quantum measurement, and entanglement. The goal of this course is to bridge the gap between popular science articles and advanced undergraduate texts, making some of the more technical aspects accessible to motivated high school students. Problem sets and simulation-based labs of various levels are included to reinforce the concepts described in the text.

Note that the module is not designed to be a comprehensive introduction to modern physics. Rather, it focuses on topics students may have heard about but are not typically covered in a general course. Given the usual constraints on teaching time, these materials could be used after the AP exams, in an extracurricular club, or as an independent project resource to give students a taste of what quantum computing is really about.

This is intended as a one-week course for high school students between the ages of 15-18 years. The course begins with the introduction of basic concepts in quantum mechanics needed to understand quantum computing.

0.2 Prerequisites

The material assumes knowledge of electricity, magnetism, and waves from high school-level physics. Introductory modern physics (photoelectric effect, wave/particle duality, etc.) is helpful but not required. No computer programming experience is necessary.

Each unit builds up to three different levels of complexity depending on the students' experience with math and abstract reasoning. All problems are labeled according to difficulty. In addition, the intermediate and advanced sections within each chapter are labeled such that one can skip over them if needed. Links to external resources are provided below for those who require a refresher.

● **Fundamental**

- Basic probability - Khan Academy Probability[1]

- Histograms - Khan Academy Histograms[2]

■ **Intermediate**

- Probability multiplication - Khan Academy Multiplication[3]

- Vector decomposition - Physics Classroom[4]

◆ **Advanced**

- Matrix multiplication - Khan Academy Matrix Multiplication[5]

- Interactive Matrix Multiplication - University of St. Andrews[6]

- Matrices as transformations - Khan Academy Matrices Transformations[7]

0.3 Learning Objectives

1. Introduction to Superposition

   - Qualitatively understand what it means for an object to be in a quantum superposition.
   - Identify the measurement outcome of a system in a classical vs. quantum superposition.

   Key Terms: *quantum system, quantum state, quantum superposition*

2. What is a Qubit?

   - Understand the difference between a classical bit and a qubit.

---

[1]https://www.khanacademy.org/math/statistics-probability/probability-library/basic-theoretical-probability/v/basic-probability

[2]https://www.khanacademy.org/math/ap-statistics/quantitative-data-ap/histograms-stem-leaf/v/histograms-intro

[3]https://www.khanacademy.org/math/statistics-probability/probability-library/multiplication-rule-independent/v/compound-sample-spaces

[4]http://www.physicsclassroom.com/class/vectors/Lesson-1/Vectors-and-Direction

[5]https://www.khanacademy.org/math/precalculus/precalc-matrices/multiplying-matrices-by-matrices/v/matrix-multiplication-intro

[6]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/MatrixMultiplication/MatrixMultiplication.html

[7]https://www.khanacademy.org/math/precalculus/precalc-matrices/matrices-as-transformations/v/transforming-position-vector

- Write a mathematical expression for the superposition of a two-state particle using "ket" notation.
- Compute the probability of finding the particle in a particular state given a normalized superposition state.
- Express a qubits' state as a vector and use matrix multiplication to change the state.

Key Terms: *qubit, ket notation, state amplitude, normalization, unitary matrix*

3. Creating Superposition: Beam splitter

- Explain how light behaves like a particle in the single-photon beam splitter experiment.
- Understand how the beam splitter creates a particle in a superposition state.
- Trace the path of light through a Mach-Zehnder interferometer from both a wave interference and particle perspective.

Key Terms: *photon, beam splitter, phase shift, Mach-Zehnder interferometer*

4. Creating Superposition: Stern-Gerlach

- Explain why electron spin could serve as an example of a qubit.
- Understand how the Stern-Gerlach experiment illustrates spin quantization, superposition, and measurement collapse.
- Define what is meant by a measurement basis and convert a given spin to a different basis.
- Compute the probability of an electron passing through one or more Stern-Gerlach apparatuses.

Key Terms: *spin, Stern-Gerlach experiment, measurement basis, orthogonal states, no-cloning theorem*

5. Quantum Cryptography

- Send a message with the one-time pad to understand what is meant by a cryptographic key.
- Generate a shared key using the BB84 quantum key distribution protocol.
- Show how the principles of superposition and measurement collapse make the protocol secure.

Key Terms: *key, quantum key distribution*

6. Quantum Gates

- Build and test simple quantum circuits on IBM's quantum computer simulator.
- Interpret the histograms produced by single qubit gates: the X, Hadamard, and Z gates.
- Predict the output of multiple gates in a row, including two successive Hadamards.
- Use the matrix representation of gates to determine the new state of the system.

Key Terms: *quantum gates, X gate, Hadamard gate, Z gate*

7. Entanglement

- Understand how measurement affects the state of entangled particles.
- Write the state of a multi-qubit system in "ket" notation.
- Identify whether two qubits are entangled given a particular state.
- Predict the output of circuits involving CNOT gates.
- Entangle two qubits using gates.

Key Terms: *quantum entanglement, product/separable states, entangled states, CNOT gate*

8. Quantum Teleportation

- Qualitatively understand how the quantum state of a particle could be transmitted from one place to another.
- Explain the limitations and paradoxes of quantum teleportation.

Key Terms: *quantum teleportation, no-cloning theorem*

9. Quantum Algorithms

- Understand the benefits and limitations of quantum computers.
- Use the Mach-Zehnder interferometer to implement the Deutsch-Jozsa quantum algorithm.
- Describe how superposition and interference are leveraged in quantum computing algorithms.

Key Terms: *quantum parallelism, Deutsch-Jozsa algorithm*

Alternative Pathways

The units are best studied in numerical order. However, for those with limited time, Figure 1 shows the minimum recommended prerequisites for each unit. A few references and examples may have to be skipped over, but the core content should still be understandable.
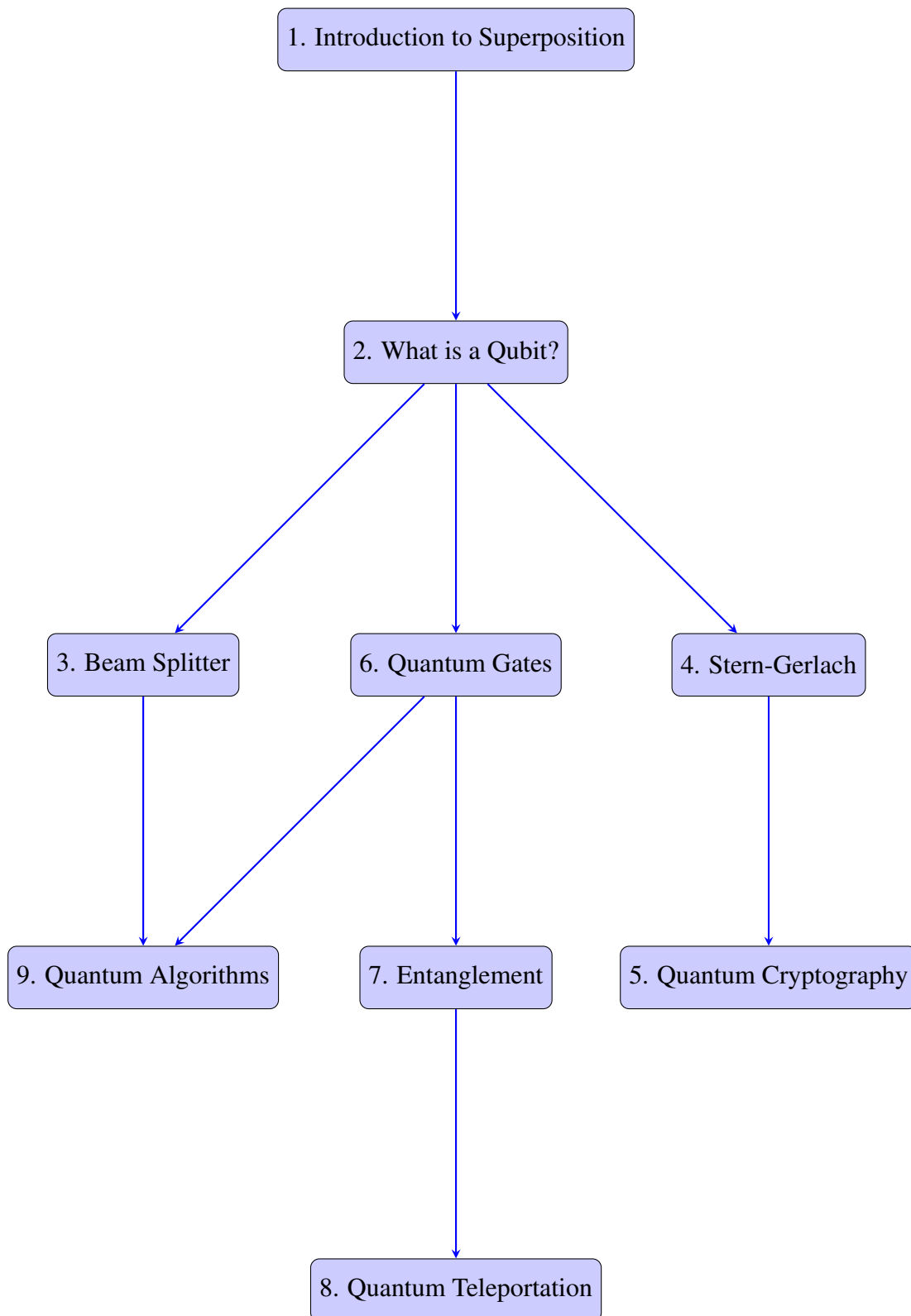
Figure 1: Flowchart of learning outcomes.

Chapter 1

Introduction to Superposition

In this section, we review the basic concepts of classical and quantum superposition. In Activities Sheet 1, we present the related activities and questions. Before going into specific details on quantum superposition, it is useful to explain how the term "superposition" is used in different contexts, i.e., in classical or quantum physics.

1.1 ● Classical Superposition

In classical physics, the concept of **superposition** is used to describe when two physical quantities are added together to make another third physical quantity that is entirely different from the original two. An example of the "superposition principle" in classical physics is clear when working with waves. Two pulses on a string which pass through each other will interfere following the principle of superposition as shown Figure 1.1. Noise-canceling headphones use superposition by creating sound waves with the same magnitude as the incoming sound wave but with a frequency completely out of phase, thereby canceling the sound wave.
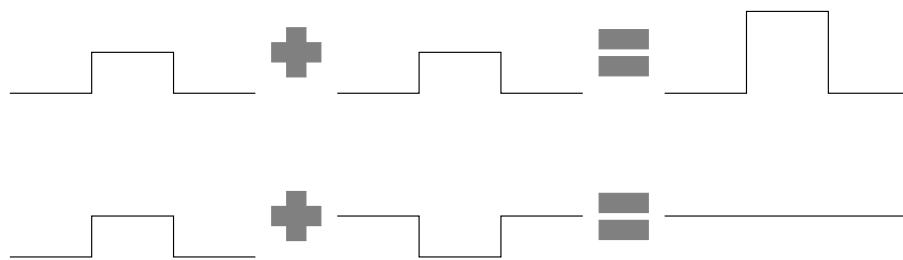

Figure 1.1: Examples of constructive and destructive interference due to the classical superposition principle.

Another common application of classical superposition is finding the total magnitude and direction of quantities such as force, electric field, magnetic field, etc.

For example, to calculate the total electric force $\vec{F}_{\text{total}}$ on a charge q_2 produced by other charges q_1 and q_3, one would sum the forces produced by each individual charge: $\vec{F}_{\text{total}} = \vec{F}_{12} + \vec{F}_{32}$. The challenge here is that forces are vectors, so vector addition is needed, as shown in Figure 1.2.
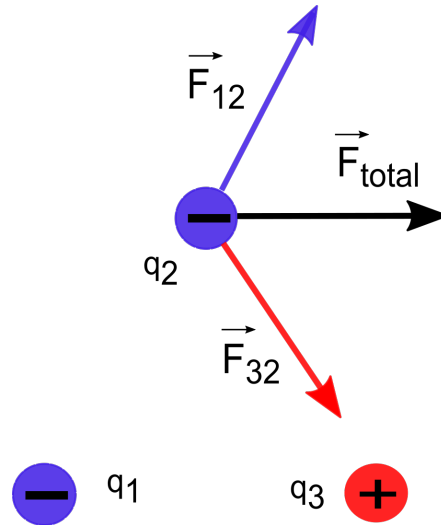
Figure 1.2: A classical superposition is used to calculate the total electric force on a charge q_2 due to charges q_1 and q_3.

1.2 ● Quantum Superposition

Quantum superposition is a phenomenon associated with quantum systems, i.e., small objects such as nuclei, electrons, elementary particles, and photons, for which wave-particle duality and other non-classical effects are observed. For example, you would normally expect that an object can have an arbitrary amount of kinetic energy, ranging from 0-∞ Joules. A baseball could be at rest or thrown at any speed. However, according to quantum mechanics, the ball's energy is **quantized**, meaning it can only take on certain values and nothing in between. This is counterintuitive, as we cannot observe it with our classical eyes. The gaps in energy are too small to be measured on the macroscopic level and as such can be treated as continuous for macroscopic physics. However, the gaps are more pronounced at smaller scales, as shown in Figure 1.3. Bohr successfully modeled the hydrogen atom by quantizing the energy levels of the proton-electron bound state. One aspect of quantum superposition is easily demonstrated using a coin. A coin has a 50/50 probability of landing as either heads or tails, as shown in Figure 1.4.

Question 1: What state is the coin in while it is in the air? Is it heads or tails?

Classical Systems   Quantum Systems

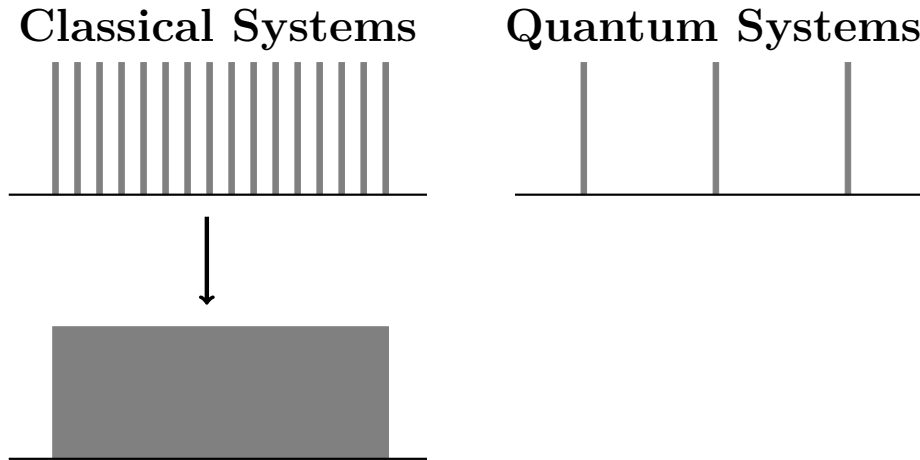Figure 1.3: Quantum effects associated with energy being quantized is important at the atomic scale and below. In this figure, the grey lines represent allowed energies. In quantum systems, the energies are quantized. As we zoom out of the quantum system to see it through a classical lens (represented by the downward arrow), the energies become more dense and appear continuous. This is the reason quantization is not noticeable in everyday objects.

We can say that the coin is in a superposition of both heads and tails. When it lands, it has a **definite state**, either heads or tails. The measurement destroys the superposition.

At any given time, a system can be described as being in a particular state. The state is related to its quantized values. For example, a tossed coin is either in a heads state or a tails state. An electron in an hydrogen atom could be in the ground state or an excited state. A quantum system is special because it can be in a superposition of these definite states, i.e., both heads and tails simultaneously. It is possible for a quantum object to exist in multiple states at the same time. The outcome of a measurement is to observe some definite state with some probability.

In Schrödinger's famous thought experiment, Schrödinger's cat is placed in a closed box with a single atom that has some probability of emitting deadly radiation at any time. Since radioactive nuclear decay is a spontaneous process, it is impossible to predict for certain when the nucleus decays. Therefore, you do not know whether the cat is alive or dead unless you open and look in the box. (Watch this video.)[1] It can be said that the cat is both alive **AND** dead with some probability. That is, the cat is in a quantum superposition state until you open the box and measure its state. Upon measurement, the cat is obviously either alive OR dead and the superposition has collapsed to a definite, non-superposition state.

Quantum systems can exist in a superposition state, and measuring the system will collapse the superposition state into one definite classical state. This might

---

[1]https://www.youtube.com/watch?v=uWMTOrux0LM
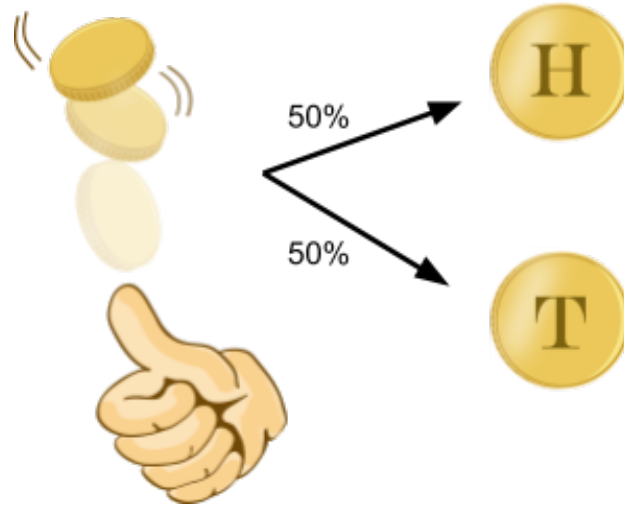
Figure 1.4: A tossed coin has a 50% chance of landing on heads or tails.

be hard to understand from a classical point of view, as we usually do not see quantum superposition in macroscopic objects. Einstein was really bothered by this feature of quantum systems. His friend, Abraham Pais, records: "I recall that during one walk, Einstein suddenly stopped, turned to me, and asked whether I really believed that the moon exists only when I look at it."[2]

● Big Ideas

1. A particle in a quantum superposition exists as different states at the same time.

2. Measurement destroys the superposition because only one state is seen with some probability.

1.3   Check Your Understanding

1. ● Discuss whether the following quantities are quantized or continuous:

   (a) electric charge
   (b) time
   (c) length
   (d) cash

---

[2]Nielsen, M. A. 1., & Chuang, I. L. (2000). *Quantum computation and quantum information*. New York: Cambridge University Press, p. 212.

(e) paint color

2. ● An ink is created by mixing together 50% red ink and 50% yellow ink. An artist uses it to stamp a picture of a sun. If the ink behaves like a quantum system in a half-yellow, half-red quantum superposition, what could the resulting picture look like? Some options are shown in Figure 1.5.

3. ● If this controversial picture of a dress[3] is always seen as blue/black by Student A and always seen as white/gold by Student B, is the dress in a quantum superposition?
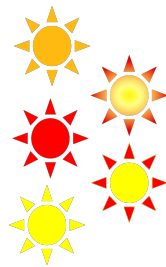
Figure 1.5: Image of the painted suns.

---

[3]https://en.wikipedia.org/wiki/The_dress

Answers

1. (a) quantized to the charge of the electron: $e = 1.6 \times 10^{-19}$ C.

   (b) time is continuous

   (c) space is continuous

   (d) quantized to $0.01

   (e) continuous because the frequency of light (which causes color) is continuous

2. It would either look all yellow or all red.

3. No. If we showed 100 copies of the picture to Student A, they would always see blue/black. In a 50/50 quantum superposition, they would see around 50 pictures as blue/black and the rest as white/gold. The two states must be an intrinsic property of the dress rather than something that depends on the observer.

Chapter 2

What is a Qubit?

In classical computers, information is represented as the binary digits 0 or 1. These are called bits. For example, the number 1 in an 8-bit binary representation is written as 00000001. The number 2 is represented as 00000010. We place extra zeros in front to write every number with 8-bits total, which is called one byte. In fact, every classical computer translates these bits into the human readable information on your laptop or phone. The word document you read or video you watch is encoded in the computer binary language in terms of these 1's and 0's. Computer hardware understands the 1-bit as an electrical current going through a wire (in a transistor) while the 0-bit is the absence of an electrical current in a wire. These electrical signals can be thought of as "on" (the 1-bit) or "off" (the 0-bit). Your computer then decodes the classical 1 or 0 bits into words or videos, etc.

Quantum bits, called **qubits**, are similar to bits in that there are two measurable states called the 0 and 1 states. However, unlike classical bits, qubits can also be in a superposition state of these 0 and 1 states, as shown in Figure 2.1. Certain computations that would normally need to be performed on 0 or 1 separately on a classical computer could now be completed in a single operation using a qubit on a quantum computer. Intuitively, this could make computations much faster. It is important to understand that although a single qubit is in a superposition of two classical bits, when a qubit is measured, the qubit actually only results in one classical bit of information: either 0 or 1.
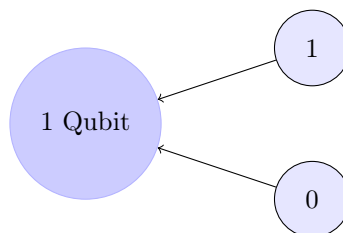

Figure 2.1: A classical bit can be either 0 or 1. A qubit can be in a superposition of both 0 and 1.

2.1 ● Mathematical Representation of Qubits

Dirac bra-ket notation

In order to work with qubits, it is useful to know how one can express quantum mechanical states with mathematical formulas. Dirac or "bra-ket" notation is commonly used in quantum mechanics and quantum computing. The state of a qubit is enclosed in the right half of an angled bracket, called the **"ket"**. A qubit, $|\Psi\rangle$, could be in a $|0\rangle$ or $|1\rangle$ state which is a superposition of both $|0\rangle$ and $|1\rangle$. This is written as

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

with α and β called the amplitudes of the states. Amplitudes are generally complex numbers (a special type of number used in mathematics and physics). However, to understand the meaning of amplitudes, we can just imagine the amplitudes as being ordinary (real) numbers. Amplitudes allow us to mathematically represent all of the possible superpositions.

Figure 2.2: The state of Schrödinger's cat expressed in bra-ket notation.

Amplitudes are very important because they tell us the probability of finding the particle in that specific state when performing a measurement. The probability of measuring the particle in state $|0\rangle$ is $|\alpha|^2$, and the probability of measuring the particle in state $|1\rangle$ is $|\beta|^2$. Why is it squared? The short answer is that it gives the correct experimental predictions for this choice of representation.[1] Squaring α and β to find the probability is similar to squaring a waves amplitude to find the energy in the wave. Since the total probability of onserving all the states of the quantum system must add up to 100%, the amplitudes must follow this rule:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

This is called a **normalization** rule. The coefficients α and β can always be rescaled by some factor to normalize the quantum state.

Examples

1. The quantum state of a spinning coin can be written as a superposition of heads and tails. Using heads as $|1\rangle$ and tails as $|0\rangle$, the quantum state of the

---

[1]We know that quantum physics is probabilistic from experiments. The squared coefficients are needed to make a quantity that behaves like a probability distribution, i.e., it is a real number and positive. There cannot be a negative probability by definition.

coin is

$$|\text{coin}\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right). \tag{2.3}$$

What is the probability of getting heads?

The amplitude of $|1\rangle$ is $\beta = 1/\sqrt{2}$, so $|\beta|^2 = \left(1/\sqrt{2}\right)^2 = 1/2$. So the probability is 0.5, or 50%.

2. A weighted coin has twice the probability of landing on heads vs. tails. What is the state of the coin in "ket" notation?

$$P_{\text{heads}} + P_{\text{tails}} = 1 \quad \text{(Normalization Condition)}$$
$$P_{\text{heads}} = 2P_{\text{tails}} \quad \text{(Statement in Example)}$$
$$\rightarrow P_{\text{tails}} = \frac{1}{3} = \alpha^2$$
$$\rightarrow P_{\text{heads}} = \frac{2}{3} = \beta^2 \tag{2.4}$$
$$\rightarrow \alpha = \sqrt{\frac{1}{3}}, \ \beta = \sqrt{\frac{2}{3}}$$
$$\rightarrow |\text{coin}\rangle = \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle.$$

One common misconception is that the measurement result will be a weighted average of the $|0\rangle$ and $|1\rangle$ states. It is important to note that after you perform the measurement, the particle is no longer in a superposition but takes on a definite state of either $|0\rangle$ or $|1\rangle$.[2] You would not be able to find α or β unless you created many particles in the same quantum state and then measured how many collapse into $|0\rangle$ (giving α) and how many collapse into $|1\rangle$ (giving β). You need multiple identical particles to count how many collapse into $|0\rangle$ or $|1\rangle$.

● Big Ideas

1. A particle is in superposition state until you look at it. When you measure the state of a particle, it collapses into one of the observable states.

---

[2]When formulating the mathematical representation of quantum mechanics, this is one of four fundamental assumptions that need to be made. The reason for the collapse is still unknown: https://en.wikipedia.org/wiki/Wave_function_collapse.

2.2 ◆ Matrix Representation

When writing one qubit in a superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, it is useful to use matrix algebra. In matrix representation, a qubit is written as a two-dimensional vector where the amplitudes are the components of the vector:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2.5}$$

The states $|0\rangle$ and $|1\rangle$ are usually represented as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.6}$$

A qubit's state can be changed by some physical action such as applying an electromagnetic laser or passing it through an optical device. Mathematically, changing a qubit's state is represented by multiplying the qubit vector $|\psi\rangle$ by some **unitary matrix** U so that after the change the state is now $|\psi'\rangle = U|\psi\rangle$. Unitary is a mathematical term which expresses that U can only act on the qubit in such a way that $|\alpha|^2 + |\beta|^2$ does not change. A matrix U is unitary if the matrix product of U and its conjugate transpose $U^\dagger$ (called U-dagger) produces the identity matrix: $UU^\dagger = U^\dagger U = \mathbb{1}$. This is very important because, in all mathematical constructions of quantum mechanics, one fundamental assumption is that each (matrix) operator must be unitary. This ensures that after changing the state by doing something to it (applying an operator) that the total probability of measuring everything still adds up to 100%. If this did not happen, then we could not interpret the results of quantum mechanics to be probabilities, and the results would disagree with the many experiments we have performed.

Examples

1. What is the conjugate transpose of the following matrix?

$$A = \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix}. \tag{2.7}$$

   The conjugate transpose of a matrix is found by two steps. The first step is to "conjugate" all of the complex numbers. The conjugate of a complex number is found by switching the sign of the imaginary part. The complex conjugate of 1 is just 1, while the complex conjugate of $+i$ is $-i$. The second step is to transpose the conjugated matrix. Transposing a matrix switches rows with columns, i.e., the first row turns into the first column, second row turns into

the second column, etc. Therefore,

$$A^\dagger = \begin{pmatrix} 1 & 1 \\ -i & -i \end{pmatrix}. \tag{2.8}$$

2. Is the above matrix A unitary?

$$AA^\dagger = \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -i & -i \end{pmatrix} \tag{2.9}$$

$$= 2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.10}$$

Multiplying A by its conjugate transpose does not produce the identity matrix, so A is not unitary.

3. What is the result of applying the unitary operator X onto a $|0\rangle$ state qubit?

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{2.11}$$

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle. \tag{2.12}$$

The X matrix changes the $|0\rangle$ qubit state to the $|1\rangle$ qubit state.

2.3 ◆ Bloch Sphere

It is sometimes convenient to visually represent a qubit using a Bloch sphere. The Bloch sphere is an abstract representation with similar geometric properties to the unit circle from trigonometry. However, it only works for a single qubit and cannot be used for two or more qubits. Therefore, we will not go over the Bloch sphere, but you can read further on the IBM Q website.[3]

Physical Realization of Qubits

In a classical computer, the 0- and 1-bit mathematically represent the two allowed voltages in a wire building a classical circuit. Semiconductor devices called transistors are used to control what happens to these voltages. A question frequently

---

[3]https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=introduction

posed by new students is "What is a qubit made out of?" As quantum computers are based on fundamentally different concepts, they must be built from completely different technology; e.g., it is not possible to have a classical current in a super-position of both flowing and not flowing through a wire. Quantum computers are still in their infancy, and so there are many different candidates for the technology to build them. Some technologies are based on optics, others use superconductors or possibly molecules. It is still unclear if any of these are more beneficial than the others, and it is even more unclear if all future quantum computers will be built from the same technology or if there will be many different types of quantum computers available (in the same way there exists both Xbox and Play station game consoles, but both do the same thing-interactive gaming). We will study two different experiments which illustrate the properties of the qubits, but the details of building a quantum computer are well beyond the scope of this introduction.

2.4   Check Your Understanding

1. ● If a coin is a classical bit of information (heads = 1 and tails = 0), how is the number 2 represented in standard 8-bit notation using coins? (Hint: Find the 8-bit representation of the number 2, then convert to H's and T's.)

2. ● Using the chart below, can you figure out what this binary message 01100011 01100001 01110100 says? (Note: This is actually how your computer and phone decode information from bits to text.)

Character	Binary Code	Character	Binary Code
A	01000001	N	01001110
B	01000010	O	01001111
C	01000011	P	01010000
D	01000100	Q	01010001
E	01000101	R	01010010
F	01000110	S	01010011
G	01000111	T	01010100
H	01001000	U	01010101
I	01001001	V	01010110
J	01001010	W	01010111
K	01001011	X	01011000
L	01001100	Y	01011001
M	01001101	Z	01011010

Table 2.1: Table for message.

3. Assume a flipped coin can be measured as either heads (H) or tails (T).

(a) ● If the coin is in a normalized state $\frac{1}{\sqrt{10}}|H\rangle + \frac{3}{\sqrt{10}}|T\rangle$, what is the probability that the coin will be tails?

(b) ■ During a flip, the coin is in a state $\frac{1}{3}|H\rangle + \frac{2}{3}|T\rangle$. Is this state normalized?

(c) ● A machine is built to flip coins and put them into a state $\frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|T\rangle$ when flipped. If 100 coins are flipped, how many coins should land on tails?

(d) ■ A coin starts in the state $\frac{1}{\sqrt{10}}|H\rangle + \frac{3}{\sqrt{10}}|T\rangle$. After a measurement is made on the coin, what could be the state of the coin?

4. ■ Multiple qubits are prepared in the same superposition state. By making measurements on these particles, can you write down their initial state?

5. ● A quantum particle is prepared in an unknown state. It is then measured with the outcome $|0\rangle$.

   (a) Which of the following could be its initial state before the measurement: $|0\rangle$, $\frac{1}{\sqrt{10}}|0\rangle + \frac{3}{\sqrt{10}}|1\rangle$, $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$?

   (b) If you tried to measure the same particle a second time, can you narrow down what the initial state was?

   (c) Another particle is prepared in the same unknown state. It is measured in the $|1\rangle$ state. What can you say about the initial state now?

6. ◆ What is the matrix product of the X matrix,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.13}$$

and $|0\rangle$ state qubit?

7. ◆ What is the matrix product of the above X matrix and the $|1\rangle$ state qubit?

8. ◆ What is the matrix product of the above X matrix and a qubit in the general state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$?

9. ◆ Find the conjugate transpose of the matrix

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{2.14}$$

10. ◆ Show that the matrix

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.15}$$

is unitary.

11. ◆ Show by example that applying a non-unitary matrix to a qubit results in probabilities that no longer add up to 100%. (Hint: Start with any initial state, e.g., $|0\rangle$. Measure the probabilities of finding either 0 or 1. Apply a non-unitary matrix to the initial state. Then measure the probabilities of finding either a 0 or 1. Do the probabilities add up to 100%?)

Answers

1. With the 8-bit representation, this would require eight coins arranged as TTTTTTHT.

2. The decoded message says "CAT"

3. (a) 9/10 or 90%. The probability is the square of the amplitude.

   (b) No, $1/9 + 4/9 \neq 1$. Normalization means the total probabilities add up to 1.

   (c) 75 coins.

   (d) Measurement collapses the superposition onto either $|H\rangle$ or $|T\rangle$.

4. Yes, by measuring how many of the qubits collapse to the $|0\rangle$ state and how many collapse to the $|1\rangle$ state, we can determine what the amplitudes are and therefore what the initial state of all the particles was.

5. (a) All of them are possible as they all can produce $|0\rangle$ after measurement.

   (b) After measurement the state in the question is in $|0\rangle$, since the superposition collapsed. Since it is in the $|0\rangle$ state after measurement, if you try to measure the same state again you will always measure $|0\rangle$. No new information is provided about the state after the collapse.

   (c) If $|0\rangle$ is measured from the unknown state, and a second identical state is prepared and is measured in the $|1\rangle$ state, then you know the unknown state contains some nonzero superposition of both $|0\rangle$ and $|1\rangle$, e.g., it is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha \neq 0$ and $\beta \neq 0$. So you can rule out $|\psi\rangle = |0\rangle$ as the initial state, but all of the other three states given in (a) are still possible. Measurements of many more particles are needed to determine the numerical values of α and β in order to find the exact state.

6.
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.16}$$

7.
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{2.17}$$

8.
$$|\Psi\rangle = \beta|0\rangle + \alpha|1\rangle. \tag{2.18}$$

9.

$$Y^\dagger = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{2.19}$$

10.

$$U^\dagger U = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}. \tag{2.20}$$

Chapter 3

Creating Superposition: The Beam Splitter

3.1 ● How is a superposition state created?

While a flipping coin is a simple model of a qubit, it is not very useful for building a quantum computer because it does not exhibit all of the properties of a true quantum superposition. For example, we cannot manipulate the superposition amplitudes. In this section, we will study some real physical examples of quantum particles in a superposition containing two states. These examples include a photon in a beam splitter, an electron in the double-slit experiment, and an electron in a Stern-Gerlach apparatus.

3.2 ● Beam Splitter

In classical optics, a **beam splitter** acts like a partially reflective mirror that splits a beam of light into two. In a 50/50 beam splitter, 50% of the light intensity is transmitted and 50% is reflected, as shown in Figure 3.1.
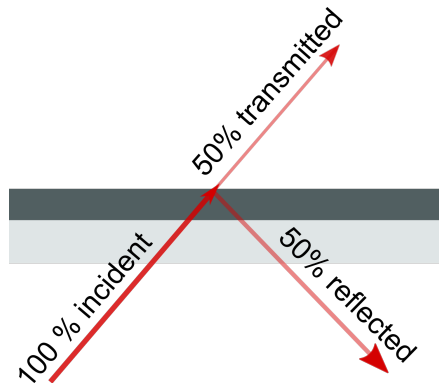

Figure 3.1: A beam splitter reflects 50% of the incident light and transmits 50% of the incident light.

One way to visualize the beam splitter is to imagine a barrier with holes randomly cut out like Swiss cheese, as shown in Figure 3.2. Imagine this barrier is placed in a pond, and a water wave moves toward the barrier. After the wave hits the barrier, we would observe a smaller wave going through the barrier and another would be reflected off the barrier.
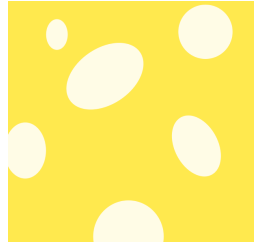

Figure 3.2: A beam splitter reflects 50% of the incident light and transmits 50% of the incident light.

Question 1: What would happen if a classical particle such as a soccer ball is randomly kicked at the barrier? Assume the ball can fit through the holes.

Experiments show that light behaves both like a wave (Young's double-slit experiment) and a particle (photoelectric effect, Compton effect). Classically, light is thought of as a wave consisting of continually oscillating electric and magnetic fields. However, light can also be thought of as a stream of particles called **photons**. Photons have no mass but carry the light's energy from one point to another at the speed of light. A laser beam is comprised of photons. If you turn down the intensity of your laser, you can even send one photon at a time, as shown in Figure 3.3. In practice, setting up a single photon source and detector requires specialized equipment, so we will instead run a simulator to see what happens.
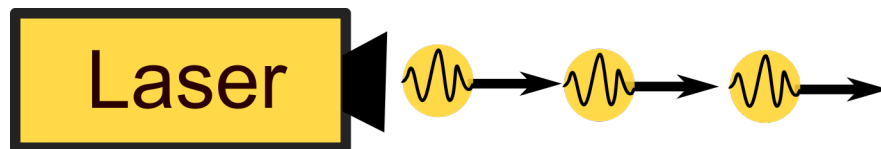

Figure 3.3: Low-intensity light is a stream of single photons.

Question 2: Open the beam splitter simulator[1], go to the Controls screen, and fire a single photon. The setup before the photon hits a beam splitter is shown in Figure 3.2. Which detectors are triggered when the photon passes through the 50/50 beam splitter?

1. Always detector 1

---

[1]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/Mach-Zehnder-Interferometer/Mach_Zehnder_Interferometer.html
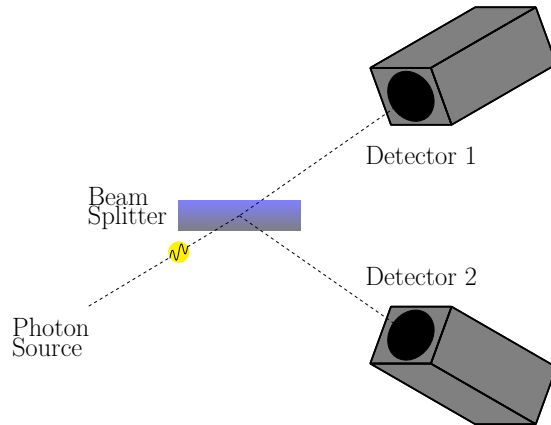
Figure 3.4: A single photon is sent at a beam splitter and the outcome measured with detectors to see whether it transmits or reflects.

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

5. Neither

Question 3: Which detector(s) would trigger if a classical **wave** is sent through the beam splitter?

1. Always detector 1

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

5. Neither

Question 4: Which detector(s) would trigger if a classical **particle** is sent through the beam splitter?

1. Always detector 1

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

5. Neither

Question 5: What does the photon do at the instance it encounters the 50/50 beam splitter?

1. Splits in half. Half the photon is transmitted and half is reflected

2. The whole photon goes through with 50% probability and reflects with 50% probability

3. The whole photon is both transmitted and reflected, essentially in two places at once

If the photon was split in half, both detectors would be triggered together. As only one detector goes off at a time, the photon could not have split up. In this case, we see that light behaves more like the soccer ball than the water wave.

At this point you may be thinking that the photon was either transmitted or reflected at the beam splitter, and we simply didn't have that information until it hit Detector 1 or 2. Unfortunately, this would be the incorrect interpretation formed by our classical lizard brain. This would be like saying the coin was Heads all along, and all we had to do was look at it to determine its state. Just like how a spinning coin will land on heads 50% of the time and tails 50% of the time, the single photon is in a superposition of both states all the way until the point when it reaches the detectors. This distinction might seem like a matter of semantics, but it will be important once the system becomes more complicated. The experimental setup after the photon hits a beam splitter is shown in Figure 3.5.
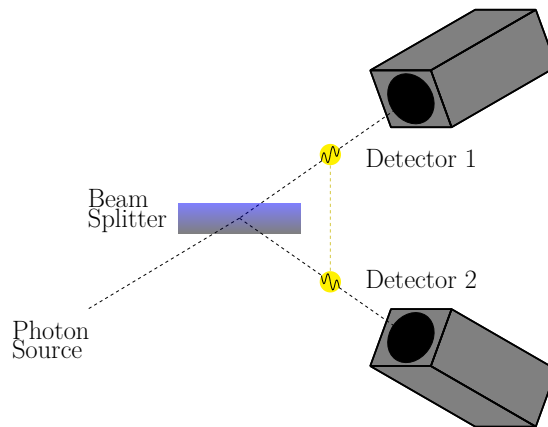

Figure 3.5: The beam splitter puts the photon into a superposition state.

If we let the transmitted path be $|0\rangle$ (detector 1), and the reflected path be $|1\rangle$ (detector 2), then the photon's state after the beam splitter is

$$|\text{photon}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \tag{3.1}$$

Upon measurement, will the superposition collapse into either 0 or 1? Unfortunately, there is no way to predict which detector will be activated at any given time. Quantum mechanics is inherently probabilistic.

The phenomenon of superposition allows quantum computers to perform operations on two bits of information at once with a single qubit. In fact, it is possible to create a general purpose (also called universal) quantum computer using photons as qubits, beam splitters to create superposition, and pieces of glass that slow down the photons along selected paths (phase shifters).[2]

3.3 ● Mach-Zehnder Interferometer

To convince ourselves that the photon really did take two paths at once, let's see what happens when a second beam splitter is added. In reality, this experimental setup is shown in Figure 3.6. The mirrors redirect the photons towards the second
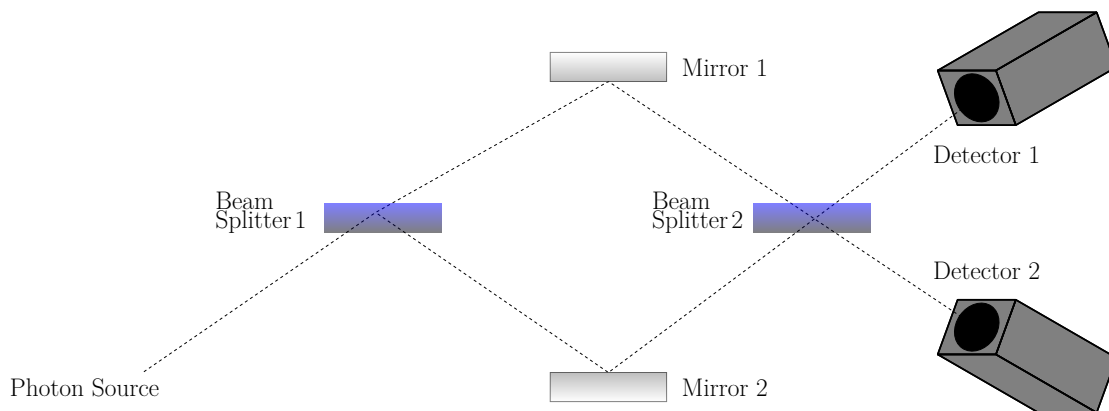

Figure 3.6: Schematic of the Mach-Zehnder interferometer from the beam splitter simulator.

beam splitter. This device configuration is known as a **Mach-Zehnder interferometer**. The set up is very sensitive to the distances between the mirrors and detectors, which essentially have to be the same or differ by an integer number of the photon's wavelength.

Question 6: If we assume that the photon was reflected by the first beam splitter, which detectors would be triggered?

1. Always detector 1

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

---

[2]Knill, E.; Laflamme, R.; Milburn, G. J. (2001). "A scheme for efficient quantum computation with linear optics". Nature. Nature Publishing Group. 409 (6816): 46–52.

5. Neither

Question 7: If we assume that the photon was transmitted by the first beam splitter, which detectors would be triggered?

1. Always detector 1

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

5. Neither.

Question 8: Construct the Mach-Zehnder interferometer in the beam splitter simulator[3] and fire a single photon. Which detectors are triggered?

1. Always detector 1

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

5. Neither

If the photon was either transmitted or reflected by the first beam splitter, it would have a 50/50 chance of transmission or reflection by the second beam splitter. Thus, both detectors should trigger with equal probability. The experimental results do not agree with this hypothesis, as only one detector is triggered with 100% probability. The results are more intuitively understood from the wave perspective of light.

To understand the operation of the interferometer, it is important to note that the beam splitters have a polarity. The beam splitter consists of a piece of glass coated with a dielectric on one side. When light enters the beam splitter from the dielectric side, the reflected light is **phase shifted** by π. Light entering from the glass side will not experience any phase shift. The phase shift only occurs when the light travels from a low to high index of refraction ($n_{air} < n_{dielectric} < n_{glass}$).

What does it mean for a photon to be phase shifted? In this case, it is more intuitive to think about the wave nature of light. The phase shift would invert the electric and magnetic field oscillations relative to the incoming wave. If a π-shifted wave overlaps with the original wave, destructive interference occurs. This is shown in Figure 3.7.

---

[3]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/Mach-Zehnder-Interferometer/Mach_Zehnder_Interferometer.html
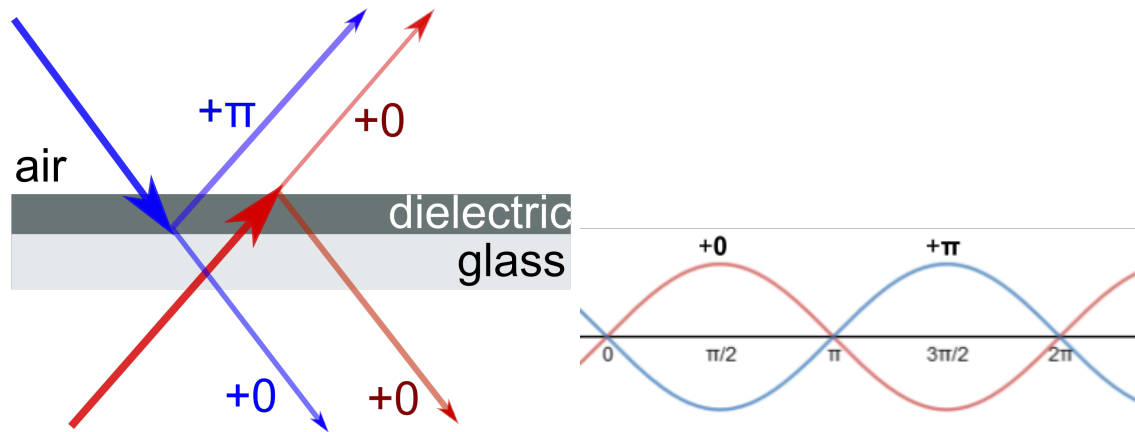
Figure 3.7: The light through a beam splitter is phase shifted if it is reflected from the dielectric side but not phase shifted from if it is reflected from the glass side.

Question 9: If we assume that light is a classical wave exhibiting interference, can you work out which detectors would be triggered? Note that the first beam splitter has the dielectric side on top, while the second has the dielectric on the bottom, as shown in Figure 3.6.

1. Always detector 1

2. Always detector 2

3. Detector 1 OR detector 2

4. Both detector 1 AND detector 2

5. Neither

Particle Explanation

The behavior of the interferometer can also be viewed from the particle perspective, though it may be less intuitive. Recall from the single beam splitter experiment that the photon did not split up or clone itself. It was in a superposition state, essentially taking both paths. The second beam splitter treats the photon as if it came in from both top and bottom simultaneously. The bottom photon is phase shifted relative to the top photon, resulting in destructive interference at Detector 2. Since there is no phase shift at Detector 1, there is no cancellation and it triggers with 100% probability, as shown in Figure 3.8.

Question 10: If the photon is sent into the Mach-Zehnder interferometer from the upper left instead of the bottom left, which detector(s) would be triggered and with what probability?
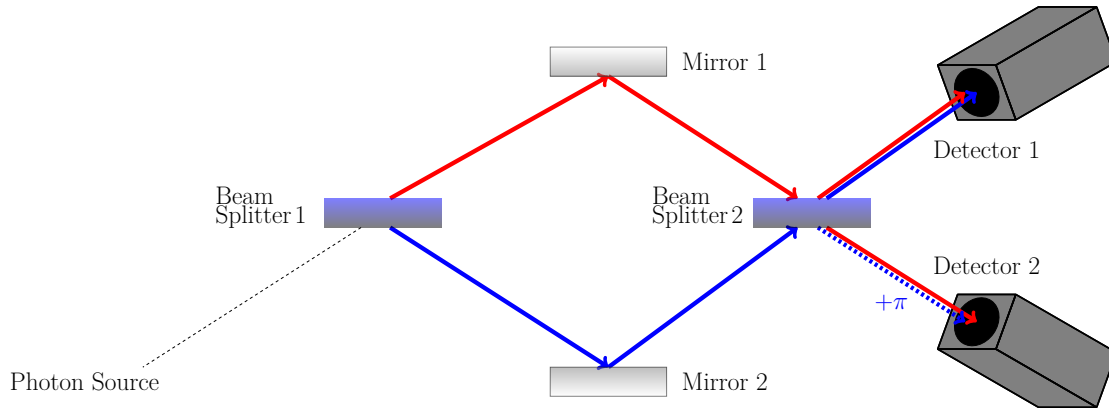
Figure 3.8: The blue path shows the photon's path if it is reflected by the first beam splitter. The red path shows the path if the photon is transmitted. Red and blue interfere constructively at Detector 1 while destructively at Detector 2.

Even though the output of the first beam splitter is 50/50, the second beam splitter can distinguish whether the laser was fired from the top of the bottom. The first beam splitter creates a superposition state, but adding a second one undoes the superposition and recovers the original state. This is a non-classical operation. It would be like starting with the coin heads up, flipping it, flipping it again while it is still in the air, and then always getting heads when it lands! This is highlighted in Figure 3.9.
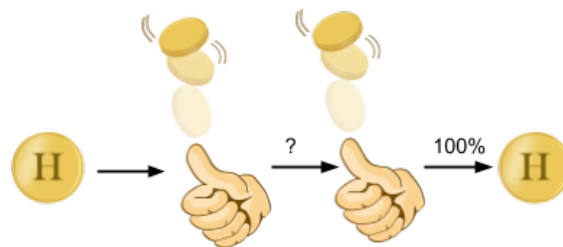

Figure 3.9: Coin analogy for the interferometer. Sending a photon through one beam splitter puts it in superposition, but adding a second beam splitter undoes the superposition and recovers the original state.

There is hidden information in the superposition state. In the Mach-Zehnder photon qubit, the information is encoded in the form of the phase shift. In the experiment shown in Figure 3.8, we choose the phase shift to have a value of π. However, we could have just as easily chosen the phase shift to have any value between 0 and 2π (the angles of a circle). Each separate choice of phase shift would produce a different type of superposition state that would still produce the same measurable 50/50 outcome.[4] This phase shift information is present in the

---

[4]A complex amplitude $e^{i\phi}$ with infinite possible phase angles ϕ does not affect the probability since $|e^{i\phi}|^2 = 1$.

amplitudes but not the square of the amplitudes (and hence hidden from us in the Mach-Zehnder experiment-though we could make an other experiment to try to determine this information). Here are two simple examples of distinct states that can be created in the Mach-Zehnder experiment which still have the same 50/50 probability:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{or} \quad \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \tag{3.2}$$

In these two states the minus sign represents the phase shift, which is what allows certain states to cancel out when adding them together. As you can see, quantum superposition is inextricably linked to wave-particle duality.

Furthermore, in the Mach-Zehnder experiment we created a superposition, performed a phase shift and then observed wave interference. These experimental operations are equivalent to mathematically applying (matrix/gate) operations on a qubit, as we shall see later. As such, the Mach-Zehnder is an example of how we can technologically implement qubits (the photon) and operations (superposition/phase shift, etc) to build a quantum computer.[5] In quantum computing, people talk about the superposition of states rather than the wave behavior. Yet, as we have seen, both frameworks lead to the same understanding of the Mach-Zehnder interferometer. Later we will use the interferometer to implement a quantum algorithm.

3.4 Check Your Understanding

1. ● Your friend who is explaining superposition to you says that:

   "A particle in the state $(1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$ represents a lack of knowledge of the system. Over time, the particle is changing back and forth between the state $|0\rangle$ and $|1\rangle$. The superposition state says that overall, the particle is in each of the two states for half of the time."

   What parts of this statement do you agree with and what do you not agree with?

2. ■ Only one detector is triggered if a single photon is sent through the beam splitter experiment shown in Figure 3.6. If the laser outputs two photons at the same time, what is the probability that both detectors will be triggered simultaneously? Now how about three photons? Ten photons? Note that this is why a higher power beam of light appears to reach both detectors simultaneously.

3. ◆ In practice, it is difficult to put the detectors the exact same distance from the beam splitter. The difference in distance is measured using the time delay

---

[5]It should be noted that the technology has progressed so that most qubits are at present implemented using superconducting transmons and not using a Mach-Zehnder.

δt between photons. The experiment is shown in Figure 3.10 and the data in Figure 3.11.
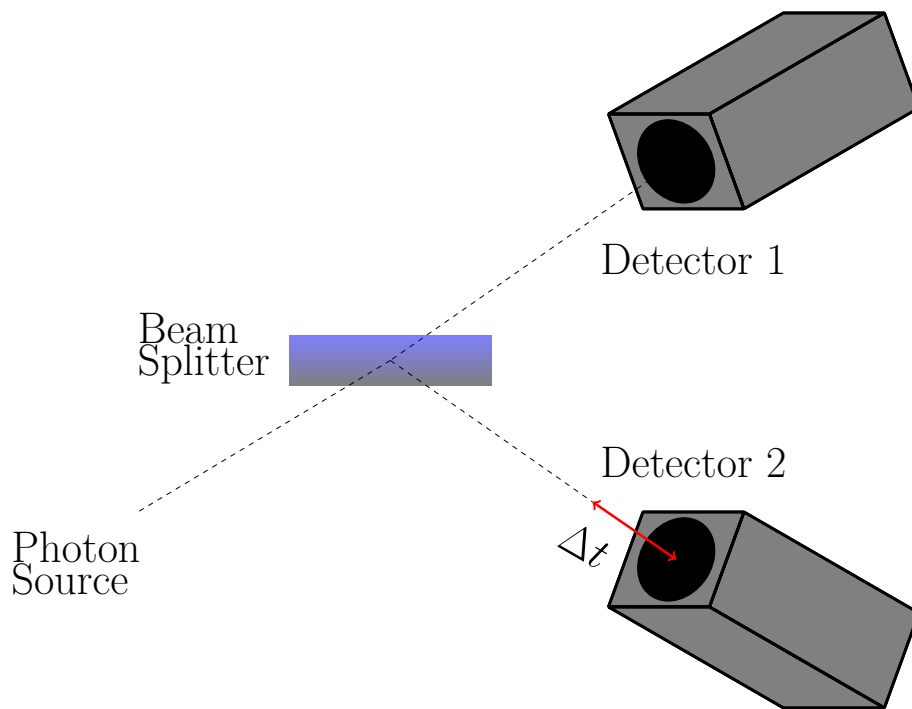

Figure 3.10: The experiment varies the position of Detector 2 and records the number of coincidences, i.e., the number of times both detectors are triggered simultaneously.

3.a. Does the data shown in Figure 3.11 at $\delta t = 0$ support that light is a particle or a wave?

3.b. Why are there large coincidence counts when $\delta t \neq 0$? (Hint: Look at the spacing between the peaks.)

4. ◆ Using matrices given in Figure 3.12, show how the superposition state is created by applying the beam splitter matrix transformation to the initial photon vector state.

5. ◆ Construct the matrix representation for a 30/70 beam splitter.

6. ■ Unsettled by the Mach-Zehnder interferometer, you decide to determine once and for all which path the photon takes after the first beam splitter. You place another detector (indicated by the eyeball) on the upper path as shown in Figure 3.13. If the eyeball sees a photon, what would be seen at Detectors 1 and 2?
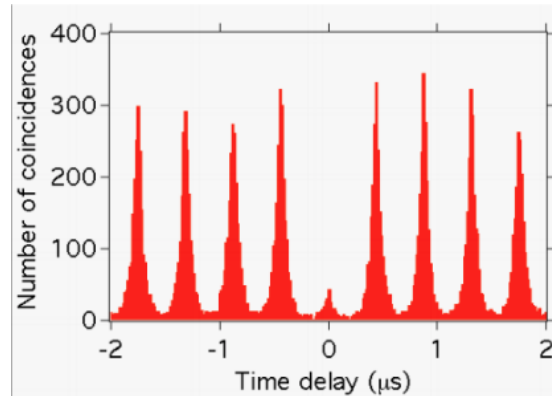
Figure 3.11: Data is shown below for light bursts sent from the laser every $0.4\mu s$. Figure reproduced with permission of Martin Laforest and the Communications and Strategic Initiatives Team at the Institute for Quantum Computing, University of Waterloo Outreach department.

Answers

1. All parts of the statement are false. The particle is in both states the entire time before measurement and has a 50% chance of being measured as 0 or 1.

2. A single photon can either be in a 0 or 1 state. So the possible states that can make up a superposition of two photons, labeled photon A and photon B (and hence the different states that can be measured), are $|0_A 0_B\rangle$, $|1_A 0_B\rangle$, $|0_A 1_B\rangle$, and $|1_A 1_B\rangle$. Both detectors are activated at the same time when we have one of the two photons in the 0 detector and one in 1 detector. This is either the $0_A 1_B$ state or the $1_A 0_B$ state. There are four total possible states, and two of them trigger both detectors so the probability is $2/4 = 50\%$. When there are three photons, the possible states are 000, 010, 011, 101, 110, 001, 100 and 111. Both detectors are activated for any state that has both a 0 and a 1. So both detectors will not be triggered by only the 000 and 111 states. Since there are six states that trigger both detectors, and eight states total, the probability of both detectors being triggered is $6/8 = 75\%$. Ten photons have 2^{10} possible outcomes, where only two outcomes do not trigger both detectors (one state is all zeros, and the other is all ones). So the probability is $(2^{10} - 2)/(2^{10}) = 99.8\%$.

3. 3.a. The coincidence counts are low when the detectors are an equal distance from the beam splitter. This points to light behaving like a particle entering only one detector at a time.

   3.b. Photons from different $0.4\mu s$ bursts can arrive at the detectors simultaneously.
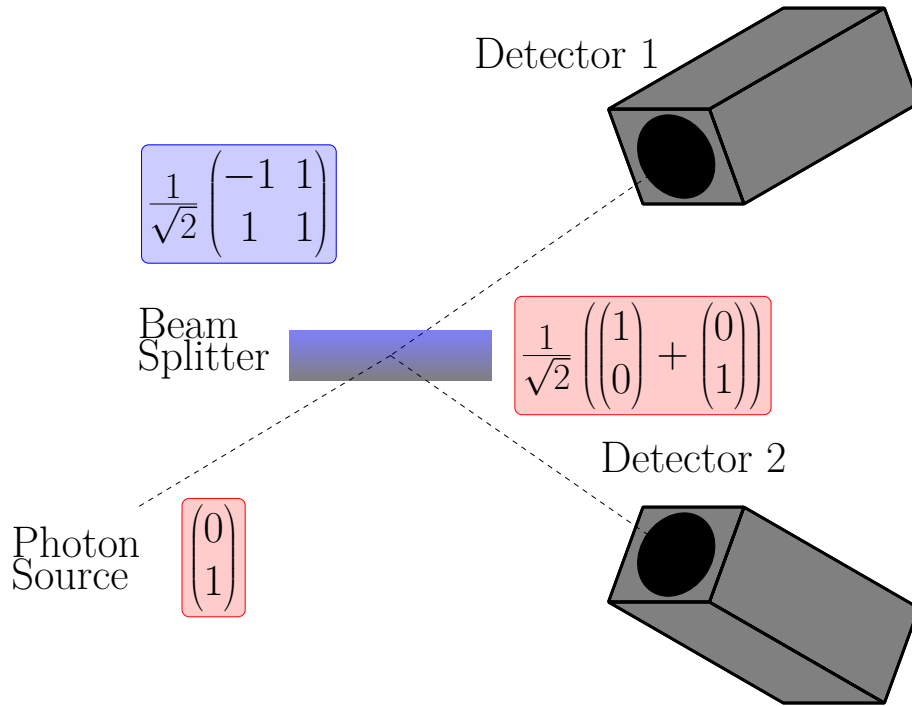
Figure 3.12: Matrix formulation of the Mach-Zehnder apparatus.

4.

$$\frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{3.3}$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{3.4}$$

5. A 30/70 superposition state would take the form:

$$\sqrt{\frac{3}{10}}|0\rangle + \sqrt{\frac{7}{10}}|1\rangle. \tag{3.5}$$

The desired beam splitter matrix M should perform the operation:

$$M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{3}{10}} \\ \sqrt{\frac{7}{10}} \end{pmatrix} \implies M = \begin{pmatrix} 1 & \sqrt{\frac{3}{10}} \\ 1 & \sqrt{\frac{7}{10}} \end{pmatrix} \tag{3.6}$$

would give the correct probabilities, but it is not unitary. And all quantum matrices must be unitary. Using the Hadamard matrix as a reference, the
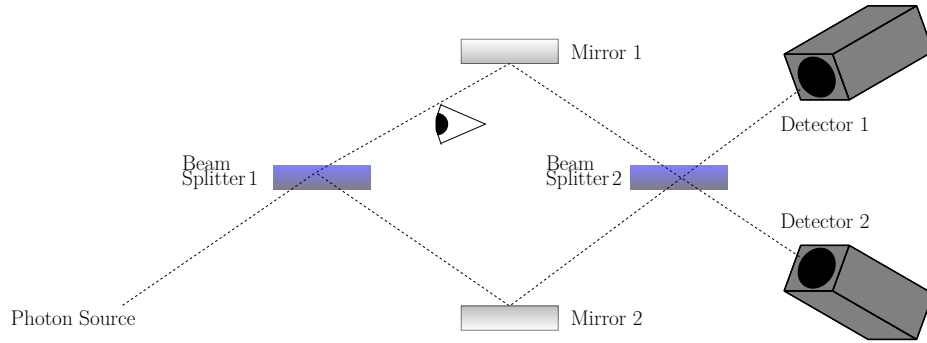
Figure 3.13: A third detector (your eye) is added to the Mach-Zehnder apparatus.

unitary 30/70 beam splitter matrix is

$$M = \begin{pmatrix} \sqrt{\frac{7}{10}} & \sqrt{\frac{3}{10}} \\ -\sqrt{\frac{3}{10}} & \sqrt{\frac{7}{10}} \end{pmatrix}. \tag{3.7}$$

6. Congratulations you have figured out the path of the photon! However, by seeing the location of the photon after the first beam splitter, you have collapsed its superposition state. Therefore, it goes into the second beam splitter from the top, where it exits in a superposition state with 50% probability of triggering Detector 1 or 2.

Chapter 4

Creating Superposition: Stern-Gerlach

4.1 ● Stern-Gerlach Apparatus

Besides the photon in the interferometer, an electron is another prototype for a qubit. An electron has many measurable properties such as energy, mass, momentum, etc. Yet, for the purposes of creating a qubit, we want to focus on a property with only two measurable values. An electron has a two-state property called **spin**.

Classically, an electron's spin can be visualized as a rotation about its own axis, like a spinning top or fidget spinner. You learned in high school physics that a moving charge creates a magnetic field according to the right-hand rule. By curling the fingers of your right hand in the direction of the electron's rotation, your thumb points in the direction of the magnetic field created by the charge. The spinning electron behaves somewhat like a tiny bar magnet.[1]

Surprisingly, the **Stern-Gerlach experiment** (SGA) showed that the electron spin is quantized into only two values. This video[2] explains the experimental apparatus used to measure the electron's spin. The key point here is that the vertically oriented apparatus (called the *z*-direction by convention) only measures the spin as either up or down, not randomly oriented at an angle. Since the spin of an electron has two measurable states, it can represent a qubit with $|0\rangle$ as spin up and $|1\rangle$ as spin down.
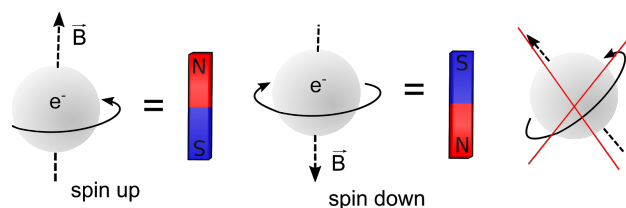

Figure 4.1: An electron can spin either up or down and produce a magnetic field.

---

[1]This classical picture is just an analogy. In reality, the quantum mechanical property we call "spin" is intrinsic to the electron (like its mass or charge) and can be described mathematically just like orbital momentum, but it is not when the electron physically rotates. See https://en.wikipedia.org/wiki/Spin_(physics).

[2]https://www.youtube.com/watch?v=rg4Fnag4V-E

Question 1: Open up the PhET Stern-Gerlach simulator[3] and try sending electrons of various initial spins into the Stern-Gerlach apparatus (SGA).
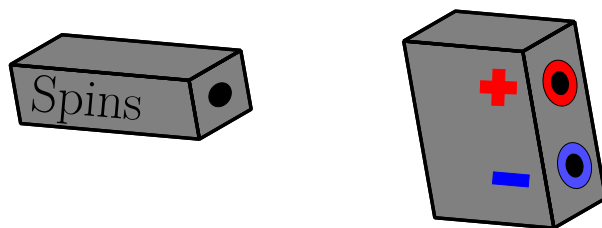

Figure 4.2: Electron spin produces a magnetic field either in the up or down direction.

Are the results what you would expect? The "up" and "down" directions are defined by the orientation of the apparatus. There is nothing inherently special about the z-direction compared to the x- or y-direction. An SGA rotated horizontally would measure either spin left or spin right. An SGA rotated by $45°$ would measure the spin to be either diagonally up or diagonally down. What is particularly interesting is if we send a single spin up electron into a horizontally oriented SGA.

Question 2: Where would you expect a spin up electron to land after passing through a horizontal SGA?
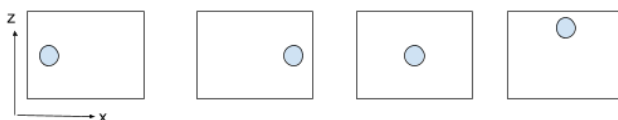

Figure 4.3: Possible positions.

Classically, vertically oriented bar magnets in a horizontal magnetic field would land at the center of the screen. However, recall that the spin can only be measured as left or right and cannot possibly land in the center. The way quantum mechanics solves this problem is to have the electron land either on the left or the right with 50% probability. Sound familiar? Sending a spin up electron through a horizontal SGA puts the electron in a superposition state of left and right.

Spin in the vertical direction can be represented as a superposition of spins in the horizontal direction. As shown in the simulation, an electron with vertical spin

---

[3]https://phet.colorado.edu/sims/stern-gerlach/stern-gerlach_en.html

has a 50% chance of being measured as right or left:

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\leftarrow\rangle, \tag{4.1}$$

$$|\downarrow\rangle = \frac{1}{\sqrt{2}}|\leftarrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle. \tag{4.2}$$

In more traditional qubit notation, spin in the $+z$ and $-z$ axis is written as $|0\rangle$ and $|1\rangle$, while spin in the $+x$ and $-x$ axis is $|+\rangle$ and $|-\rangle$:

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle, \tag{4.3}$$

$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle. \tag{4.4}$$

This is non-classical because you can't add or subtract horizontal magnetic field vectors to get a vertical magnetic field vector. One analogy might be to think about a person looking at a coin vertically to determine its state. If they see heads or tails, someone looking from the side would see a superposition. If they are forced to make a choice via measurement, they would say heads or tails with 50% probability.
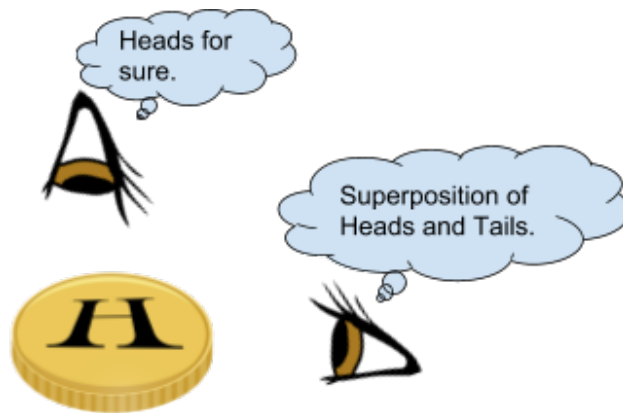

Figure 4.4: Analogy for how a definite vertical spin is seen as a superposition in the horizontal direction.

Example: Write the $|+\rangle$ state in terms of $|0\rangle$ and $|1\rangle$.

Solution: Adding Equations 4.3 and 4.4 we find

$$|0\rangle + |1\rangle = \frac{2}{\sqrt{2}}|+\rangle. \tag{4.5}$$

Rearranging, we get

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \qquad (4.6)$$

Similarly, by subtracting Equations (4.3) and (4.4), we find

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \qquad (4.7)$$

These equations show that a horizontal spin is a superposition of spin up and spin down.

As we saw in the beam splitter example, the minus sign encodes information about the original state of the particle before it is put in superposition. It is possible to choose other complex amplitudes that give the same probability, but the details are mathematically beyond our scope. The conclusion we reached is that spins in one direction can be written as a superposition of spins in another direction. The Stern-Gerlach experiment shows that qubits in superposition are an accurate description of how nature actually works. Therefore, one promising application of quantum computers is simulating natural systems such as atomic bonding.

4.2 ● Measurement Basis

The "*z*-basis" is composed of $|0\rangle$ and $|1\rangle$ while $|+\rangle$ and $|-\rangle$ compose the "*x*-basis." A basis is analogous to a coordinate system for quantum states. Any state can be written in terms of a different choice of basis, similarly to how any vector can be broken down into components along a different choice of axes.

In the figure below, a box on a ramp is subject to a force. The vector decomposition of $\vec{F}$ is shown for three different coordinate systems. All three coordinate systems are valid for describing the force, but only the first two are convenient to use in physics class. By choosing *x-y* to be perpendicular, you have made the components mutually exclusive: if a vector is horizontal, you know it's definitely not vertical. The *x*- and *y*- directions can be treated as two independent problems. A more mathematical way of saying the axes are independent is to say they are orthogonal.

In quantum mechanics, there are an infinite number of possible choices for a basis. However, the basis should have two properties:

1. The basis must describe all possible quantum states for the system.
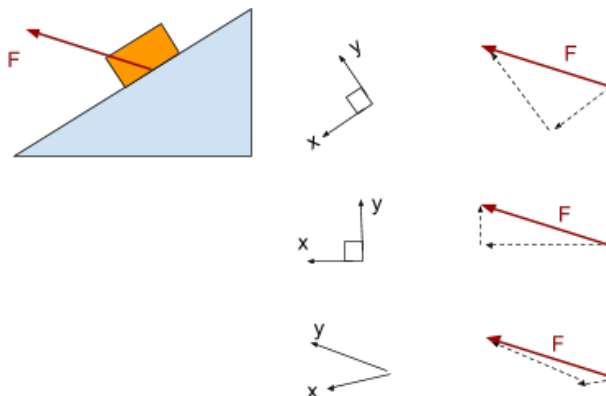
2. The basis must be orthogonal.

Figure 4.5: Rewriting quantum states in terms of a different basis is similar to decomposing a classical vector into a different choice of coordinate system.

Let us check these conditions for the z-basis, which consists of states $|0\rangle$ and $|1\rangle$:

1. Because the Stern-Gerlach experiment shows that an electron is either spin up or spin down, the most general state of the electron would be a superposition of up and down:

$$|\text{electron}\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{4.8}$$

   A linear combination of $|0\rangle$ and $|1\rangle$ completely describes the electron's state.

2. If you measure the spin as $|0\rangle$, it is definitely not $|1\rangle$, so $|0\rangle$ and $|1\rangle$ are orthogonal.

The same argument can be made for the x-basis or any other angle of the SGA.

4.3 ▪ Geometric Representation of a Basis

In this geometric representation of the z-basis and x-basis, the orthogonal states are drawn perpendicular to one another. If the electron is in a particular state $|0\rangle$ in the z-basis, the state vector can be decomposed into $1/\sqrt{2}|+\rangle + 1/\sqrt{2}|-\rangle$ in the x-basis. Physically turning the SGA from vertical to horizontal is how one changes from measuring in the z to x-basis. Since $|0\rangle = 1/\sqrt{2}|-\rangle + 1/\sqrt{2}|-\rangle$, the spin up particle became a 50/50 superposition when the measurement device became horizontal.

Question 3: Use Figure 4.6 and trigonometry to show that $|1\rangle = 1/\sqrt{2}|+\rangle - 1/\sqrt{2}|-\rangle$.

Often, there is hidden information about the state that cannot be measured unless we change to a different basis. In the x-basis, there is no measurable difference
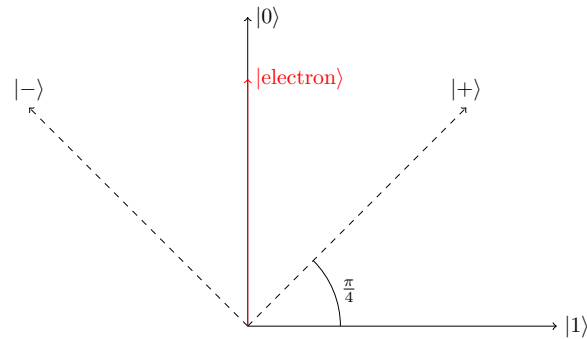
Figure 4.6: Geometric representation of the z-basis and x-basis. The state of a spin up electron is shown.

between $|0\rangle$ and $|1\rangle$. In the z-basis, $|0\rangle$ would have 100% probability of going up and 0% down, while $|1\rangle$ would have 0% probability of going up and 100% down.

4.4 ■ Effect of Measurement

You learned that measuring a qubit collapses its superposition state into one of two possibilities. A spinning coin is in a superposition state, but once it lands, it becomes either heads or tails. The photon is in a superposition state after passing through a beam splitter, but once it reaches the detectors, we know for sure whether it was reflected or transmitted. To see the truly strange nature of quantum measurement, let's see what happens when electrons are sent through multiple Stern-Gerlach devices in a row.

Question 4: Open the PhET Stern-Gerlach simulator[4] and send electrons with randomly oriented spins through a vertical SGA. What is the spin of the electrons that pass through the hole?

(a) $+z$

(b) $-z$

(c) Superposition of $+z$ and $-z$

Question 5: Add a second SGA, oriented horizontally. What is the spin of the electrons before entering the second SGA?
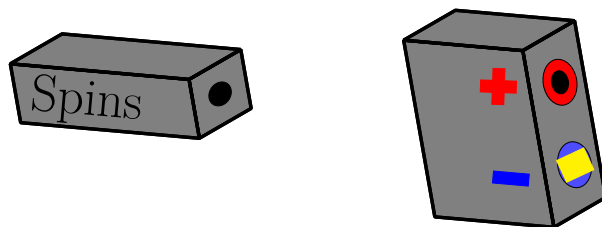
(a) $+x$

(b) $-x$

(c) Superposition of $+x$ and $-x$

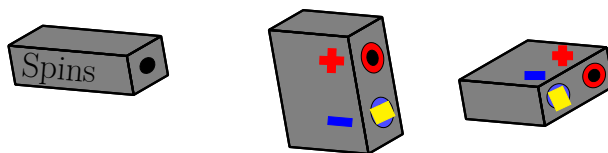Figure 4.7: The *z*-axis SGA lets through spin up electrons but blocks spin down electrons.

Figure 4.8: The *z* and *x*-axis SGA.

Question 6: What is the spin of the electrons after passing through the second SGA?

(a) $+x$

(b) $-x$

(c) Superposition of $+x$ and $-x$

Question 7: What is the *z*-spin of the electron coming out of the second SGA? Design an experiment to confirm this in the simulation.

(a) $+z$

(b) $-z$

(c) Superposition of $+z$ and $-z$

Given that only spin up electrons passed through the first SGA, one would expect that the electron is still spin up after the second SGA, no matter what is measured in *x*. However, if you measure the *z*-spin with a third SGA, it has a 50% chance of being up or down!

By looking at the electron, we fundamentally changed its state. Measuring the *x*-spin of the qubit puts it into a superposition of up and down, even when it started as up to begin with. When you measure the length of an object with a ruler, you don't expect the objects' length to change after you measure the width!

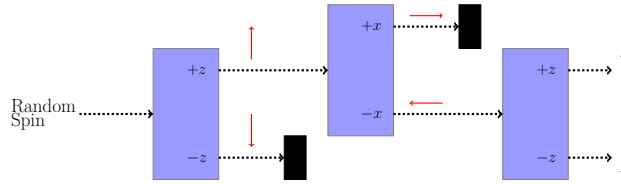[4]https://phet.colorado.edu/sims/stern-gerlach/stern-gerlach_en.html

Figure 4.9: The first SGA selects for $+z$ spin and the second SGA puts it in a superposition of $+x$ and $-x$. The third SGA shows that measuring the x puts the electron in a superposition of $+z$ and $-z$.

Quantum measurement collapse is used in many applications such as cryptography where one could detect if a message has been intercepted. Moreover, this property of quantum states implies a qubit in an unknown state cannot be copied. This property is known as the no-cloning theorem. Classical computers can make a copy of a text and the original stays the same. If you try to copy an unknown qubit you first have to measure it, which collapses its superposition state. Therefore, quantum computers are unlikely to replace your laptop. However, for certain applications, the hidden information in superposition states allows information processing beyond what is possible in a classical computer.

4.5   Check Your Understanding

1. ● The Stern-Gerlach apparatus is rotated by $90°$ so that the magnetic field is in the x-direction. If electrons from a random source are sent through the apparatus, what pattern would be formed on the screen?
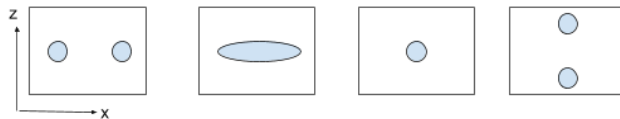
Figure 4.10: Stern Gerlach apparatus.

2. ▪ Would $|0\rangle$ and $|+\rangle$ together satisfy the criteria for a valid basis?

3. ▪ An electron is in a superposition state shown in the geometric representation below.

   (a) What is the state of the electron in the z-basis? i.e. find α and β in $|\text{electron}\rangle = \alpha|0\rangle + \beta|1\rangle$

   (b) What is the probability of measuring spin up?

   (c) What is the state of the electron in the z-basis? i.e, find α and β in $|\text{electron}\rangle = \alpha|+\rangle + \beta\alpha|+\rangle$.

Figure 4.11: Superposition state of the electron.

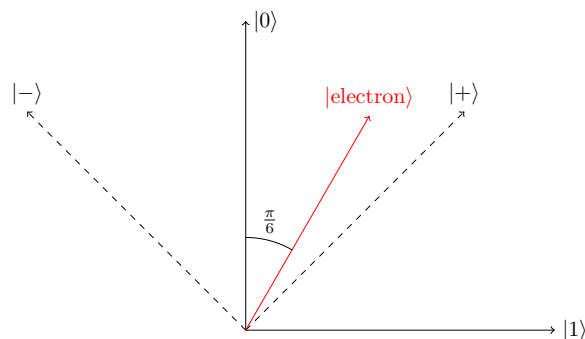(d) What is the probability of measuring the spin in the $\alpha|+\rangle$ direction?

4. ◆ To measure the difference between an electron in a spin state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and one in $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, one could use:

  I A horizontal SGA.

 II A vertical SGA.

III A 45° diagonal SGA.

(a) I only

(b) II only

(c) I or III

(d) II or III

(e) I, II, or III

5. ● An electron with random spin is sent through two vertical SGAs. What would be the output of the second SGA?
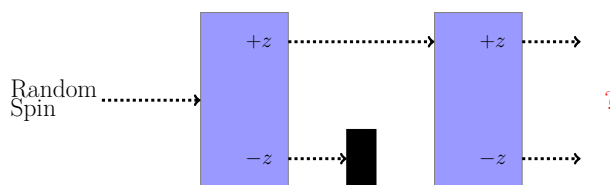
6. ● An electron with random spin is sent through two vertical SGAs, where the second SGA is rotated upside down, or 180°.

(a) If the second $+z$ port is blocked, what would be the output of the second SGA?
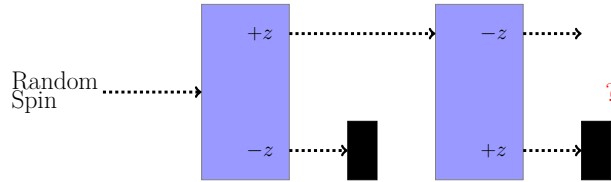
(b) If both ports on the second SGA are open, what would you see at the output?
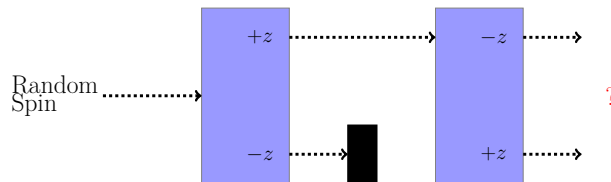
7. ● An electron with random spin is sent through a horizontal SGA followed by a vertical SGA. What would be the output of the second SGA?
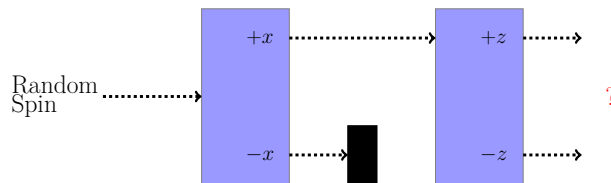
8. ● An electron with random spin is sent through three SGAs as shown. What would be the output of the third SGA?
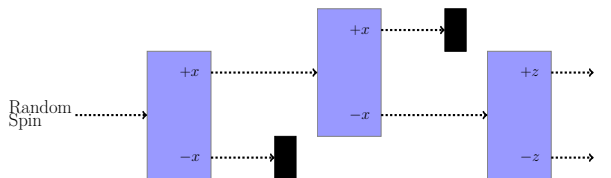
9. ● An electron with random spin is sent through four SGAs as shown. What would be the output of the fourth SGA?
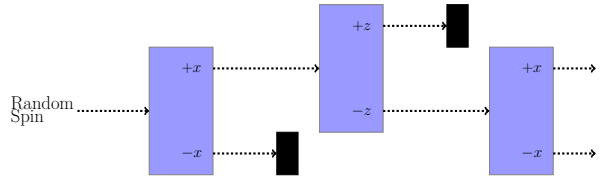
Answers

1.
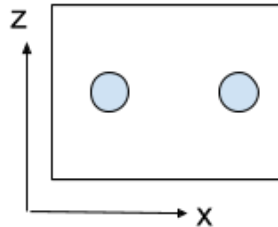
2. No. $|+\rangle = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$ are not independent of each other. $|0\rangle$ and $|+\rangle$ satisfy condition #1 but not condition #2.

   (a) $\cos(\pi/6)|0\rangle + \sin(\pi/6)|1\rangle$

   (b) $\alpha^2 = \cos^2(\pi/6) = 0.75$

   (c) $\cos(\pi/6 + \pi/4)|0\rangle + \cos(\pi/6 + \pi/4)|1\rangle$

   (d) $\cos^2(\pi/6 + \pi/4) \approx 0.067$

3. D. The two states are $|+\rangle$ and $|-\rangle$. The horizontal SGA would distinguish them with 100% certainty. They would also produce different probabilities in the diagonal SGA.

4. 100% $+z$

5. (a) Nothing comes out since the $+z$ entering the second SGA is blocked.

   (b) 100% $+z$.

6. 50% up, 50% down

7. Nothing: the second SGA blocks the electron.

8. 50% $+x$, 50% $-x$

9. The $-z$ selected by the 50% $+x$, 50% $-x$

Chapter 5

Quantum Cryptography

The Internet can be thought of as a channel of information being sent from you to everyone else connected to the Internet. If you wanted to transmit your sensitive information (such as bank account numbers, military secrets, etc.) over the Internet, then you have to ensure that only the persons you intend to read your information can read your sensitive data. Otherwise, everyone would be able to read your information, e.g., access to your bank account details and transfer money out of your account. Therefore, one needs to encrypt any data sent over the Internet. Encryption, in this context, ensures that only the intended sender and receiver can understand any message being sent over an Internet channel.

Encryption relies on the sender and receiver sharing a secret key (that no one else has) and using that to encrypt and decrypt messages. In this way, since no one else has the secret key, no one else can understand the shared information. Because no one else understands the shared information, they cannot misuse it for their own benefit. The fundamental caveat with encryption is this: you require a secure channel, to share the secret key (if you do not have a secure channel then someone random can just take the secret key and encryption would be pointless), but if you have a secure channel then why do you need to encrypt your data? You need a way around this issue. How do you share a secret key in an insecure channel, where anyone can be listening?

The way around this in the majority of online communications is called public key cryptography.[1] A person called Alice makes two keys such that each key knows that only the other key is related to it (think of the keys as siblings). They are called the private and public key. Alice then gives the public key to everyone in the world but importantly keeps the private key for herself. Anybody else, say Bob, who wants to send a private message to Alice has to encrypt their message with the public key that Alice generated. There are many different types of encryption protocols that one can use. The special part of public key cryptography is that *only* Alice's private key can decrypt the message that was encrypted using its sibling public key. In this way, only Alice can read the message from Bob. Since no one else has Alice's private key, no one else can read Bob's message. However,

---

[1]https://en.wikipedia.org/wiki/Public-key_cryptography

if Bob did not use Alice's public key but used a different public key to encrypt his message, then Alice cannot decrypt that message, as her private key is not a sibling key of the different public key. This whole cryptography scheme relies on the fact that no one can break the encryption protocol. If they could break it, then they could read Alice's message even if they did not have Alice's private key. Note, this is how your information is protected over the Internet.

The one-time pad, also known as the Vernam Cipher, is the only type of encryption protocol known to be perfectly secure.[2] It is assumed that two people exchange a shared key at least as long as the message in a completely secure way. The shared key encrypts the message to create the cipher, and the cipher is decoded by decrypting with the shared key. The protocol is best understood by trying it out with the associated worksheets. In practice, due to not having a secure channel to share such a complicated key, despite being unbreakable, this method is usually not employed.[3]

The most commonly used modern Internet encryption protocol is called RSA encryption. RSA encryption relies on encrypting messages with keys that are made out of very large integers. To decrypt a message, one would need to factorize this very large integer into its (prime) factors. Factorizing a large integer into its (prime) factors is known to be a problem that classical computers cannot solve in any reasonable amount of time.[4] For example, while it takes just a fraction of a second to multiply two prime numbers together to produce this large integer, finding which two prime numbers produced the integer would take a classical supercomputer thousands of years. RSA encryption works by encrypting the message with the public key. If an eavesdropper wanted to decrypt this message, they would need to factorize a large integer in the public key, which would take thousands of years. However, the private key related to the public key knows how to check the prime factors of the public key and can decrypt the message easily.

Alternatively, a bad actor could try to steal the private key, which Internet firewalls protect against. If a private key tries to decrypt a message that was encrypted with a public key not related to it, it has the wrong prime factors associated with the public key and the decryption fails. As such, nearly all Internet encryption relies on a computer not being able to factor large integers in a short amount of time.

However, in 1995, Peter Shor proposed a quantum computing algorithm, based on superposition and interference, that drastically speeds up the factoring process. A 4000-digit number, which would take a classical computer longer than the lifetime of the universe to factorize, would take less than a day on a quantum computer. Shor's algorithm[5] can theoretically break modern encryption schemes,

---

[2]Shannon, Claude (1949). "Communication Theory of Secrecy Systems." *Bell System Technical Journal*. 28 (4): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x.

[3]https://en.wikipedia.org/wiki/One-time_pad

[4]https://en.wikipedia.org/wiki/Integer_factorization

[5]https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/110-Shor%27s_algorithm.html

although quantum hardware is not advanced enough yet to make this decryption practical. If it were, all your bank details, military and industrial secrets, water and electric supply, etc., would be easily hacked. The details of Shor's algorithm are beyond our scope, so we will instead discuss how the same quantum computer could be used to establish a secure key. Together, the one-time pad and **quantum key distribution** (QKD) would be a formidable combination.

The BB84 QKD[6] simulation demonstrates how one could create a shared key using electrons and a Stern-Gerlach apparatus. The BB84 protocol is summarized below.

5.1 ▪ BB84 Protocol

Before sending the message

The sender (Alice) and receiver (Bob) publicly agree to the relationship between spins and bit value shown in Table 5.1.

	Alice		Bob	
Spin	$\uparrow$	$\leftarrow$	$\downarrow$	$\rightarrow$
Bit value	0	0	1	1

Table 5.1: Table for the relationship between Alice and Bob for quantum cryptography.

Quantum part

1. Alice randomly chooses either the x- or z-basis (horizontal or vertical Stern-Gerlach apparatus).

2. Alice sends an electron in superposition in the chosen basis through the SGA, measures the spin, and records the corresponding bit value as 0 or 1. The electron is sent to Bob.

3. Bob randomly chooses either the x- or z-basis.

4. Bob measures the spin of the electron and records whether it was 0 or 1.

5. Repeat steps 1–4 as many times.

Alice's Basis	z	z	z	x	x
Spin	↑	↓	↓	→	←
Bit value	0	1	1		

	↑	↓	↓	→	←

Bob's Basis	z	x	x	x	z
Spin	↑	→	←		
Bit value	0	1	0		

Figure 5.1: Alice and Bob's measurements of the BB84 protocol.

Example

Alice sends five electrons to Bob. When Alice sends an electron prepared in one basis and Bob measures in the same basis, they measure the same spin. However, if Bob measures in different basis than Alice, then the electron will be in a superposition state and there will be a 50% probability of the state collapsing into 0 or 1. Example values for the first three bits of a BB84 experiment are shown in Figure 5.1. Can you fill in the last two bits?

Classical post-processing

1. Alice and Bob publicly share the basis used for each bit measurement *without revealing the actual bit value they measured.*

2. If they measured in the same basis, they keep that bit. If they measured in a different basis, they discard that bit. This is shown in Figure 5.2. For the measurements performed in the same basis, Alice and Bob are guaranteed to have the same string of bits *unless there was an eavesdropper.*

---

[6]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-bb84/Quantum_Cryptography.html

3. They publicly compare a subset of the bits, say 20 out of 100 bits. If all 20 are the same, then it is unlikely that there was an eavesdropper. The remaining 80 becomes the shared key.

Alice's Basis	z	z	z	x	x
Spin	↑	↓	↓	→	←
Bit value	0	1	1	1	0

Bob's Basis	z	x	x	x	z
Spin	↑	→	←	→	↓
Bit value	0	1	0	1	1

Key	0			1	

Figure 5.2: Alice and Bob's measurements of the BB84 protocol completed from Figure 5.1. The discarded bits are grayed out, and the key is 01.

5.2 ▪ Detecting an Eavesdropper

If an eavesdropper (Eve) overhears the post-processing part where Alice and Bob share the basis used for each bit measurement, Eve has no information about whether any bit was either a 0 or 1. The only way for Eve to determine the spin value is to measure it with her own Stern-Gerlach *before* it gets to Bob. However, since the basis is not shared during the transmission, Eve must randomly pick a basis to use. If Alice and Bob randomly choose to not measure in the same basis, they throw away all the bits, then in this case, it doesn't matter what basis Eve chooses. If Alice and Bob randomly choose to measure in the same basis, however, then there are two outcomes depending on what Eve does: 1) If Eve randomly chooses the same basis as Alice, then she does not alter the state. This is bad, as Eve has successfully eavesdropped information without Alice and Bob knowing. 2) If Eve randomly chooses a different basis than Alice, then she alters the state and puts it into a superposition. Even though Bob is using the same basis

as Alice, due to Eve altering the state, Alice and Bob can have a different spin measurement. This is how they can catch an eavesdropper.

Example

The eavesdropping situation is shown in Figure 5.3. If Eve chooses the same basis as Alice, the spin is unchanged when it gets to Bob (bit #1). If Eve chooses a different basis than Alice, the spin will be different when it gets to Bob (bits #2 and #3). Eve could get lucky and Bob's bit could agree with Alice (bit #2). However, Bob is equally likely to measure something different from Alice (bit #3). Can you fill in what might happen with bits #4 and #5?

When Alice and Bob compare a portion of their key bits, a discrepancy would indicate the presence of an eavesdropper. If they compare a sufficient number of key bits and all of them match, they can be reasonably sure that the rest of it is secure.

5.3   Check Your Understanding

1. ● If Alice and Bob exchange measure 1 million bits in order to use the BB84 quantum cryptography protocol, approximately how long will their bit-key string be? Assume they do not check for eavesdropping.

2. ● Alice and Bob share their lists of measurement basis, but do not share any more information about the bits. What is the probability that Eve will guess the correct bit for a single bit-key?

3. ■ Alice and Bob perform 20 bit-key measurement but do not share any information about the bits. What is the probability that Eve will guess the correct 20-bit key?

4. ● If Eve tries all possible key combinations with the one-time pad, can she crack the one-time pad?

5. ■ If Eve uses a Stern-Gerlach to measure the spin in between Alice and Bob's measurements, what percentage of the time will she be lucky and get the correct key-bit value without detection?

6. ■ If Alice and Bob measure in the same basis and compare 20 bits of their key, what is the probability that Eve could have eavesdropped all 20 bits without being detected?

7. ● Suppose that Eve discovers that the no-cloning theorem is wrong and finds a way to clone the state of each photon. How could she use a cloning machine to learn about the entire key without leaving any trace?

Answers

1. Their basis will match half of the time, so their key will be 500,000 bits long.

2. The probability is 50%. Knowing that it's the z-basis could mean either 0 or 1 with equal probability. Similarly in the x-basis.

3. $(1/2)^{20} \approx 10^{-6}$.

4. Not with certainty. As mentioned in the one-time pad exercise, different keys could give a meaningful message. You couldn't tell which one was the correct one.

5. If Alice and Bob both use the z-basis, the different cases are:

   (a) Alice sends +z, Eve measures in z, Bob measures +z. ✓
   (b) Alice sends -z, Eve measures in z, Bob measures -z. ✓
   (c) Alice sends +z, Eve measures in x, Bob measures +z (will happen with 50% probability). ✓
   (d) Alice sends +z, Eve measures in x, Bob measures -z (will happen with 50% probability).
   (e) Alice sends -z, Eve measures in x, Bob measures +z (will happen with 50% probability).
   (f) Alice sends -z, Eve measures in x, Bob measures -z (will happen with 50% probability). ✓

   Therefore there is a 4/6 probability that Eve has not been detected.

6. $(4/6)^{20} \approx 0.0003$.

7. Copy the state of each electron, passing the originals along to Bob. Once the correct basis is revealed, pass those cloned electrons through SGAs oriented in the correct basis and get the key.
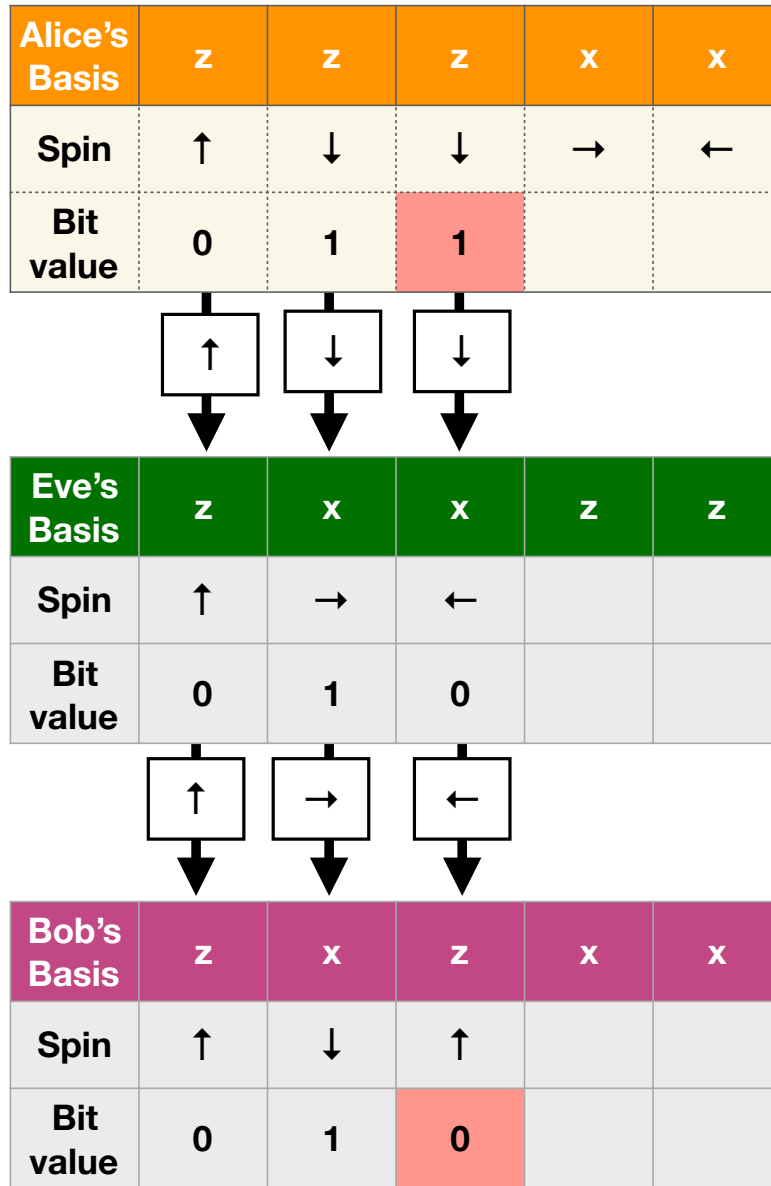
Alice's Basis	z	z	z	x	x
Spin	↑	↓	↓	→	←
Bit value	0	1	1		

	↑	↓	↓

Eve's Basis	z	x	x	z	z
Spin	↑	→	←		
Bit value	0	1	0		

	↑	→	←

Bob's Basis	z	x	z	x	x
Spin	↑	↓	↑		
Bit value	0	1	0		

Figure 5.3: An example of how to catch an eavesdropper using the BB84 protocol.

Chapter 6

Quantum Gates

6.1 ● Single Qubit Gates

As discussed in Chapter 2, information in classical computers is represented by bits. However, if the bits did not change, then the computer would remain the same forever and would not be very useful! Therefore, it is necessary to change the values of bits depending on what you want the computer to do. For example, if you want a computer to multiply the number 2 and the number 3 together to produce the number 6, then you need to put each of the numbers 2 and 3 into an 8-bit binary representation, and then have a computational operation to multiply the two 8-bit values together to produce 6. The operation of changing bits in a classical computer to do what you want is performed by what are called classical logic gates.

Classical computers manipulate bits using classical logic gates, such as OR, AND, NOT, NAND, etc. This link[1] provides a basic review of classical logic gates. Similarly, quantum computers manipulate qubits using quantum gates. The gates are applied to qubits and the state of the qubits changes depending on which gate is applied. A quantum algorithm has to be implemented on a quantum computer using the quantum gates. After running a quantum algorithm, the result is retrieved by measuring the qubit's state. The hardware implementation of quantum gates depends on how the qubit and quantum computer has been implemented technologically.[2] As an example, one could have a qubit based on spin. Then gates could be implemented using an external magnetic field to change the spin (and hence the qubit state). This chapter will focus on gates from the computing perspective rather than the engineering perspective. You will learn about several important gates that act on a single qubit, interpret histograms produced by a quantum computer simulator, and use matrices to describe the operation of these gates.

---

[1]https://whatis.techtarget.com/definition/logic-gate-AND-OR-XOR-NOT-NAND-NOR-and-XNOR

[2]E.g., topological qubits and superconducting qubits have very different hardware implementations due to their very different nature.

6.2 ▪ *X* (also called NOT) Gate

In classical computers, the NOT gate takes one input and reverses its value. For example, it changes the 0 bit to a 1 bit, or changes a 1 bit to a 0 bit. This is like a light-switch flipping a light from ON to OFF, or from OFF to ON. A quantum *X* gate is similar in that a qubit in a definite state $|0\rangle$ will become $|1\rangle$ and vice versa. When the qubit is in a superposition of all basis states, then the superposition also flips, e.g., see Equation (6.1).

$$\alpha|0\rangle + \beta|1\rangle \quad \boxed{X} \quad \beta|0\rangle + \alpha|1\rangle \qquad (6.1)$$

To see how it works, you can try out the IBM Q simulator.[3] Traditionally, all qubits on the IBM Q machine (or any other quantum simulator) start with the incoming qubits in the $|0\rangle$ state. To run this simple gate, drag the *X* gate onto any qubit. To see the results, add the measurement operation at the end. This is shown in Figure 6.1.
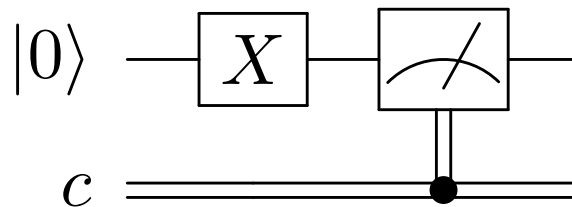

Figure 6.1: Applying the *X* gate on the IBM Q simulator and measuring the output.

After you click the "Simulate" button, you should see a histogram showing the measurements of the qubit's final state for 100 independent trial runs. Since the qubit always starts as the $|0\rangle$ state, applying the *X* gate produces the $|1\rangle$ state and so the measurement outcome is $|1\rangle$ 100% of the time as shown in Figure 6.2.

It is worth noting that any computer will have hardware errors. In a classical computer, this could be an electrical short of the motherboard, degradation of the technology storing memory on a hard drive and corrupting the stored classical bits. A real quantum computer will also have hardware errors. The quantum state of a qubit can change accidentally because of these hardware errors. Such errors may arise from the lack of full control of the interference between electromagnetic fields, variations in temperature, or energy dissipation. The accidental and incorrect change of a qubit state gives rise to the wrong answer which is called "noise".[4] As quantum computers only measure the state of a qubit, they cannot

---

[3]https://quantumexperience.ng.bluemix.net/qx/experience
It can also be run on IBM's real quantum computer, but you get a limited number of trials per day.

[4]Background noise is an event that causes unwanted or incorrect affects on a signal.
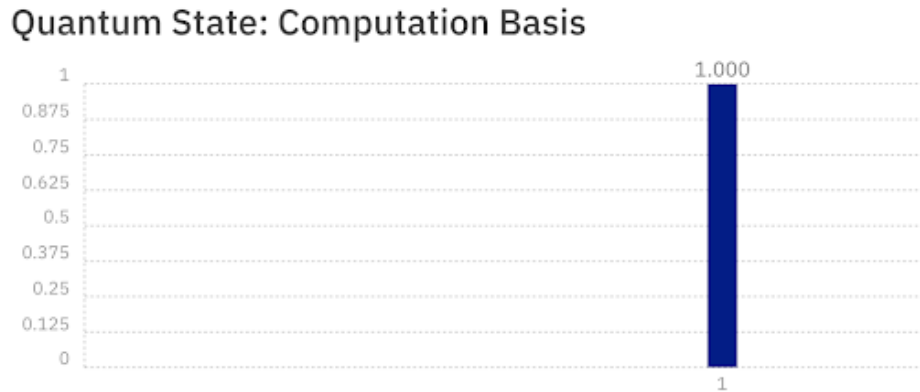
Quantum State: Computation Basis

Figure 6.2: Histogram showing that the qubit is measured in the $|1\rangle$ state with a probability of 1. Reprint Courtesy of International Business Machines Corporation, ©International Business Machines Corporation.

easily tell if the measurement is correct or incorrect. When we humans look at the measurements to interpret the results, noise can cause confusion on which answer is actually correct. Minimizing noise error is the greatest obstacle to building quantum computers.[5] For example, noise will cause the histogram in Figure 6.2 to not have the perfect 100% outcome. Instead, noise will cause the qubit to be in the $|0\rangle$ state incorrectly some of the time, and the measurement histogram will incorrectly be $x\%$ in the $|0\rangle$ state and $(100 - x)\%$ in the $|1\rangle$ state. If the noise is large, then $x = 50\%$ and measurement will be completely random. It should be understood that noise is an effect that occurs in both classical and quantum computers, but because quantum computing technology is in its infancy, the noise is not as well under control.

Mathematically, the quantum NOT gate is represented as a matrix X which acts on qubit states using matrix multiplication. The matrix representation is

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{6.2}$$

---

[5]Noise can also occur in classical computers. Here, it can be because a wire in the computer which holds the 0- or 1-bit breaks, and gives the wrong bit value. However, since classical computation has no probability associated with it, a single classical computation can be rerun twice and should give the exact same result. In practice, your computer reruns the same code many times to spot if there has been any errors and chooses the result which occurs most frequently. In this way you do not notice the hardware noise.

6.3 ■ **Hadamard Gate**

The Hadamard gate is very important in quantum computing. If the qubit starts in a definite $|0\rangle$ or $|1\rangle$ state, the Hadamard gate puts each into a superposition of $|0\rangle$ and $|1\rangle$ states. Applying a Hadamard gate to the $|0\rangle$ state qubit on the IBM Q simulator and measuring the output is shown in Figure 6.3.
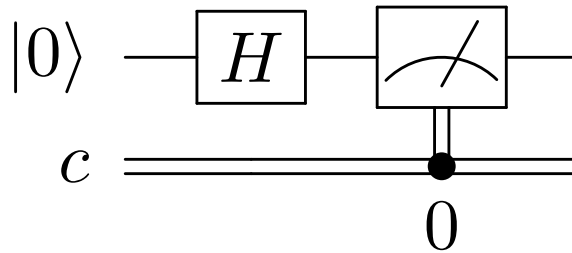

Figure 6.3: Applying a Hadamard gate and measuring on the IBM Q machine.

The result of running the circuit 100 times is a histogram shown in Figure 6.4. Note that each run is independent: before each measurement, the qubit has to be reset to the $|0\rangle$ state and passed through the gate, and then the measurement happens. We repeat this process 100 times. Each bin in the histogram shows the frequency/probability of measuring $|0\rangle$ or $|1\rangle$. You can clearly see that applying Hadamard gate to a single qubit creates a superposition state of both $|0\rangle$ and $|1\rangle$. The probabilities are not exactly 50/50 because of statistical error. The more data you collect, the closer the result converges to 50/50. This is similar to flipping a coin and counting the number of heads or tails; the greater the number of flips, the more likely you are to observe 50/50 probability of seeing heads/tails.

Recall that measurement collapses the superposition. Only one classical state can be observed, and all of the other quantum information is lost. Measurement collapse is the reason why a qubit's state cannot be duplicated which is known as the no-cloning theorem of quantum computing. Once a superposition state is measured, it fundamentally changes into one of the basis states, and hence cannot be duplicated. Still, it is not know how or whether measurement collapse happens.[6]

Question 1: Create a qubit in the $|1\rangle$ state and pass it through a Hadamard gate. From the measurement histogram, can you tell whether the qubit started as a $|0\rangle$ or $|1\rangle$ initial state?

The measurement histogram should look identical whether $|0\rangle$ or $|1\rangle$ were the initial state. Then how can we tell what the initial state was after a Hadamard operation? In the beam splitter, we determined where the photon came from by adding a second beam splitter to create interference. The way to measure and distinguish

---

[6]https://en.wikipedia.org/wiki/Measurement_problem

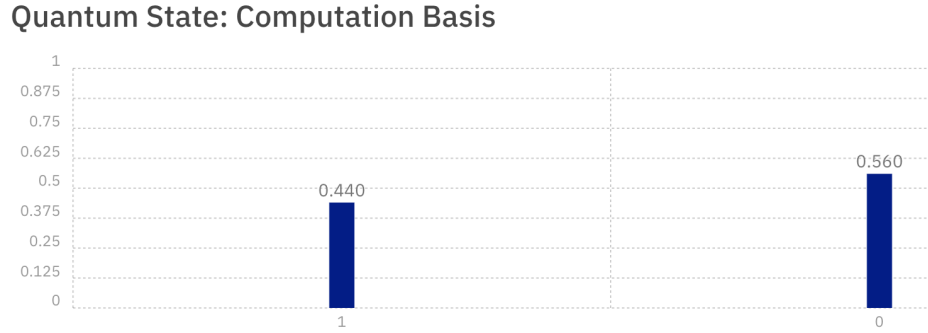## Quantum State: Computation Basis

Figure 6.4: Measurement histogram after applying the Hadamard gate from Figure 6.3 100 times. Reprint Courtesy of International Business Machines Corporation, ©International Business Machines Corporation.

between them is to add a second Hadamard gate.

Question 2: Build a circuit that applies two Hadamard gates to a qubit in the $|0\rangle$ initial state as shown in Figure 6.5. What is the output? Repeat this experiment for the $|1\rangle$ initial state.
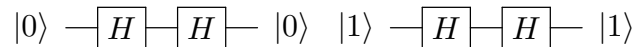
$$|0\rangle \; \text{—}\boxed{H}\text{—}\boxed{H}\text{—} \; |0\rangle \quad |1\rangle \; \text{—}\boxed{H}\text{—}\boxed{H}\text{—} \; |1\rangle$$

Figure 6.5: Applying two Hadamard gates to the $|0\rangle$ state or $|1\rangle$ state.

Mathematics of the Hadamard Gate

The Hadamard gate has the following matrix representation:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{6.3}$$

Using matrix multiplication we can show that application of the Hadamard gate to an $|0\rangle$ initial state puts the qubit into the $(1/\sqrt{2})(|0\rangle + |1\rangle)$ state, also called the $|+\rangle$ state which is shown in Equation (6.4).

$$|0\rangle \; \text{—}\boxed{H}\text{—} \; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{6.4}$$

If the initial state is $|1\rangle$, the Hadamard gate will create the superposition $(1/\sqrt{2})(|0\rangle - |1\rangle)$ state, called the $|-\rangle$ state as shown in Equation (6.5).

$$|1\rangle \; \text{—}\boxed{H}\text{—} \; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{6.5}$$

In the Stern-Gerlach experiment, you learned that the $|0\rangle$ and $|1\rangle$ states make up the z-basis and are associated with spin up and spin down. The $|+\rangle$ and $|-\rangle$ states make up the x-basis and are associated with spin right and spin left. While the Stern-Gerlach could be rotated to measure at any angle, a quantum computer is physically built to only measure in the z-basis. Therefore, the spin right $1/\sqrt{2}(|0\rangle + |1\rangle)$ and spin left $1/\sqrt{2}(|0\rangle - |1\rangle)$ look the same when measured by a quantum computer. However, the two states have hidden information that can be recovered by using a second Hadamard gate to change back into the z-basis.

Examples

1. A spin right $1/\sqrt{2}(|0\rangle + |1\rangle)$ is sent through a Hadamard gate, creating a superposition of $|+\rangle$ and $|-\rangle$ given by $1/\sqrt{2}(|+\rangle + |-\rangle)$. By making a basis change substitution, show that this is equivalent to producing a $|0\rangle$ state.

$$\frac{1}{\sqrt{2}}\Big(|+\rangle + |-\rangle\Big) = \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) + \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big), \quad (6.6)$$

$$= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle, \quad (6.7)$$

$$= |0\rangle. \quad (6.8)$$

2. Use matrix multiplication to show how applying the Hadamard gate twice to a $|0\rangle$ state qubit recovers its original state.

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad (6.9)$$

$$HH|0\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \quad (6.10)$$

In fact, all quantum gates are reversible as a consequence of the unitary matrix condition. Recall that the gates must be unitary so that the probabilities always add up to 1. Multiplying any unitary matrix by its conjugate transpose will return the identity matrix, i.e., reverses the gate to get the original state by $UU^\dagger = U^\dagger U = 1$.

6.4 ▪ Z **Gate**

The Z-gate matrix representation is

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (6.11)$$

The Z gate leaves a $|0\rangle$ state unchanged but flips the sign of the $|1\rangle$ state to $-|1\rangle$ by

$$\alpha|0\rangle + \beta|1\rangle \; \boxed{Z} \; \alpha|0\rangle - \beta|1\rangle. \qquad (6.12)$$

This is equivalent to changing the qubit from a $|+\rangle$ state to a $|-\rangle$ state. The effects of the X, H, and Z gates are summarized in Figure 6.6.
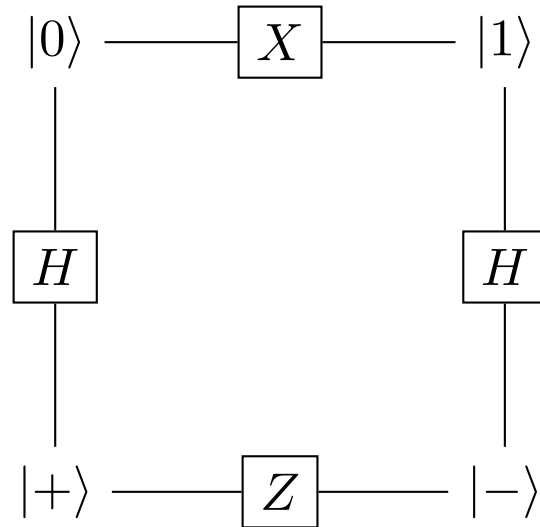

Figure 6.6: The X, H, and Z gates change the qubit's state in the z- and x-basis and are related according to this diagram.

6.5 Check Your Understanding

1. ◆ Use matrix multiplication to show how applying an X gate flips:

   (a) A qubit in the $|0\rangle$ state.
   (b) A qubit in the general $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ state.

2. ● Explain the relationship between a beam splitter and a Hadamard gate.

3. ● A $|0\rangle$ qubit is passed through a Hadamard gate. We measure the qubit state as $|1\rangle$. What is the result if we perform a measurement on the qubit a second time without reinitializing?

   (a) $|0\rangle$
   (b) $|1\rangle$

    (c) 50% chance of $|0\rangle$ or $|1\rangle$

4. ● Assume a qubit represents a light bulb that can be measured as either ON or OFF.

    (a) The light bulb is originally ON. What gate would you use to turn it OFF?

    (b) The light bulb is originally ON and passes through a Hadamard gate. What do you measure as the output?

    (c) The light bulb is originally ON and passed through two Hadamard gates in series. What do you measure as the output?

5. ■ Explain how the Hadamard gate is implemented in the Stern-Gerlach experiment.

6. ■ Explain the output of the Mach-Zehnder interferometer using what you learned about Hadamard gates.

7. ◆ Use matrix multiplication to demonstrate

    (a) The Hadamard gate applied to a $|1\rangle$ state qubit turns it into a $|-\rangle$.

    (b) A second Hadamard gate turns it back into the $|1\rangle$ state.

    (c) The output after applying the Hadamard gate twice to a general state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

8. ● Which of the quantum circuits in the Figure 6.7 would produce the histogram shown in Figure 6.4?
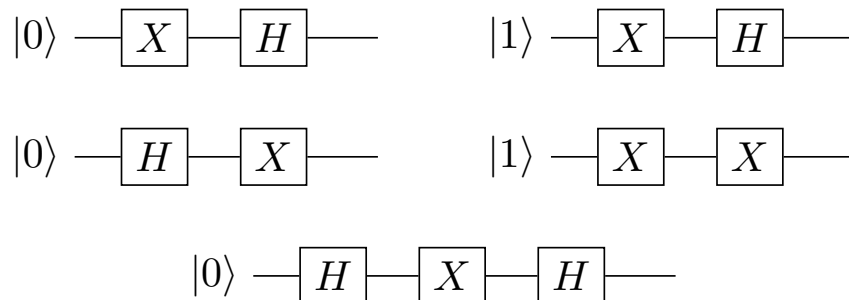
$$|0\rangle - \boxed{X} - \boxed{H} - \qquad |1\rangle - \boxed{X} - \boxed{H} -$$

$$|0\rangle - \boxed{H} - \boxed{X} - \qquad |1\rangle - \boxed{X} - \boxed{X} -$$

$$|0\rangle - \boxed{H} - \boxed{X} - \boxed{H} -$$

Figure 6.7: Six quantum circuits.

9. ◆ Use matrix multiplication to show how applying the Z gate to $|+\rangle$ changes it to $|-\rangle$.

10. ■ Using only the Hadamard and Z gates, design a quantum circuit that outputs the same result as an X gate.

11. ▪ Using the IBM Q simulator, apply the Z gate to a qubit in the following initial states and interpret the measurement histogram.

    (a) $|0\rangle$

    (b) $|1\rangle$ (Hint: You need to first flip the $|0\rangle$ state using the X gate.)

    (c) $|+\rangle$ (Hint: You need to first create the $|+\rangle$ state using the H gate.)

    (d) $|-\rangle$ (Hint: You need to first create the $|-\rangle$ state using the X and H gates.)

12. ▪ What is the expected measurement histogram produced by the circuit in Figure 6.8?

$$|0\rangle - \boxed{X} - \boxed{H} - \boxed{Z} - \boxed{H} - \boxed{\measuredangle}$$
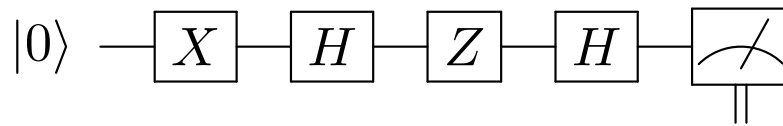
Figure 6.8: Circuit diagram.

13. ◆ Show that the Hadamard gate is unitary and therefore reversible.

Answers

1. (a)

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle. \tag{6.13}$$

(b)

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle. \tag{6.14}$$

2. The 50/50 beam splitter is an example of a Hadamard gate because it puts the photon into a 50/50 superposition.

3. A; the superposition has collapsed.

4. (a) An X gate reverses the state of the qubit.

   (b) It could either be ON or OFF with equal probability.

   (c) The light bulb will be ON with 100% probability. Applying a second Hadamard undoes the first Hadamard. This is a non-classical result because the first Hadamard creates the 50/50 superposition no matter whether its input is originally ON or OFF.

5. Sending spin up electrons into a horizontal SGA is identical to applying a Hadamard gate to a $|0\rangle$ qubit.

6. The Mach-Zehnder experiment is essentially two Hadamard gates in a row. The second gate undoes the superposition and returns a definite state.

7. (a)

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle. \tag{6.15}$$

(b)

$$HH|1\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle. \tag{6.16}$$

(c)

$$HH|1\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{6.17}$$

8. $|0\rangle \rightarrow X \rightarrow X \rightarrow |1\rangle$ and $|0\rangle \rightarrow H \rightarrow X \rightarrow H \rightarrow |1\rangle$.

9.

$$Z|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle. \tag{6.18}$$

10. $X = HZH$.

11. (a) The Z gate does not affect the $|0\rangle$ state.

    (b) The sign on the $|1\rangle$ state is changed, but this does not affect probabilities and so cannot be seen in the histogram.

    (c) The $|+\rangle$ is changed to a $|-\rangle$, which shows up as 50% $|0\rangle$ and $|1\rangle$.

    (d) The $|-\rangle$ is changed to a $|+\rangle$, which shows up as 50% $|0\rangle$ and $|1\rangle$.

12. 100% $|0\rangle$ as shown in Figure 6.6.

13.

$$H^\dagger H = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{6.19}$$

Performing the Hadamard operation twice is the same as multiplying by the identity matrix. Thus, the qubit is unchanged.

Chapter 7

Entanglement

So far, we have only discussed the manipulation and measurement of a single qubit. However, **quantum entanglement** is a physical phenomenon that occurs when multiple qubits are correlated with each other. Entanglement can have strange and useful consequences that could make quantum computers faster than classical computers. Qubits can be "entangled," providing hidden quantum information that does not exist in the classical world. It is this entanglement that is one of the main advantages of the quantum world!

To provide one example of the strange behavior of entanglement, suppose we have two fair coins. Classically, if you flipped two fair coins, you would measure the outcomes HH, HT, TH, or TT, each occuring with a 25% probability. However, by quantum entangling these two fair coins, it is possible to create a state $(1/\sqrt{2})(|HH\rangle + |TT\rangle)$ as illustrated in Figure 7.1. Many other types of entangled coins are possible, but this is one famous example. If you flipped this "entangled" pair of coins, they are entangled in such a way that only two measurement outcomes are possible: 1) both coins land on heads; or 2) both coins land on tails; each outcome occurring with 50% probability. Isn't that weird!

Furthermore, if the two entangled coins are separated by thousands of miles,
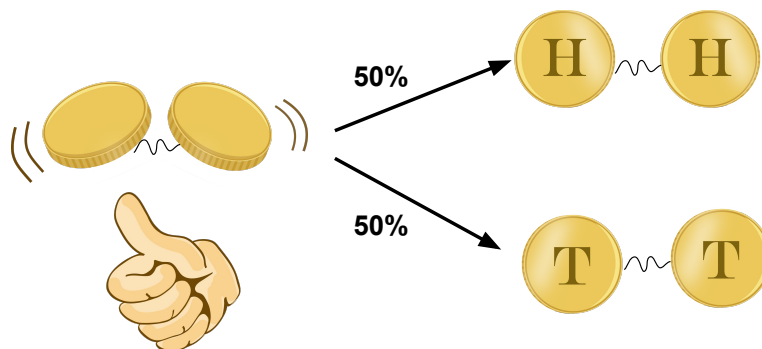
Figure 7.1: Two coins that are entangled in such a way that they either both land on HH or both land on TT.

one coin can be flipped and measured. In this case, if the measured coin produced the outcome heads, then we automatically know that the other coin must also land on heads. If the measured coin produced the outcome tails, then we automatically know that the other coin must also land of tails! If this isn't strange enough, the two coins could be separated by a distance greater than what light (which travels at the fastest speed in the universe) could travel as shown in Figure 7.2. If the two coins are flipped at the exact same time, somehow the two coins know to land on the same side as the other even though there can be no classical communication between them.[1]

How does the other coin instantaneously "know" what was measured on the other? Is information somehow being transmitted faster than the speed of light? Einstein called this behavior a "spooky action at a distance." It has since been shown that no information is being transmitted from one place to the other, and so no information is being transmitted faster than the speed of light. Rather, the particles share non-classical information at the time of entanglement, which is then observed in the measurement process. The correlation between entangled qubits is the key that allows quantum computers to perform certain computations much faster than classical computers.
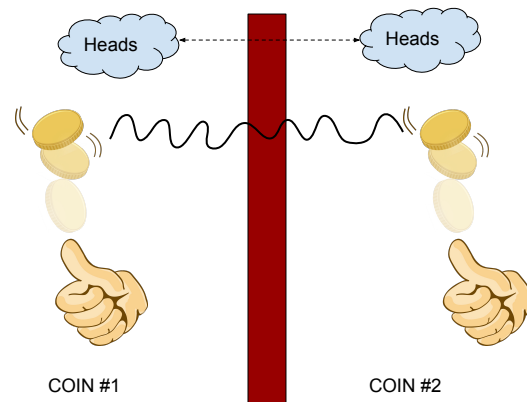
Figure 7.2: Two coins are separated with no means of communication between each other. Classically, the flip of the second coin would be unrelated to the first flip. However, entangled coins would still produce correlated results.

---

[1]"Bounding the speed of spooky action at a distance." *Physical Review Letters*. 110: 260407. 2013. arXiv:1303.0614.

7.1 ● Hidden Variable Theory

It is tempting to think that there may be some classical explanation for entanglement. For example, maybe when causing the coins to interact and entangling them, the same interaction might have changed the coins? Did the entanglement change the fair coins by adding extra mass to the heads side or the tails side, thereby making them unfair? To give a more realistic classical example, if one particle decays into two smaller particles, the momenta of the two particles are related according to the conservation of momentum by $\vec{p}_i = \vec{p}_{f1} + \vec{p}_{f2}$. Given a known total initial momentum, then by measuring the momentum of one of the smaller particles, we can determine the momentum of the other. By measuring one particle's momentum, we know the other. Momentum is the hidden classical variable that is encoded when the two particles are created. This is shown in Figure 7.3.
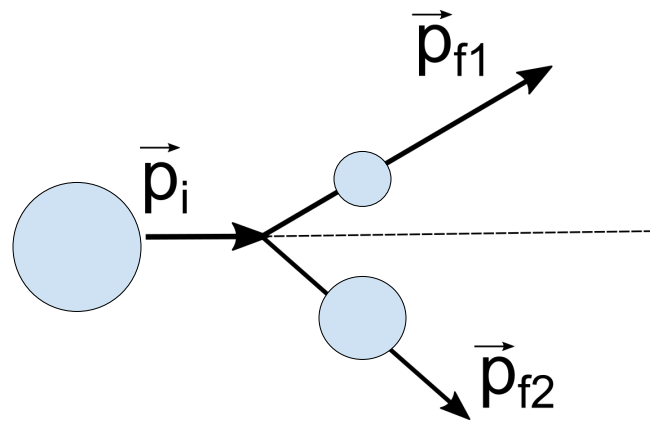
Figure 7.3: When a particle decays into two smaller particles, the decay products are "classically entangled" according to the conservation of momentum.

However, Bell's theorem[2] showed that the correlation between entangled quantum particles is more than what is possible classically, disproving the idea of a hidden variable. All other potential loopholes have been resolved as of 2016.[3] As such, entanglement is a purely quantum phenomenon with no classical explanation.

---

[2]https://brilliant.org/wiki/bells-theorem/

[3]The BIG Bell Test Collaboration (9 May 2018). "Challenging local realism with human choices." *Nature*. 557: 212–216. doi:10.1038/s41586-018-0085-3.

7.2 ▪ Multi-Qubit States

Given multiple qubits, the total state of a system can be written together in a single ket. For example, if coin #1 is heads and coin #2 is tails, the two-coin state is expressed as $|HT\rangle$. In general, a system of two qubits which is in a superposition of four classical states may be written as

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

As we saw for the single qubit states, the coefficients α_{ij} are called the amplitudes and are generally complex numbers. Measuring the two qubits will collapse the system into one of the four basis states with probability given by α_{ij}^2. This is shown in Figure 7.4.
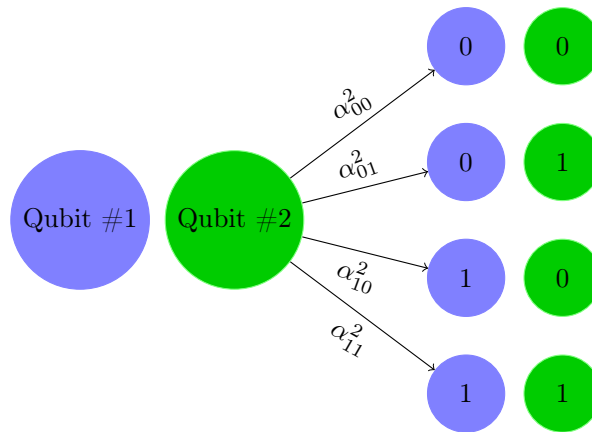
Figure 7.4: A two-qubit system can collapse into one of four states with probability α_{ij}^2.

Example

A system of two qubits is in a superposition state given by $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$.

a) What is the probability of measuring both qubits as 1?
   $\text{Prob}(|11\rangle) = \left(\frac{-1}{2}\right)^2 = \frac{1}{4}$.

b) If we only measure the first qubit and get a value of 1, what is the new state of the system?

   Since $|00\rangle$ is the only basis state of $|\psi\rangle$ that doesn't have a 1 in the first qubit, we eliminate the state $|00\rangle$ from the possibilities. This results in

$|\psi'\rangle = \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle.$

Finally, we renormalize the state so that the probabilities add up to 1. There-fore, the new state is $|\psi'\rangle = \frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$.

7.3 ● Non-Entangled Systems

It is possible to have a system of particles that are not entangled with each other. In this case, changing one particle will not cause any change in the other particle. For example, in a classical system, flipping two coins and measuring one coin as heads does not tell you any information about whether or not the other coin will land on heads or tails. These events are said to be independent. If you wanted to calculate the probability of $|HT\rangle$, you would simply multiply the probability of getting H on coin #1 by the probability of getting T on coin #2. This is given by

$$\text{Prob}\left(|HT\rangle\right) = \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) = \frac{1}{4}.$$

Non-entangled states are also called product states or separable states because they can be factored into a product of single-qubit states.[4] The single-qubit probabili-ties multiply to produce the two-qubit probabilities.

Example:

One qubit is in a $\alpha_0|0\rangle + \alpha_1|1\rangle$ state, while another is in a $\beta_0|0\rangle + \beta_1|1\rangle$ state. What is the state of the non-interacting two-qubit system?

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle) = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle.$$

7.4 ● Entangled Systems

In an entangled system, measuring the value of one qubit changes the probability distribution of the second qubit.

Example Is $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ an entangled state?

Yes! To see this, examine qubit #2. The probabilities for measuring qubit #2 in the $|0\rangle$ or $|1\rangle$ states are originally 50/50 respectively. However, if we measured

---

[4]More recently, it has been shown that there can exist quantum correlations in separable states that are not due to entanglement. These are called quantum discord: https://en.wikipedia.org/wiki/Quantum_discord.

qubit #1, then the probability for measuring qubit #2 becomes 100%. The same argument holds if qubit #2 is measured first. As such, measuring one of the qubits affects the probability of measuring the other qubit in a certain state, and so they are entangled. Mathematically, an entangled state is a special multi-qubit super-position state that cannot be factored into a product of the individual qubits.

Example: Show that $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ cannot be written as a product of two single qubits.

Assume that the state can be written as the product of two states.

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \stackrel{?}{=} (\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle), \tag{7.1}$$

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \stackrel{?}{=} \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle. \tag{7.2}$$

Comparing the amplitudes on the left vs. the right, the α_i's and β_j's must satisfy:

$$\alpha_0\beta_0 = \frac{1}{\sqrt{2}}, \quad \alpha_0\beta_1 = 0, \quad \alpha_1\beta_0 = 0, \quad \alpha_1\beta_1 = \frac{1}{\sqrt{2}}. \tag{7.3}$$

However, this is not possible. For example, take $\alpha_0\beta_1 = 0$. This means that either $\alpha_0 = 0$ or $\beta_1 = 0$. If $\alpha_0 = 0$, then $\alpha_0\beta_0 = 0$, but $\alpha_0\beta_0 = \frac{1}{\sqrt{2}}$ in the above equation. A similar contradiction occurs with $\beta_1 = 0$. So the initial assumption must be incorrect and this entangled state cannot be written as the product of two separate states.

7.5 ■ Entangling Particles

As there are many different ways of building a quantum computer, there are many different ways of entangling particles. One method called "spontaneous paramet-ric down-conversion" shines a laser at a special nonlinear crystal. The crystal splits the incoming photon into two photons with correlated polarizations. For example, one could produce a pair of photons that always have perpendicular polarizations (see Figure 7.5).

7.6 ■ CNOT Gate

You have already learned about the X, Hadamard, and Z gates. These act on a single qubit. There are also quantum gates that perform a logic operation on two or more qubits. The most important multi-qubit gate is the controlled NOT
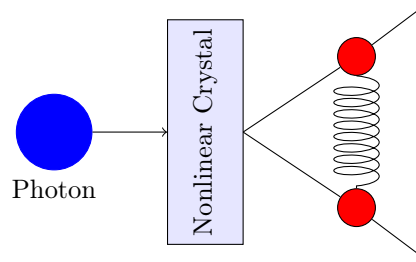
Figure 7.5: A nonlinear crystal creates two photons with entangled polarizations.

(CNOT) gate. The CNOT is used to entangle two qubits together and is essential in quantum computing/algorithms. The CNOT takes in two qubits, a control qubit and a target qubit, and outputs two qubits. The control qubit stays the same, while the target obeys the following rule.

- If the control qubit is $|0\rangle$, then leave the target qubit alone.

- If the control qubit is $|1\rangle$, then on the target qubit flip $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$.

Figure 7.6 is the circuit for the CNOT gate.
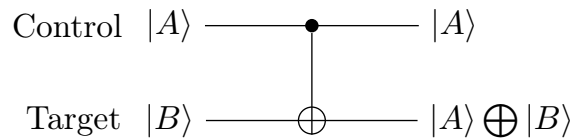
Figure 7.6: The CNOT gate performs an X gate on the target qubit if the control qubit is $|1\rangle$.

Examples

1. Figure 7.7 shows the IBM Q quantum circuit sending $|10\rangle$ through a CNOT gate. What is the output?

   The figure shows that the control qubit is q[1] and the target is q[0]. Since the control is in the $|1\rangle$ state, the target qubit is flipped to $|1\rangle$. So measurement will always result in $|11\rangle$.

2. Examine Figure 7.8. The control qubit is in a superposition of $|0\rangle$ and $|1\rangle$. What is the effect of a CNOT gate?

$$|10\rangle$$

Control   Target
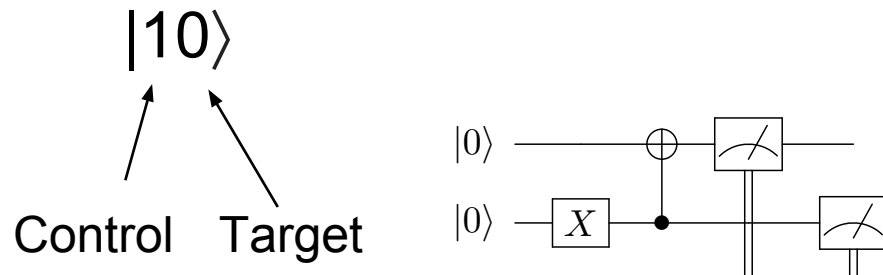
Figure 7.7: The IBM Q quantum circuit that sends a control qubit in the $|10\rangle$ state through a CNOT gate.
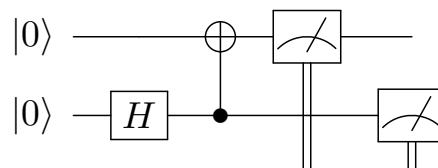
Figure 7.8: The IBM Q quantum circuit that sends a control qubit in a superposition state through a CNOT gate.

Before the CNOT operation, in ket notation, the control qubit is in the $\frac{1}{\sqrt{2}}|0\rangle +$ $\frac{1}{\sqrt{2}}|1\rangle$ state, while the target qubit is in the $|0\rangle$ state. The two-qubit input state is therefore $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$. Applying the rules for the CNOT, the first state $|00\rangle$ does not change as the control qubit is $|0\rangle$. However, for the second state $|01\rangle$, the control qubit is $|1\rangle$ and so the target qubit is flipped from $|0\rangle$ to $|1\rangle$. The result of the CNOT gate is the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. The histogram from measuring this state is shown in Figure 7.9. This is a special state called the Bell state.

The two qubits are entangled after the CNOT! As illustrated in the previous example, this state cannot be written as the product of two separate qubits. As with the single-qubit gates, the CNOT gate operates on ALL states in the superposition. Quantum algorithms leverages this parallelism to ensure speed improvements over classical computers. In addition, as with all quantum gates, the CNOT is reversible, meaning the operation can be undone (which can be used to figure out the original qubit states).
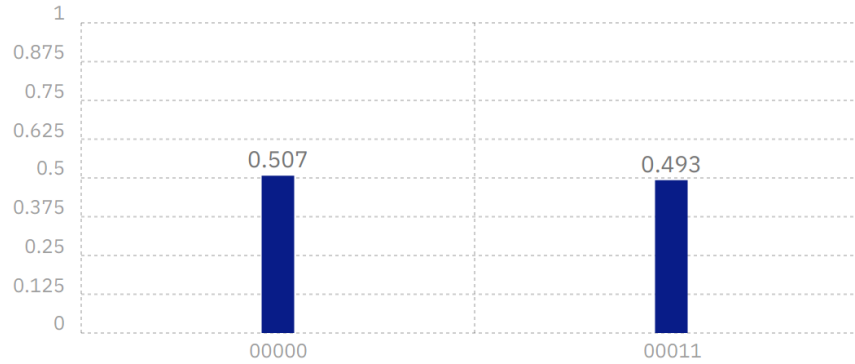
Figure 7.9: The measurement histogram produced by running the circuit in Figure 7.8. Reprint Courtesy of International Business Machines Corporation, ©International Business Machines Corporation.

7.7 Check Your Understanding

1. ● For each of the questions below, assume that two-qubits start in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle. \qquad (7.4)$$

   a) What is the probability of measuring both qubits as 0?
   b) What is the probability of measuring the first qubit as 1?
   c) What is the probability of measuring the second qubit as 0?
   d) What is the new state of the system after measuring the first qubit as 0?
   e) What is the new state of the system after measuring the first qubit as 1?

2. ● Two fair coins are flipped. What is the state of the two-coin system while the coins are in the air?

3. ● Two six-sided dice are rolled. What is the total probability of rolling an even number on one die and an old number on the other die?

4. ■ Is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$ an entangled state? If so, show that it cannot be written as a product. If not, what is the individual state of the two qubits?

5. ■ Are the following two-qubit states entangled?

   a) $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$
   b) $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$
   c) $\frac{\sqrt{3}}{2}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

d) $\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$

e) $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

f) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

6. ● Two qubits are passed through a CNOT. The first qubit is the control qubit. What is the output for the following initial states?

   a) $|00\rangle$

   b) $|01\rangle$

   c) $|11\rangle$

   d) $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$

   e) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

7. ● The output of a CNOT gate is shown in the figure below. What were the inputs?
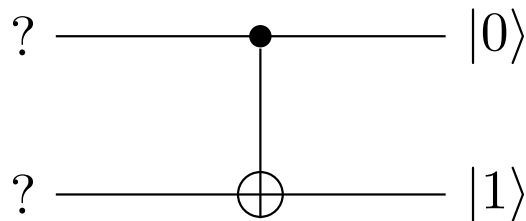
Figure 7.10: CNOT gate.

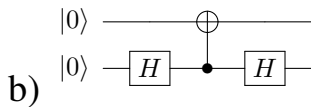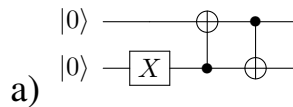8. ● Can you predict the state produced by these quantum circuits?

9. ■ Can you predict which states will be produced by these quantum circuits?

a)

$|0\rangle$ —[H]—⊕—
$|0\rangle$ ————●—

b)

$|0\rangle$ ————⊕—
$|0\rangle$ —[H]—●—

c)

$|0\rangle$ —⊕—[H]—
$|0\rangle$ —●————

d)

$|0\rangle$ —⊕————
$|0\rangle$ —●—[H]—
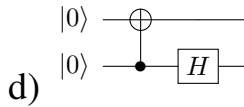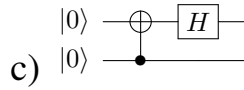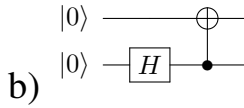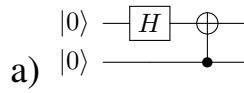
10. ◆ Can you predict the state produced by these quantum circuits?

a)

$|0\rangle$ ————⊕—●—
$|0\rangle$ —[X]—●—⊕—

b)

$|0\rangle$ ——————⊕————
$|0\rangle$ —[H]—●—[H]—

11. ■ Use the IBM Q simulator to create the entangled state $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$.

12. ■ Suppose Alice has one half of an entangled pair and Bob has the other half. When Alice makes a measurement on her qubit, Bob's qubit instantaneously changes its state. Can Alice and Bob use entanglement to transmit information faster than the speed of light? Why or why not?

Answers

1. a) The probability of measuring $|00\rangle$ is

$$\mathscr{P}(|00\rangle) = |\langle 00|\psi\rangle|^2 = \left(\frac{1}{\sqrt{2}}\right)^2. \qquad (7.5)$$

   We get this by taking the coefficient of the $|00\rangle$ term and then squaring it.

   b) The probability of measuring the first qubit as 1, $\mathscr{P}(\text{first qubit } |1\rangle)$, is the sum of all outcomes which have the first qubit in the $|1\rangle$ state. In this example, this is $\mathscr{P}(\text{first qubit } |1\rangle) = \mathscr{P}(|10\rangle) + \mathscr{P}(|11\rangle)$, which is equal to

$$\left(\frac{1}{2}\right)^2 + \left(\frac{-1}{2}\right)^2 = \frac{1}{2}. \qquad (7.6)$$

   c) The probability of measuring the second qubit as 0, $\mathscr{P}(\text{second qubit } |0\rangle)$, is the sum of all outcomes which have the second qubit in the $|0\rangle$ state. In this example, this is $\mathscr{P}(\text{second qubit } |0\rangle) = \mathscr{P}(|00\rangle) + \mathscr{P}(|10\rangle)$, which is equal to

$$\frac{1}{2} + \frac{1}{4} = \frac{3}{4}. \qquad (7.7)$$

   d) After measuring the first qubit as 0, then we know that the only part of $|\psi\rangle$ that has the first qubit as 0 is $(1/\sqrt{2})|00\rangle$. However, we need to renormalize the state to make sure it has probability of one. So the new state of the system after the measuring the first qubit as 0 is $|\psi'\rangle = |00\rangle$.

   e) After measuring the first qubit as 1, then we know that the only parts of $|\psi\rangle$ that have the first qubit as 1 are $(1/2)|10\rangle - (1/2)|11\rangle$. However, we need to renormalize the state to make sure it has probability of one. So the new state of the system after the measuring the first qubit as 1 is $|\psi'\rangle = \frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$.

2. The two-coin system can have four possible states: $|HH\rangle$, $|HT\rangle$, $|TH\rangle$, or $|TT\rangle$. The equal superposition of these states while the coin is in the air is $|\psi\rangle = \frac{1}{2}|HH\rangle + \frac{1}{2}|HT\rangle + \frac{1}{2}|TH\rangle + \frac{1}{2}|TT\rangle$.

3. $2 \times \text{Prob}(even) \times \text{Prob}(odd) = 2 \times \frac{3}{6} \times \frac{3}{6} = \frac{1}{2}$.

4. Not entangled. Knowing that the first qubit is 0 does not narrow down whether the second qubit is 0 or 1. Qubit 1 is $|0\rangle$ and Qubit 2 is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The tensor product gives the state in the question.

5. a) Yes

  b) Yes

  c) Yes

  d) No

  e) No

  f) Yes

6. a) $|00\rangle$

   b) $|01\rangle$

   c) $|10\rangle$

   d) $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$

   e) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|11\rangle - \frac{1}{2}|10\rangle$

7. The control qubit stays the same as 0. Since the control is 0, the target was unaffected. Therefore, the input was $|01\rangle$.
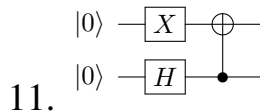
8. Note which qubit is the control qubit.

   a) $|01\rangle$

   b) $|10\rangle$

   c) $|11\rangle$

   d) $|01\rangle$

9. Note which qubit is the control qubit.

   a) The states change from the start to the end after every gate as: $|00\rangle \rightarrow |00\rangle + |10\rangle \rightarrow |00\rangle + |10\rangle$.

   b) The states change from the start to the end after every gate as: $|00\rangle \rightarrow |00\rangle + |01\rangle \rightarrow |00\rangle + |11\rangle$.

   c) $|00\rangle$ and $|10\rangle$

   d) $|00\rangle$ and $|01\rangle$

10. a) The states change from the start to the end after every gate as: $|00\rangle \rightarrow |01\rangle \rightarrow |11\rangle \rightarrow |10\rangle$.

   b) $|00\rangle, |01\rangle, |10\rangle$, and $-|11\rangle$

11.

12. No. Alice measures a random value. This automatically changes Bob's state. However, Alice would need to send a classical message to Bob to find out which state Bob measured; therefore information is still bounded by the classical speed of light. This scenario is known as Bell's theorem.

Chapter 8

Quantum Teleportation

One interesting application of entanglement is **quantum teleportation**, which is a technique for transferring an *unknown* quantum state from one place to another. In science fiction, teleportation generally involves a machine scanning a person and another machine reassembling the person on the other end. The original body disintegrates and no longer exists. Similarly, quantum teleportation works by "scanning" the original qubit, sending a recipe, and reconstructing the qubit elsewhere. The original qubit is not physically destroyed in the science fiction sense, but it is no longer in the same state. (Otherwise it would violate the previously mentioned **no-cloning theorem** − which says that a qubit cannot be exactly copied onto another qubit.[1]) The "scanning" part poses a problem though.

Question 1: Create a qubit in the $|1\rangle$ state and pass it through a Hadamard gate. From the measurement histogram, can you tell whether the qubit started as a $|0\rangle$ or $|1\rangle$ initial state?

The measurement histogram should look identical if either of the $|0\rangle$ or $|1\rangle$ states is used initially. Then how can we tell what the initial state was after performing a Hadamard operation? In the beam splitter, we determined where the photon came from by adding a second beam splitter to create interference. The way to measure and distinguish between them is to add a second Hadamard gate.

Question 2: If a qubit is in the unknown state $a|0\rangle + b|1\rangle$, what is the result of a single measurement?

  (a) 0

  (b) 1

  (c) 0 with probability a^2 and 1 with probability b^2

  (d) A number between 0 and 1

---

[1]The no-cloning theorem poses a big problem for correcting errors that happen on quantum computers: https://en.wikipedia.org/wiki/Quantum_error_correction.

Question 3: What is the result of a second measurement after the first from Question 2?

(a) 0 if the first measurement is 0 or 1 if the first measurement is 1

(b) 0 if the first measurement is 1 or 1 if the first measurement is 0

(c) 0 with probability a^2 and 1 with probability b^2

(d) A number between 0 and 1

Given a single qubit, it is not possible to determine how much of a superposition it is in if you only have this single qubit, i.e., you cannot determine the coefficients of $|0\rangle$ and $|1\rangle$ in a general state from one measurement! Note that if the state is known (from measuring many independent qubits that have been prepared identically), then you can just directly send the recipe to prepare this qubit. It is only when the state is unknown and when there is only one qubit that we have to think harder about how to efficiently "scan" the particle.

The way to get around the problem of not being able to measure the qubit (and avoid collapsing the unknown state onto a basis state) is to "scan" the qubit indirectly with the help of entangled particles. This comic[2] illustrates the basic idea. The protocol is as follows:

1. Alice and Bob meet up and make a qubit each (which we will call qubit #2 and #3). At this point, the two qubits are completely independent, i.e., think of the qubits as two different balls that do not contain any information about the other. Then, Alice and Bob decide to entangle their qubits by causing an interaction between the qubits such as application of a two-qubit CNOT gate. Using the previous metaphor, think of entanglement as Alice writing some information on Bob's ball that only she knows how to read, and Bob writing information on Alice's ball that only he knows how to read. For Bob to read Alice's information on his ball, Alice needs to send him a (classical) message with how to understand it, and vice-versa. They do not tell each other how to read the information yet. One possible entangled state (called the Bell-state) that they decide to make is

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle. \tag{8.1}$$

   Alice takes her qubit and walks away, and Bob takes his and walks in a different direction as shown in Figure 8.1.

2. Now Alice obtains a third different qubit in an unknown state (qubit #1) that she wants to transfer to Bob. She can only communicate with him classically by email or phone, and it would take too long to physically bring the qubit to Bob. The current situation is shown in Figure 8.2.
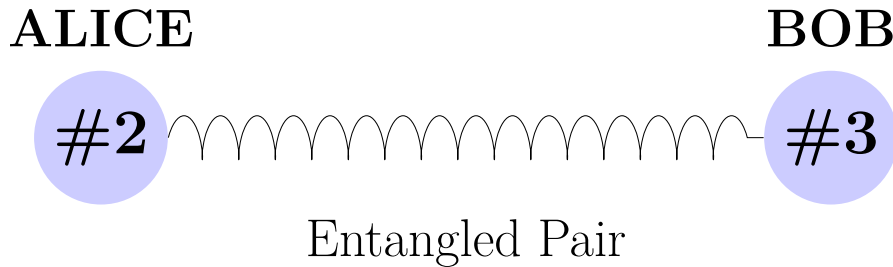
[2]https://www.jpl.nasa.gov/news/news.php?feature=4384

ALICE **BOB**

Figure 8.1: Alice and Bob's qubits are entangled.
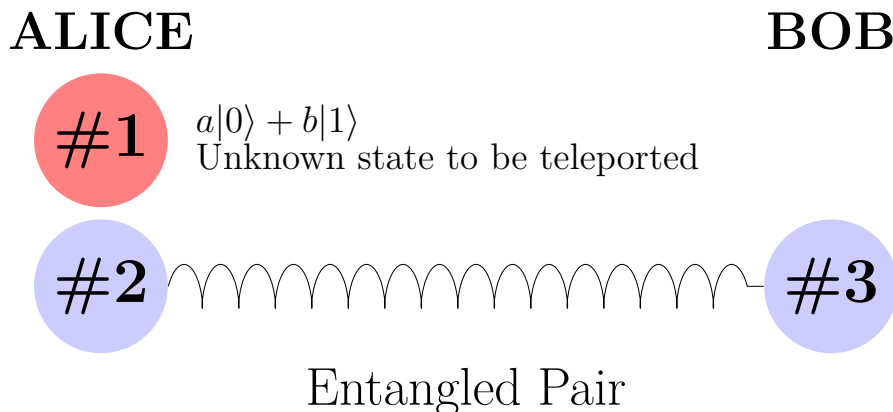
ALICE **BOB**

Figure 8.2: Alice has a qubit (#1) in an unknown state she wants to transfer to Bob.

3. Alice interacts her two qubits using a CNOT gate (qubits #1 and #2) and measures the qubit she originally had (qubit #2). She then sends the unknown qubit to be teleported (qubit #1) through a Hadamard gate and afterwards measures the output. Recall that the Hadamard gate is used to create a superposition of states. The current situation is shown in Figure 8.3.

Because Alice's original qubit (qubit #2) was entangled with Bob's, the CNOT interaction with qubit #1 immediately changes the state of Bob's qubit. By doing the math and drawing the full quantum circuit, one finds that Bob's qubit has changed into one of four possible superposition states. The four possible superposition states that Bob's qubit can be in depends on Alice's original qubit #2 through the initial entanglement in Step 1, as well as depending on the unknown qubit #1 to be teleported from the CNOT gate in Step 3. The reason we need to measure the state of Alice's qubit #2 and qubit #1 is to figure out the way Bob's qubit depends on these two. The current situation is shown in Figure 8.4. Note that Bob has not done anything with his qubit at this stage.

4. Alice sends the two classical bits of information from the measurements to
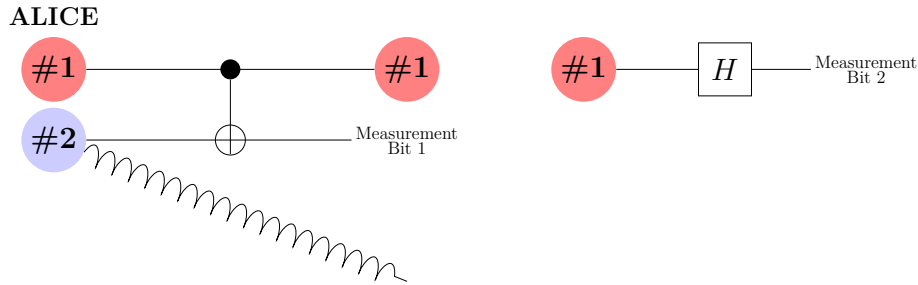
ALICE

Figure 8.3: Alice passes her two qubits through a CNOT gate.

BOB

$a|0\rangle + b|1\rangle$
$a|0\rangle - b|1\rangle$
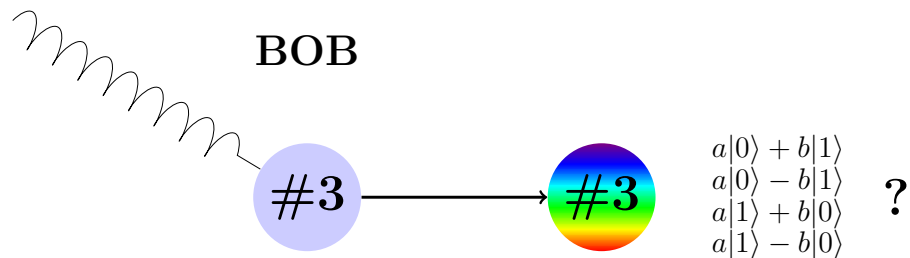$a|1\rangle + b|0\rangle$
$a|1\rangle - b|0\rangle$

?

Figure 8.4: Four possible superposition states of Bob's qubit.

Bob by email or phone.

5. Bob uses the two classical bits as the recipe for turning his qubit (now in an unknown state) into the correct state identical to qubit #1. Depending on the values of the classical bits, Bob will know which of the four possibilities he has and he can then change it into the correct state using *Z* and/or *X* gates. If he has the correct state already, he does nothing. The result of this is shown in Figure 8.5.

BOB

$a|0\rangle + b|1\rangle$
$a|0\rangle - b|1\rangle$
$a|1\rangle + b|0\rangle$
$a|1\rangle - b|0\rangle$

$a|0\rangle + b|1\rangle$
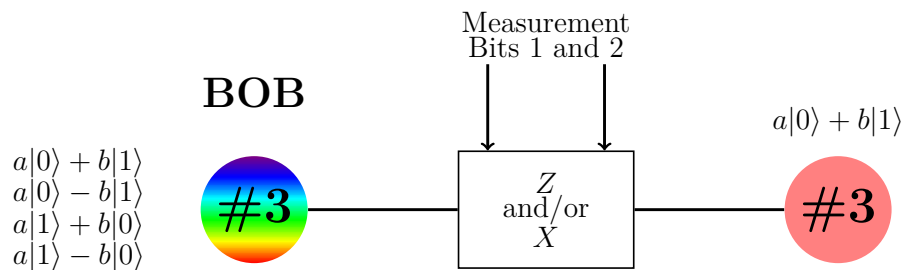
Figure 8.5: Final situation of entanglement between Bob and Alice.

It is important to understand that neither Alice nor Bob know what qubit #1's coefficients *a* or *b* are at any point in the process. All they know at the end is that qubit #1 has been teleported from Alice to Bob.

Why is this protocol interesting? To answer this, imagine Alice and Bob met a long time ago and each took one qubit of the entangled pair. Bob is now traveling around the world and can only communicate with Alice by phone or email. If Alice wanted to transfer quantum data to Bob without quantum teleportation, she would have to meet Bob and physically give Bob her qubit. Quantum teleportation allows Alice to send *quantum* information using a *classical* communications channel. All she has to do is make some measurements and email Bob the values. Bob can then apply the correct recipe to his qubit to get the data. Quantum teleportation is a useful way of causing interaction between different parts of a quantum computer (by teleporting a qubit to a different part of the quantum computer you want to interact with) as well as quantum cryptography (to prevent eavesdropping when sending information).

8.1 Check Your Understanding

1. ● Could quantum teleportation be used to teleport a physical object from one place to another? Why or why not?

2. ● What would lead someone to think quantum teleportation can transmit information faster than the speed of light? Explain why this is not possible.

3. ■ By the no-cloning theorem, it is not possible to make a copy of an unknown qubit. At what point in the teleportation protocol does the unknown qubit collapse into a definite state?

4. ■ In the original protocol, Alice applies the CNOT and then measures Bit 1 (see Figure 8.3). After this, Alice then applies the Hadamard to qubit #1 and then measures Bit 2 (see Figure 8.3). What happens if she decides to reverse the procedure by measuring Bit 2 first, before applying the two-qubit CNOT gate?

5. ● If Bob knows that his qubit is in the $b|0\rangle + a|1\rangle$ state, which gate(s) would he need to use to change it back into the original needed $a|0\rangle + b|1\rangle$ state?

   (a) X
   (b) Z
   (c) X then Z

6. ● If Bob knows that his qubit is in the $a|0\rangle - b|1\rangle$ state, which gate(s) would he need to use to change it back into the original needed $a|0\rangle + b|1\rangle$ state?

   (a) X
   (b) Z
   (c) X then Z

7. ● If Bob knows that his qubit is in the $a|1\rangle - b|0\rangle$ state, which gate(s) would he need to use to change it back into the original needed $a|0\rangle + b|1\rangle$ state?

   (a) X

   (b) Z

   (c) X then Z

8.2 Answers

1. No, the qubits stay in place. Teleportation only changes the state of an existing qubit.

2. If one entangled particle is measured, the state of the other changes instantaneously no matter how far apart. This was originally why people thought entanglement could transfer data faster than the speed of light. However, no information is communicated between these two particles. You don't know the state of the other entangled qubit unless information about the measurement is transmitted classically. This avoids Einstein's initial reservations about quantum mechanics which he called "spooky action at a distance."

3. Once it is measured after the Hadamard gate.

4. The qubit would collapse into a definite state, and there would be no information about the coefficients a and b when applying the CNOT gate.

5. The X gate flips the $|0\rangle$ into $|1\rangle$ and $|1\rangle$ into $|0\rangle$.

6. The Z gate flips the sign on the $|1\rangle$.

7. The X gate changes the state into $a|0\rangle - b|1\rangle$ and the Z gate flips the sign on the $|1\rangle$ to produce the desired state.

Chapter 9

Quantum Algorithms

9.1 ▪ The Power of Quantum Computing

The main advantage that quantum computers have over classical computers is **parallelism**. Because qubits can be in a superposition of states, a quantum computer can perform an operation on all of the states simultaneously. Let's say we want to know the result of applying some function $f(x)$ to some number x. Two classical computations are needed to find the result for $x = 0$ and for $x = 1$, whereas a quantum computer can evaluate both answers in parallel as displayed in Figure 9.1.
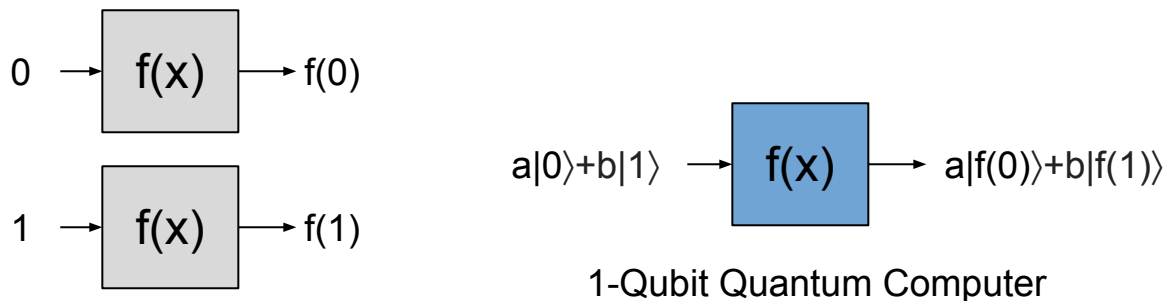
Figure 9.1: It takes a classical computer two operations to operate on two pieces of information. A quantum computer with one qubit can operate on two classical pieces of information at once.

If we wanted to compute $f(x)$ for $x = 2$ (represented as 10 in binary) and $x = 3$ (represented as 11), we would need to add a second qubit. The two-qubit quantum computer can then evaluate all four possibilities at once as shown in Figure 9.2.

f(x) → f(00)

f(x) → f(01)

f(x) → f(10)

f(x) → f(10)

Classical Computer

$a|00\rangle+b|01\rangle$
$+c|10\rangle+d|11\rangle$ → f(x) → $a|f(00)\rangle+b|f(01)\rangle$
$+c|f(10)\rangle+d|f(11)\rangle$

2-Qubit Quantum Computer
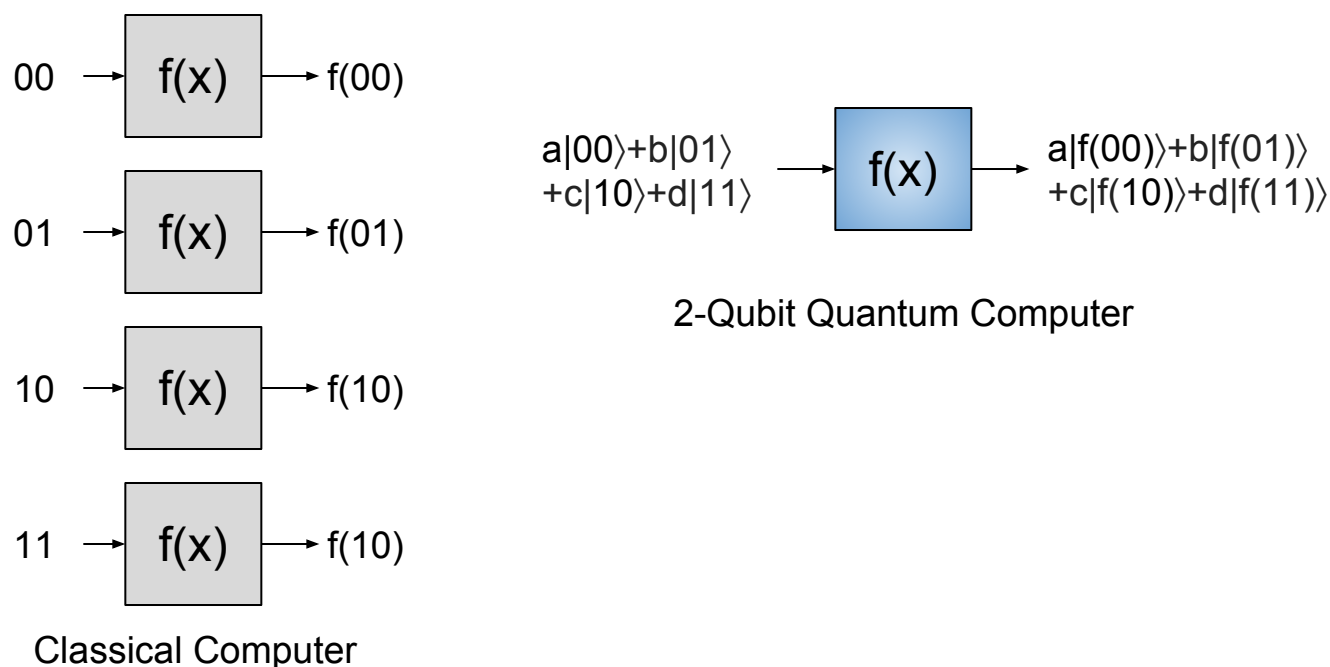
Figure 9.2: It takes a classical computer four operations to operate on four pieces of information. A quantum computer with two-qubits can operate on four classical pieces of information at once.

Question 1: How many pieces of information can a three-qubit quantum computer process in parallel? Write down all of the states. They are

$$|000\rangle,|001\rangle,|010\rangle,|100\rangle,|011\rangle,|110\rangle,|101\rangle,|111\rangle \rightarrow 8 \text{ pieces of information.} \tag{9.1}$$

Adding a qubit to a quantum computer doubles its processing power! For a classical computer, you need to double the number of wires in the processor to get double the processing power.[1] However, with a quantum computer, you only need to add a single qubit to double the processing power! Further, an n-qubit system can perform certain 2^n operations at once!

Separate from the issue of processing power is a concept known as memory. In a classical computer, on a standard 64-bit laptop, each number can be represented in the 64-bit binary representation (a simple extension of the 8-bit binary representation you already learned about). However, if you wanted four numbers on a 64-bit machine at the same time, then you need to have $4 \times 64 = 256$-bits of

---

[1]It is an observation that classical computers double their processing power roughly every 18 months. This is known as Moore's law.

memory on your hard drive to store them. On a 64 bit classical computer, for M different numbers, you need $M \times 64$-bits of memory; i.e., the bits needed for the memory is linear as a function of the number of numbers required. However, on an n-qubit quantum computer, there can be 2^n different coefficients of the quantum state that could in principle hold the numbers and therefore can be used as memory; i.e., the qubits needed for memory is logarithmic as a function of the number of numbers you want.

Because classical computers are very advanced and have large processing power and terabytes of memory, classical computers can simulate small quantum computers. As the addition of a single qubit would double the memory required, the largest supercomputer in the U.S.[2] would only be able to simulate a 46-qubit quantum computer. As of 2018, Google has a quantum computer with a quantum chip (called the Bristlecone) which has 72-qubits.

9.2 ▪ Limitations

While parallelism sounds amazing in theory, it is not immediately useful on its own. A quantum computation can calculate a superposition of the 2^n numbers, however a measurement still needs to be performed in order to extract information from the quantum computer. One measurement will only show one of those answers and afterwards collapse the superposition into a basis state. Think about it as if the 2^n numbers are all on a secret scratchpad that we cannot see, and nature shows you one random page at a time, then burns the scratchpad. You would need to run the quantum computer at least 2^n times to get all the numbers, therefore negating any advantage over classical computers. As an example of this, the two-qubit quantum computer can calculate the superposition $a|f(00)\rangle + b|f(01)\rangle + c|f(10)\rangle + d|f(11)\rangle$, but measuring this state will result in either $f(00)$, $f(01)$, $f(10)$, *OR* $f(11)$. If you are unlucky, due to the randomness of quantum physics, you could repeat the computation four times and still not see all of the possibilities.

Quantum computers are therefore only practical for certain types of problems. Since quantum computers are based on fundamental principles of nature (quantum physics) that includes classical physics, we intuitively expect those types of problems are the ones that can take advantage of more quantumness, e.g., simulating quantum physics directly. Generally, these types of problems look for correlations between different outputs. Due to this, it is generally accepted that quantum computers will not replace classical computers but will be able to perform different calculations that classical computers simply cannot. We will study an example problem which the quantum computer can solve more efficiently than a classical computer.

---

[2]The Titan at Oak Ridge Laboratory as of 2018

9.3 ◆ Deutsch-Jozsa Algorithm

Here we give a proof that quantum computers can be faster than classical computers by explicit construction of a problem.

The Problem

Let $f(x)$ be an unknown function that operates on a single qubit. There can only be four different functions that satisfy this requirement, and the four different functions are shown in Table 9.1.

f_1	f_2	f_3	f_4
$f_1(0) = 0$	$f_2(0) = 0$	$f_3(0) = 1$	$f_4(0) = 1$
$f_1(1) = 0$	$f_2(1) = 1$	$f_3(1) = 0$	$f_4(1) = 1$

Table 9.1: There are only four possible single qubit functions.

The question posed to the computer is this:

"Is $f(x)$ going to output the same two numbers or opposite numbers?"
A function is called **constant** if it always outputs the same result for all values of x. A function is called **balanced** if it outputs 1 for half of all the possible values of x and 0 for the other half.

Question 2: Which of the functions in Table 9.1 are constant and which are balanced?

The functions f_1 and f_4 are constant, while f_2 and f_3 are balanced.

Question 3: If you run the classical algorithm and see that $f(0) = 1$, could you tell whether the function is constant or balanced?

No, it could either be the balanced function f_3 or the constant function f_4. A classical computer would have to evaluate both $f(0)$ and $f(1)$ to determine the answer.

Quantum Solution

Procedure:

1. Put a qubit in a superposition of 0 and 1 with a Hadamard gate.

2. Operate on the qubit with the unknown function.

3. Apply another Hadamard gate.

4. Measure the qubit's state. A single measurement will tell you whether the function was constant or balanced.

We will not go into the math behind the algorithm, but it can be demonstrated using the Mach-Zehnder interferometer with phase shifters[3] as shown in Figure 9.3. Recall from the chapter on the beam splitter that the beam splitter will shift the phase of a photon depending on whether the photon hits the glass or dielectric side. The π phase shifters are pieces of glass that can be placed along the path to shift the phase an additional $180°$. Here is how the algorithm is implemented:

1. The two inputs $x = 0$ and $x = 1$ are represented by the two possible photon paths as shown in Figure 9.4. A photon taking the yellow path is $x = 0$, while a photon taking the red path is $x = 1$. The first beam splitter therefore creates a superposition of 0 and 1 since the photon takes both paths.

2. The four functions will be modeled by four different phase shifter configurations, as shown in Figure 9.5. A phase shifter is placed in the path whenever the function returns a 1.

3. The second beam splitter creates the interference necessary to tell whether there was an odd or even number of phase shifters in the way.

4. Measure which detector is activated. There is only one single measurement made. The single measurement made tells you the answer of the question.

Question 4: Which detector would go off for each function? Can you explain these results by thinking of light as a wave?

Question 5: How many photons would you need to send to determine whether the function was constant or balanced?

Thanks to superposition and interference, only one quantum measurement is needed to determine the answer to the Deutsch-Jozsa problem. In fact, the algorithm can be extended to test functions with any number of inputs.

9.4 ▪ Quantum Computers Today

While the Deutsch problem has no known commercial applications, useful quantum algorithms such as Shor's factoring algorithm rely upon similar concepts. Quantum algorithms are believed to exist that can speed up machine learning algorithms and efficiently simulate the quantum behavior of molecules. Unfortunately, current quantum computers are still very far from achieving quantum supremacy, i.e., outperforming the best classical computers. As of 2018, companies such as IBM and Google have built different types of quantum computers that contain up

---

[3]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/SinglePhotonLab/SinglePhotonLab.html.
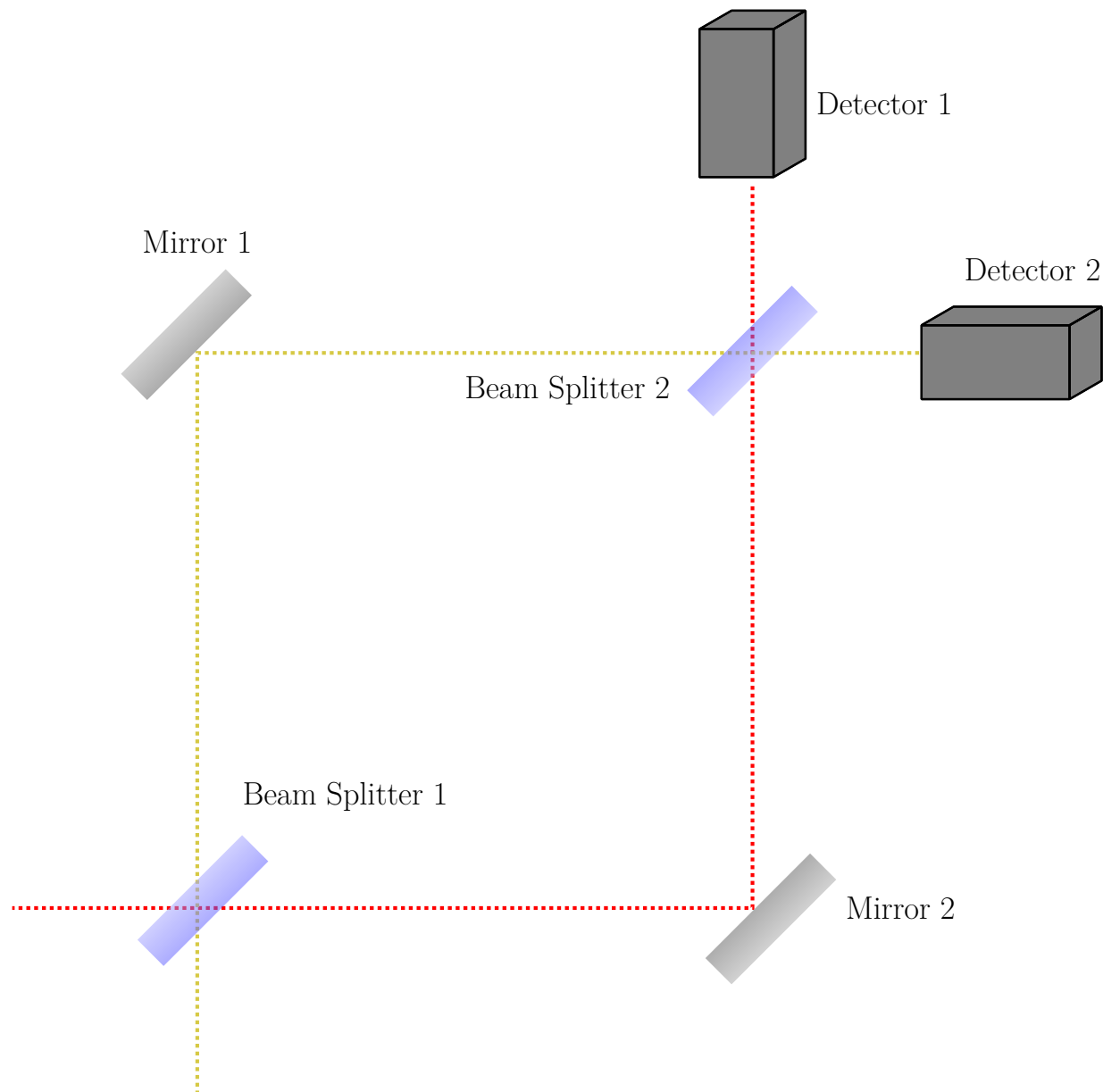
Figure 9.3: Mach-Zehnder interferometer with optional phase shifters.

to 72 qubits. To give you an idea of where we need quantum computers to be, factoring a 1024-bit modern encryption key using Shor's algorithm would require more than 5,000 qubits.

There are different technological difficulties when improving a quantum computer. As we have seen one way, a quantum computer can be built using lasers, which are bunches of photons. However, there are also random photons outside of the quantum computer in the environment that may accidentally leak into the quantum computer, and these environmental photons can then cause accidental changes to the quantum state. Such accidental changes are called "noise". To re-
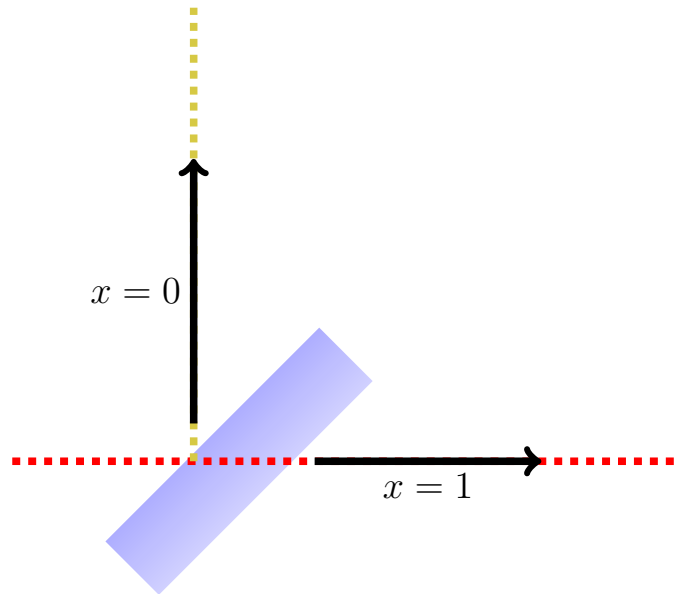
Figure 9.4: Inputs to the function are photons along two different paths. A photon taking the yellow path is $x = 0$, while a photon taking the red path is $x = 1$.

duce the number of these environmental photons, the quantum computer can be cooled down to near absolute zero (around -450° Fahrenheit). However, this is difficult. The more qubits you add, the more you need to keep at this low temperature (a technological challenge). Also, the more qubits you add, the more lasers you need to interact the qubits, which can be technologically difficult to keep lots of qubits in one small space but also cause isolated interactions between them. Further, the more qubits you add, the more likely it is that the qubits will interact accidentally with the environment, which will then destroy the system's quantum properties through a process known as decoherence. However, given how classical computers went from being the size of a room in the 1960s to an iPhone within a few decades, governments and industries are investing billions of dollars towards making quantum computers realistic. Ultimately, quantum computers are destined to complement classical computers, not replace them, so don't expect to have a quantum phone in your pocket anytime soon!

9.5   Check Your Understanding

1. a) How many different classical pieces of information can be represented by eight classical bits (1 byte)?
   b) What about a quantum computer with eight-qubits?
   c) What advantage does the quantum computer have over the classical computer?

f1

f2

Phase Shift
by π

Phase Shift
by π

Phase Shift
by π

f3

f4
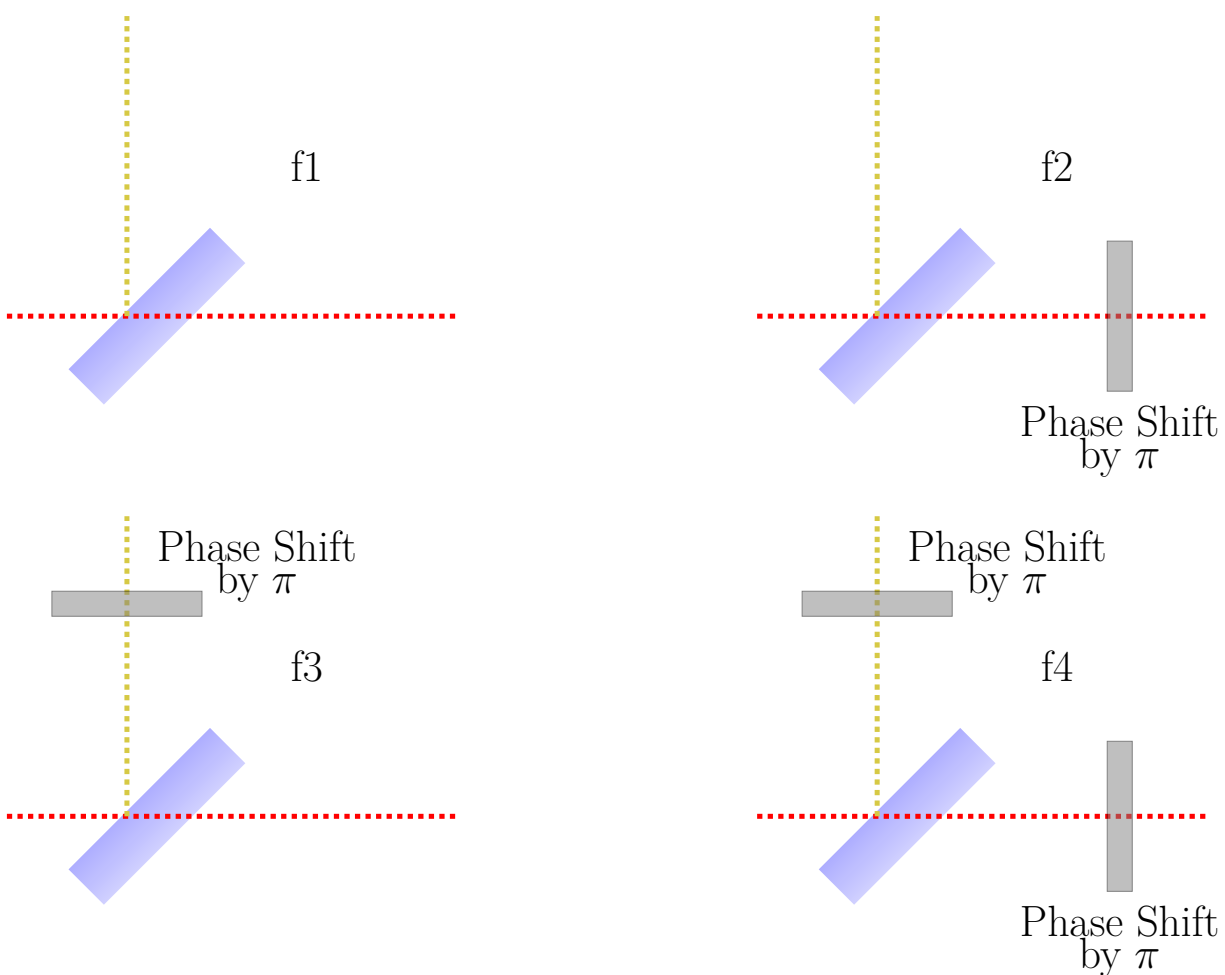
Phase Shift
by π

Figure 9.5: Four different functions modeled by four different phase shifter configurations.
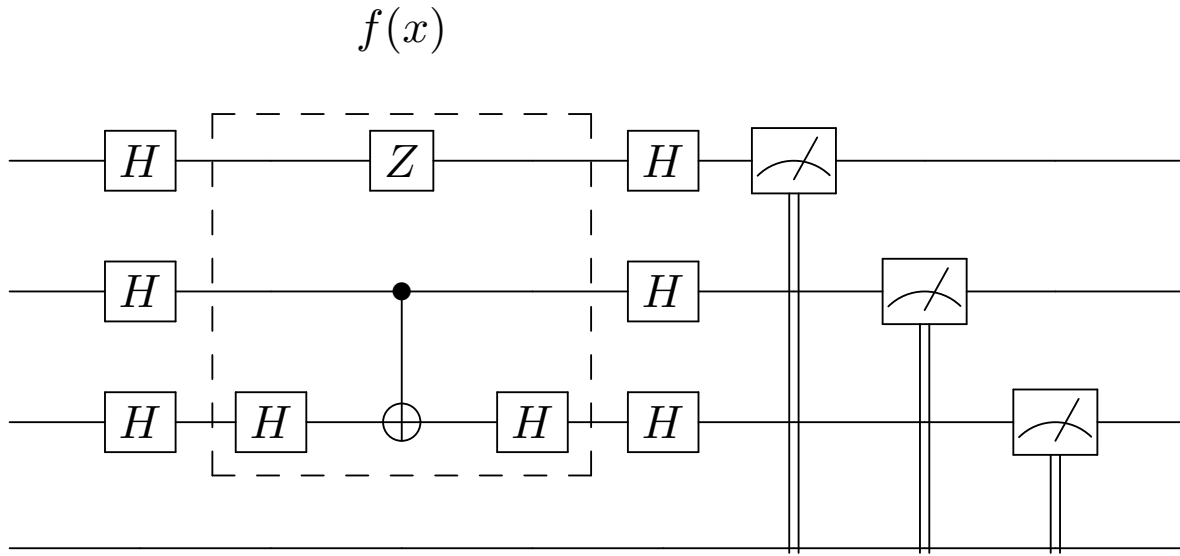
Figure 9.6: The gate implementation for testing the different possible three-qubit functions.

2. ■ Explain how superposition and interference allows the Deutsch-Jozsa algorithm to beat the classical algorithm.

3. ■ Figure 9.6 shows the gate implementation for testing a three-qubit function $f(x)$. A constant function will always result in $|000\rangle$.

    a) How many evaluations would be needed on a classical computer to tell whether this function is constant or balanced?

    b) By running this algorithm on IBM Q, can you determine whether this function is constant or balanced?

Answers

1. a) Both the classical and quantum computer can represent $2^8 = 256$ classical pieces of information.

   b) Both the classical and quantum computer can represent $2^8 = 256$ classical pieces of information.

   c) The quantum computer can create a superposition of up to 256 possibilities and do a computation on all of them. However, the output will be only one classical value.

2. The photon is put in a **superposition** such that the function can evaluate both $x = 0$ and $x = 1$ simultaneously. If the second beam splitter was not there, there would be a 50/50 chance of the photon being in either path and the detectors would not provide a definite answer. The second beam splitter creates the **interference** necessary to create the 100% probability of being in the right situation.

3. a) The most naive classical algorithm is one where you evaluate every function value and make a list of the results. In this case there are $2^3 = 8$ different function values that would need to be evaluated separately. If each element in the list is identical then the function is constant.
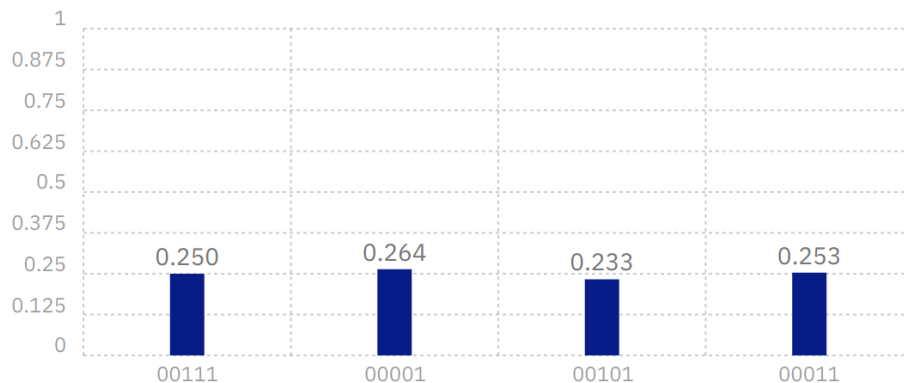
   b)

   Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

   Since there are results other than $|000\rangle$, the function is not constant. Also, since the function has four non-zero outcomes (each with 25% probability) out of the eight possible outcomes, the function is balanced.

Chapter 10

Worksheets

10.1 ■ Correlation in Entangled States Lab

Objectives:

- Experimentally determine the difference between two particles in a product state vs. an entangled state using the entanglement simulator.[1]

- Apply the idea of basis changing to explain the correlation that is observed.

Questions

Alice and Bob each measure one of two qubits with a Stern-Gerlach apparatus. Start with both SGAs along the z-axis
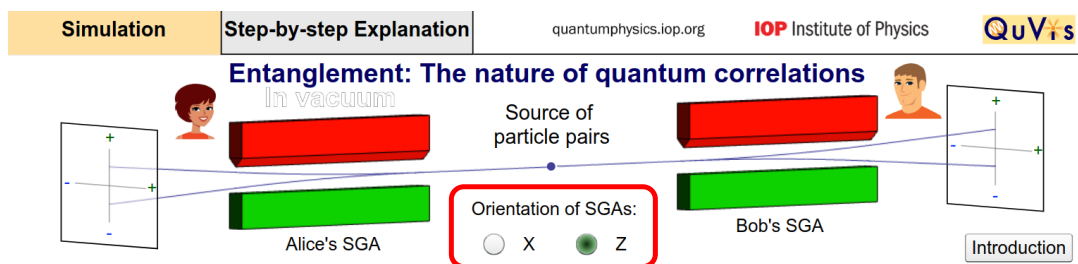
Figure 10.1: Figure reproduced from the QuVis website, licensed under creative commons CC-BY-NC-SA.

1. Try sending pairs of particles in a product state $|\uparrow_A\rangle|\downarrow_B\rangle$. What do Alice and Bob measure individually?

---

[1]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/entanglement/entanglement.html

2. Try sending pairs of particles in an entangled state: $\frac{1}{\sqrt{2}}(|\uparrow_A\rangle|\downarrow_B\rangle - |\downarrow_A\rangle|\uparrow_B\rangle)$. What do Alice and Bob measure individually?

3. If Alice measures her spin, would you be able to predict Bob's result:

   a) In the product state?
   b) In the entangled state?

 Now rotate both SGAs along the x-axis.
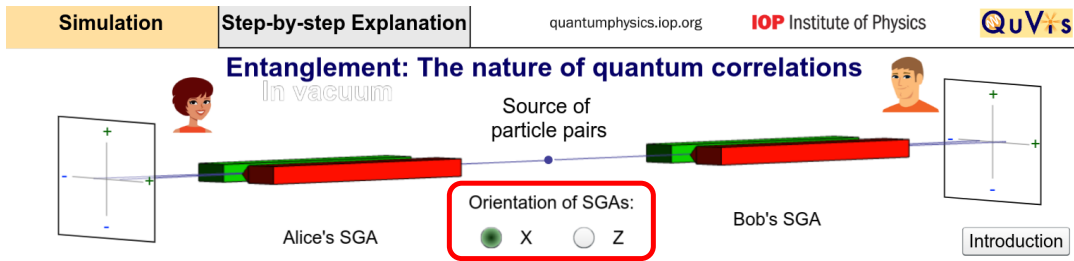
Figure 10.2: Figure reproduced from the QuVis website, licensed under creative commons CC-BY-NC-SA.

4. Try sending pairs of particles in a product state $|\uparrow_A\rangle|\downarrow_B\rangle$. What do Alice and Bob measure individually?

5. Try sending pairs of particles in an entangled state $\frac{1}{\sqrt{2}}(|\uparrow_A\rangle|\downarrow_B\rangle - |\downarrow_A\rangle|\uparrow_B\rangle)$. What do Alice and Bob measure individually?

6. If Alice measures her spin, would you be able to predict Bob's result:

   a) In the product state?
   b) In the entangled state?

7. Convert the product state $|\uparrow_A\rangle|\downarrow_B\rangle$ into the x-basis and use it to explain the observations in the x-basis. Recall that $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|\downarrow\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$.

8. Convert the entangled state $\frac{1}{\sqrt{2}}(|\uparrow_A\rangle|\downarrow_B\rangle - |\downarrow_A\rangle|\uparrow_B\rangle)$ into the x-basis and use it to explain the measurements in the x-basis.

9. Suppose that there are two possible sources of particles. Source #1 randomly emits two particles in either the state $|\uparrow_A\rangle|\downarrow_B\rangle$ or $|\downarrow_A\rangle|\uparrow_B\rangle$ with equal probability. Source #2 emits two particles in the entangled state $\frac{1}{\sqrt{2}}(|\uparrow_A\rangle|\downarrow_B\rangle - |\downarrow_A\rangle|\uparrow_B\rangle)$. How can Alice and Bob tell whether the source is #1 or #2?

Answers

1. Alice always measures up; Bob always measures down.

2. They each see up and down 50% of the time.

3.   a) Yes.

    b) Yes. Every time Alice measures up, Bob measures down and vice versa.

4. They each see up and down 50% of the time

5. They each see up and down 50% of the time

6. (a) No, the results are random.

   (b) Yes. Every time Alice measures $+$, Bob measures $-$ and vice versa. The entangled state is still correlated in the x-basis.

7.

$$|\uparrow\downarrow\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \times \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) = \frac{1}{2}|++\rangle - \frac{1}{2}|+-\rangle + \frac{1}{2}|-+\rangle - \frac{1}{2}|--\rangle$$

All four possible states are observed. The middle two terms do not cancel out because they are different states: Alice measures $+$ and Bob measures $-$, or Alice measures $-$ and Bob measures $+$.

8.

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle) = \frac{1}{\sqrt{2}}(-|+-\rangle + |-+\rangle).$$

Only two states are observed where Alice and Bob always get opposite results.

9. They cannot tell them apart in the z-basis, but they could measure the particles in the x-basis. If Alice and Bob always get opposite results, the source emits entangled particles. If there is no correlation, the particles are not entangled.

10.2 ■ Polarizer Demo

For students who have learned about polarization, the creation of superposition states can be demonstrated using three polarizing filters. When unpolarized light is sent through a vertical filter, only vertically polarized light is able to pass through. Sending vertically polarized light through a horizontal filter results in no light passing through, since the vertical and horizontal polarizations are mutually exclusive. Surprisingly, adding a diagonal filter in between recovers the light! The diagonal polarizer introduced a horizontally polarized component, similar to how passing a spin-up electron through a horizontal SGA created a horizontal superposition.
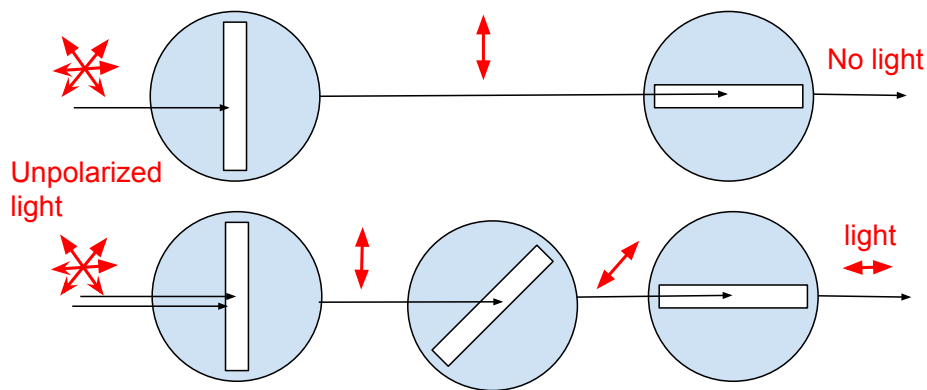
Figure 10.3

Question: Relate the behavior of the polarizers to what you saw in the SGAs.

10.3 ● Quantum Tic-Tac-Toe

Quantum Tic-Tac-Toe was developed by Alan Goff in 2004 as a metaphor to teach quantum concepts such as superposition, entanglement, and measurement collapse. It has been found to be a helpful strategy in teaching quantum mechanics to undergraduate students at Purdue, especially for students who struggle with grasping the concepts.[2]

Quantum Tic-Tac-Toe resembles the classical Tic-Tac-Toe game in its setup and objective of completing three in a row. However, the game uses characteristics of quantum systems, so instead of using one marker *X* or *O*, the players use pairs of *X*s and *O*s, which are traditionally called "spooky," after Einstein's reference to entanglement as "spooky action at a distance".[3] Using indices for each marker's move is important when determining the winner of the game. Additionally, we use a color code for each player and connect the spooky markers to help students better visualize the game process. We also number the squares for future reference.
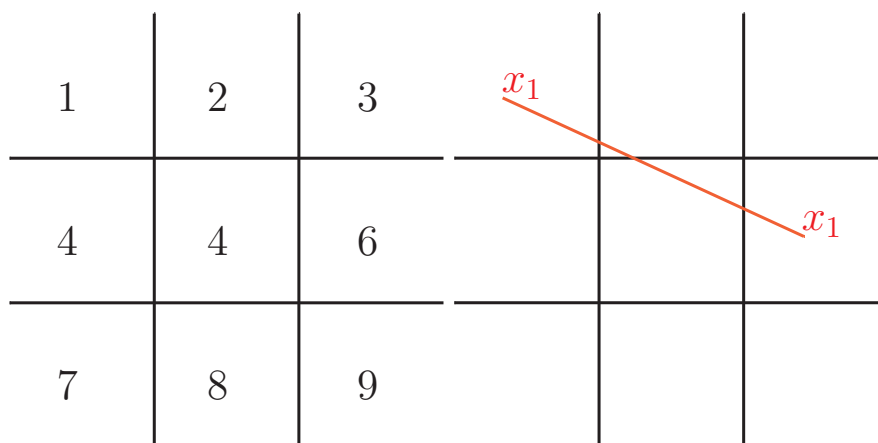
Figure 10.4: The Quantum Tic-Tac-Toe layout with numbered squares (left): one player's move with spooky markers x_1 (right).

The Rules

1. The X player goes first. We note that keeping indices helps to track the game. The markers can be placed in any of the two spaces on the game board (Figure 10.4).

2. The O player goes next. The markers can be placed in any two squares, even ones that are already occupied by other X or O markers. Notice in Figure 2

[2]Hoehn R.et al (2014). "Using Quantum Games to teacher quantum mechanics, Part 1." *Journal of Chemical Education* 91 (3), 417-422. Retrieved from https://pubs.acs.org/doi/ipdf/10.1021/ed400385k

[3]Einstein, Podolsky, and Rosen (1935) "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review, 47* : 777-780. Retrieved from https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

that the index for the O player also starts with 1, representing its first move placing markers in squares 1 and 6.

3. Player X goes again and can place their spooky markers at any two squares, even ones occupied by other Xs or Os. The game goes on until the players create a "cyclic loop" as seen in the following example:
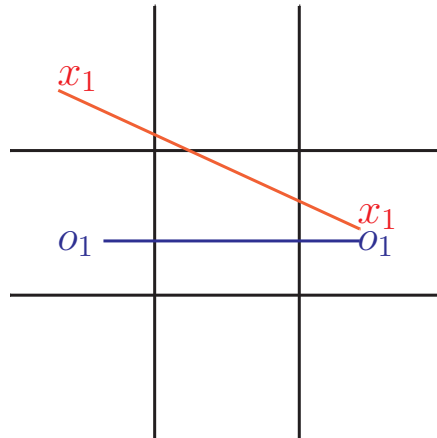

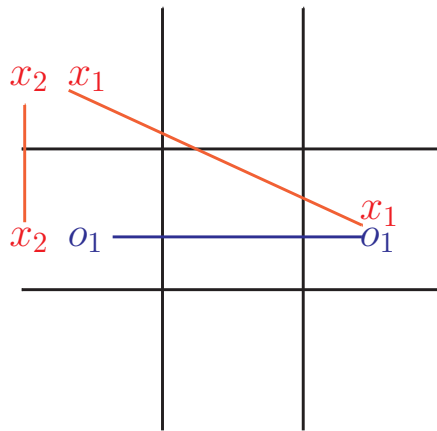Figure 10.5: Example of the second player's move.

Figure 10.6: The cyclic loop is created by the player X. Using lines between the spooky markers helps in identifying the loop.

4. **Collapsing the quantum state**. When a loop is created, the players have to collapse their state. The are three options for who makes the decision on how the markers will be collapsed. The fair choice would be by the player who did not create the cycle (in this case, player O). When the markers are forced to collapse, only one of the two squares for each move can be chosen, so player O can choose either square 4 or 6. Depending on their choice, the outcome would be different (Figure 4). Once the states are collapsed, the "spooky markers" change into classical markers and they fully occupy the state of one particular square.
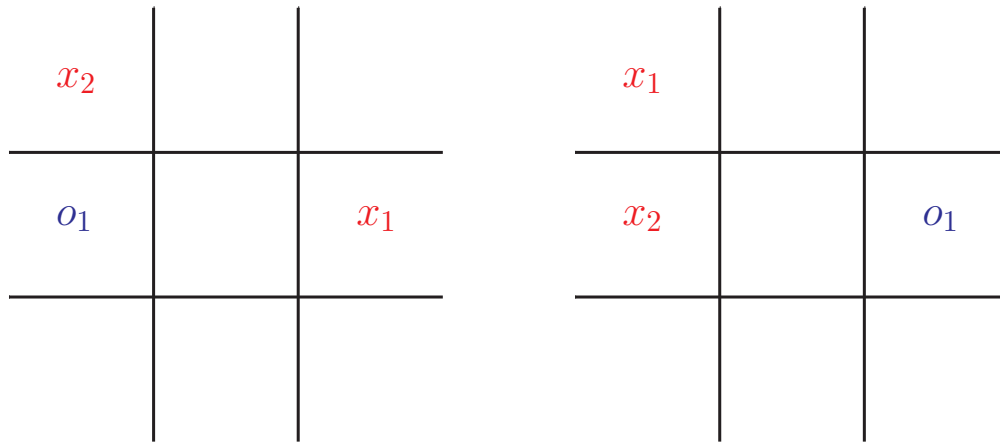
Figure 10.7: The two collapse outcomes due to player O's decision.

5. The next player can place his spooky markers in any two squares except the ones that are occupied by the collapsed markers. The game goes on until another cycle is created and the players are forced to collapse the state.

6. **Winning the game**. In some cases both players will create three in a row after collapsing their spooky markers. In this case, the player with the smallest sum of indexes wins. For example, in Figure 5 player X wins because their has the smaller sum.
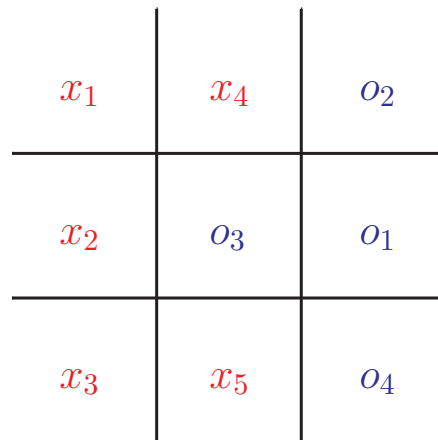
Figure 10.8: Player X wins, because the sum of their indexes is $1 + 2 + 3 = 6$. Player O got three in a row, but the sum of their indexes is $2 + 1 + 4 = 7$.

Some other rules can be added or modified. One of the requirements could be that players cannot place both markers in the same square like the one shown in Figure 10.3. Another way to make the collapse more quantum (or more random) is using a coin flip to decide which player chooses the collapse.

Other modifications may include assigning different point values for three in a row, such as the winner with lowest sum of the indexes gets 1 point, while the

$$x_1 - x_1$$
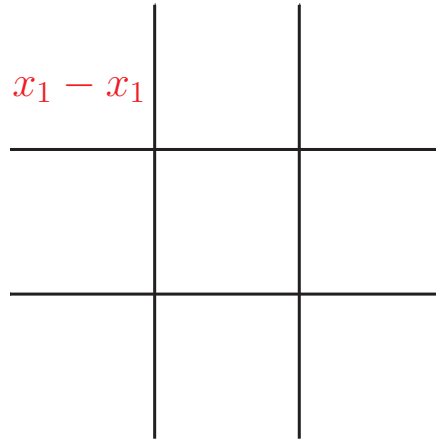
Figure 10.9: Player X wins because the sum of its indexes is $1 + 2 + 3 = 6$. Player O got three in a row, but the sum of the indexes is $2 + 1 + 4 = 7$

other player gets $1/2$ point.

One of the main challenges of playing the game is to observe when a cycle has been created so the state of the spooky markers can be collapsed at the right time. A computer-simulated game will automatically keep track of this and will force students to collapse their markers, such as this game simulator.[4]

We found that using color codes and connecting lines helps visually track loops. Another way is to create a model of the game where students can see the connections and collapse the states using physical pieces. It would be interesting to see students' responses as to which medium helps them understand the game principle better.

Connection to quantum physics

How are the game rules and principles connected to the real applications of quantum mechanics? There are three major themes that can be drawn from the game: superposition, the effect of measurement, and entanglement.

Superposition

In classical physics all objects have defined states. However, quantum systems can exist in a superposition of several classical states at the same time. The example could be electron with a spin that is in superposition of up and down, or a photon in a superposition of vertical and horizontal polarization. QTTT spooky markers exist in two separate locations on the game board, representing their state as a superposition state of two classical TTT markers.

---

[4]http://qttt.rohanp.xyz/

Measurement

When measuring the state of a quantum system, the quantum state of a system collapses and only one classical state is observed with some probability. In QTTT, the rule of creating the loop forces players to collapse their markers (measure their quantum state). In this case the player decides how to collapse the markers, which corresponds to the scientist choosing the way of measuring quantum system, such as axis orientation. The rule of forcing the measurement when the loop is created does not have exact corresponding physical meaning. Quantum systems can exist in a superposition state for an extended time, and the measurement is not forced, but chosen by the observer.

Entanglement

Entanglement is the quantum phenomenon of creating two or more particles, whose states cannot be described separately, but have some correlation even when they are separated by a significant distance. When measuring the state of one of the entangled particles, the state of the other particle can be known even without measurement. Einstein called it "spooky action at a distance." When the players collapse their states after creating a loop in QTTT, they know for sure in which state each marker would collapse into.

10.4 ● Schrödinger's Worm Using Five Qubits

Getting Started

- **Objectives:** Design, build, and test quantum circuits that model systems in superposition and entanglement.

- **Setup:** Open the IBM Q simulator[5] and start a new experiment.
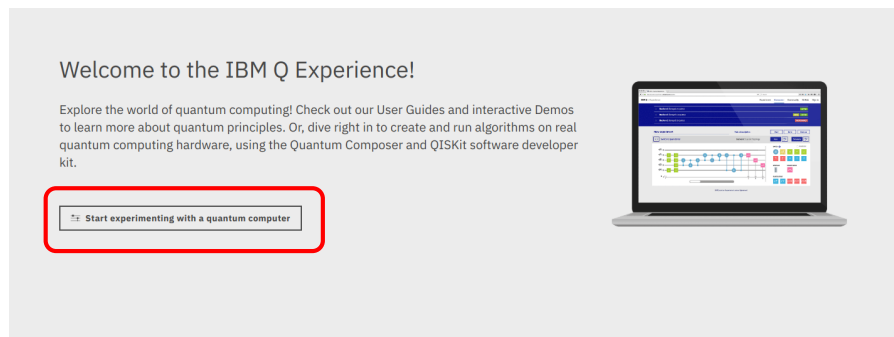
Figure 10.10: Select "Start experimenting with a quantum computer." Reprint Courtesy of International Business Machines Corporation, ©International Business Machines Corporation.
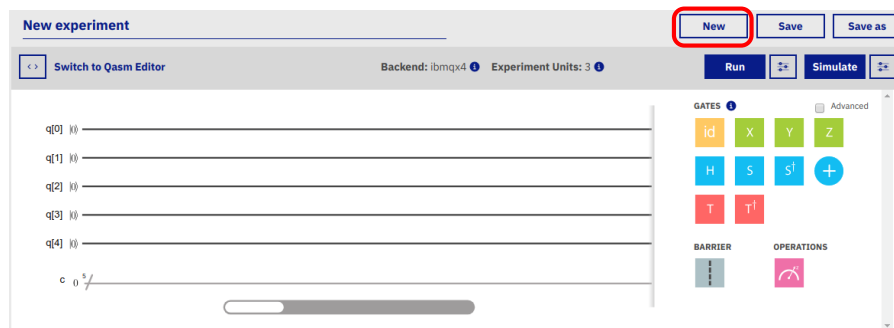

Figure 10.11: Select "New" option at top right. Reprint Courtesy of International Business Machines Corporation, ©International Business Machines Corporation.

Choose the "Custom Topology" backend with the default 5-qubit setting to enable unrestricted gate placements.

---

[5]https://quantumexperience.ng.bluemix.net/qx
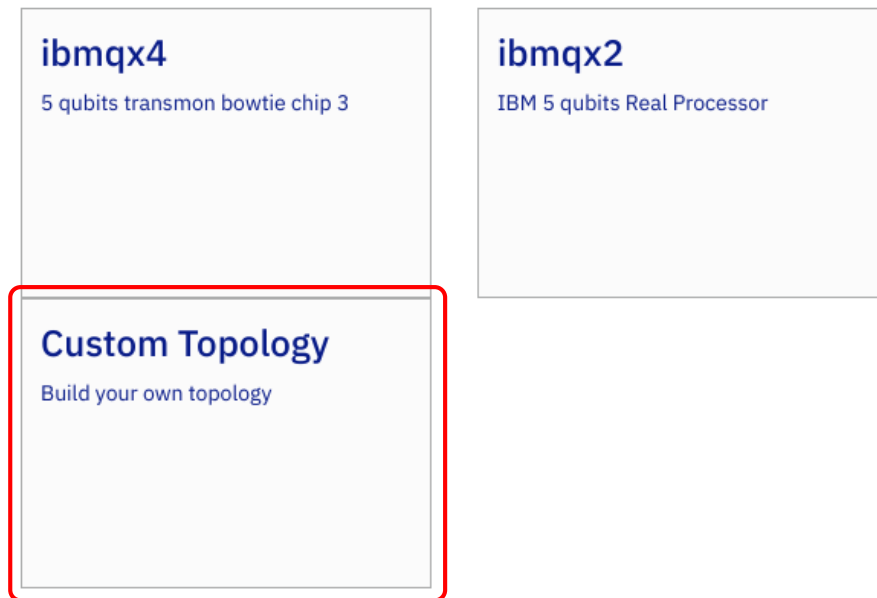
Figure 10.12: Select "Custom Topology" option at the bottom left. Reprint Courtesy of International Business Machines Corporation, ©International Business Machines Corporation.

Part I: Superposition

The worm is alive when all five squares are black and dead when only four are black. Use a 0 to represent a white square and 1 to represent a black square.
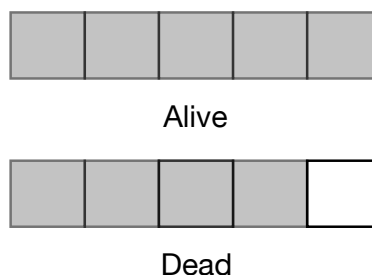
Alive

Dead

Figure 10.13: Dead or alive worms.

1. What is the classical state of the live 5-bit worm?

2. What is the classical state of the dead 5-bit worm?

3. Use IBM Q to create a worm in a superposition state of alive and dead. Let q[0] correspond to the bit on the far right.

4. Run the simulation and interpret the histogram.

5. How can you modify the circuit so that the worm is first put in a superposition state and then brought to life?

6. How can you modify the circuit so that the worm in a superposition state becomes definitely dead?

Part II: Entanglement
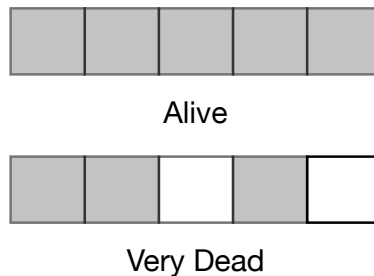
Figure 10.14: Very dead or alive worms.

The worm is next to a hungry bird such that it is either alive or chomped to pieces.

1. What is the classical state of the very dead worm?

2. Create a circuit that produces a worm in a superposition state of alive and very dead. (Hint: Two of the qubits are entangled.)

3. Run the simulation and interpret the histogram.

4. How can you modify the circuit so that the worm in a superposition state becomes either definitely dead or definitely alive?

Answers

Part I: Superposition

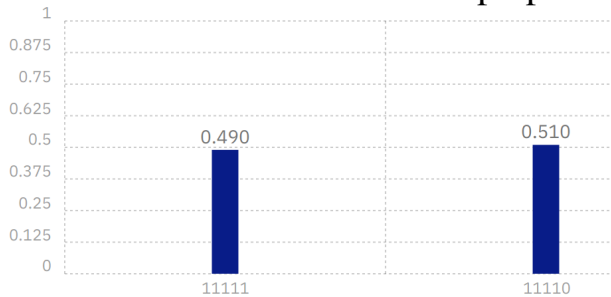1. $|11111\rangle$

2. $|11110\rangle$
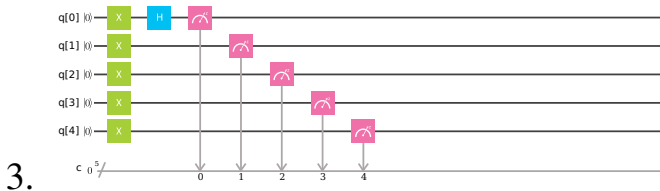
3.

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.
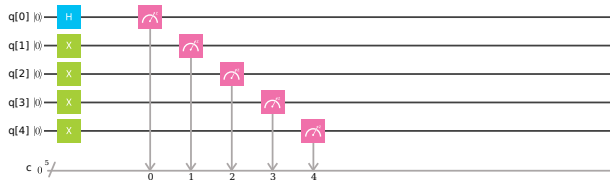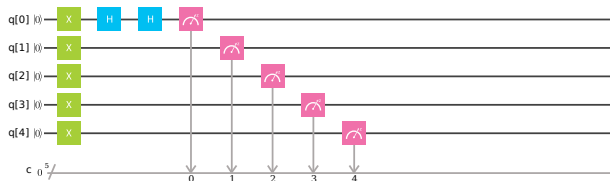

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

4. The histogram shows about 50/50% chances of both measurements: 11111 and 11110. The worm is in a superposition of the dead and alive states.
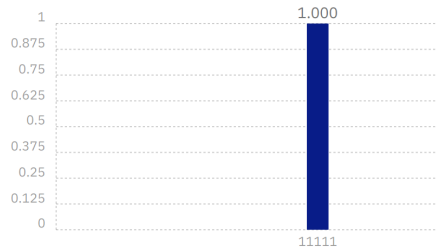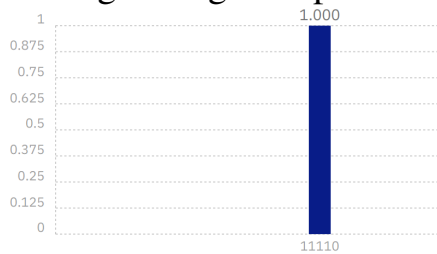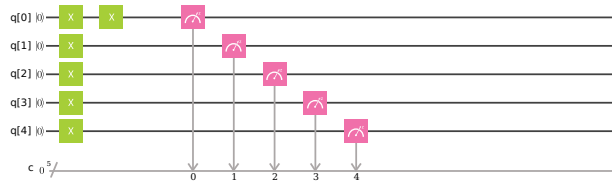

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

5. Adding a second Hadamard gate undoes the superposition.

6. Adding an X gate flips the bit.

Part II: Entanglement

1. $|11110\rangle$

2. A CNOT gate is used to entangle the two qubits such that they are either both white or both black.

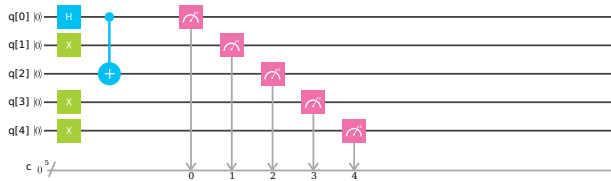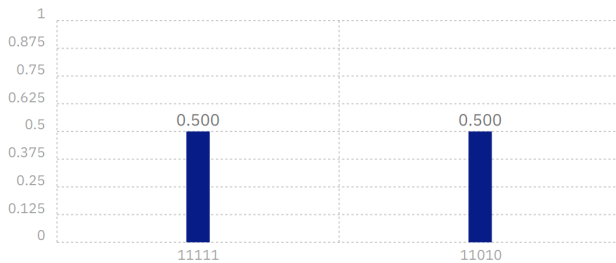Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

3. 50% chance of alive and 50% chance of very dead

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

4. Adding a second CNOT undoes the entanglement.

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.
Adding a second Hadamard undoes the superposition.

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.
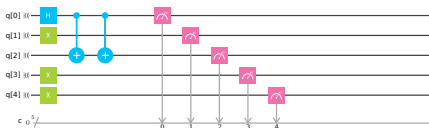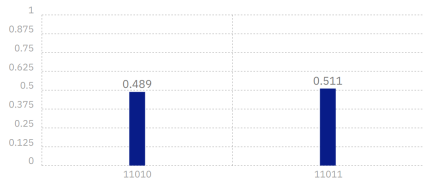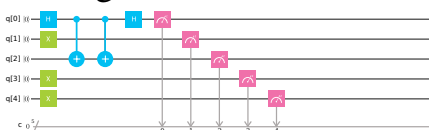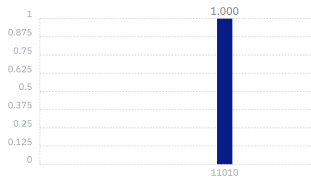

Reprint Courtesy of International Business Machines Corporation, © International Business Machines Corporation.

10.5 ◆ Superposition vs. Mixed States Lab

Objectives:

- Experimentally determine the difference between particles in a **superposition state** and a **mixed state** using the superposition states and mixed states simulator.[6]

- Apply the idea of basis changing to explain the experimental results.

- Compute the probability amplitudes given measurement results.

Questions:

1. We send 100 electrons of unknown spin into a Stern-Gerlach apparatus. We measure that 50 are spin up and 50 are spin down. We can conclude that:

   a) 100 electrons were in a 50/50 superposition state of up and down (superposition state).

   b) The electrons were a mixture of 50 electrons spin up and 50 spin down (mixed state).

   c) Not enough information

2. Use the simulator to compare the measurement outcomes of the mixed particles vs. the superposition particles. What are the similarities and differences?

---

[6]https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/superposition/superposition-mixed-states.html

Superposition states and mixed states

Input particles

Introduction   Orientation of SGA: ○ x   ● z

Input particles

● $|\uparrow\rangle$ Spin state with $S_z = +\hbar/2$

○ $|\downarrow\rangle$ Spin state with $S_z = -\hbar/2$

○ 50% $|\uparrow\rangle$, 50% $|\downarrow\rangle$ **Mixture**

○ $1/\sqrt{2}$ ($|\uparrow\rangle$ +$|\downarrow\rangle$)   **Superposition**

○ Superposition or mixture?
                              Hint

○ Superposition or mixture??

Display controls

☐ Show probabilities

☐ Show probability histogram

Main controls
Send particles through the SGA
Take more measurements
Single particle

Continuous stream of particles

Fast forward 100 particles

Figure reproduced from the QuVis website, licensed under creative commons
CC-BY-NC-SA.

3. By making a basis change with $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$ and $|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$, can you explain the similarities and differences mathematically?

4. Which of the two inputs labelled "Superposition or mixture?" and "Superposition or mixture??" is a random mixture and which is a superposition?

5. The mixture consists of a fraction A of spin up particles and a fraction B of spin down particles. Find these fractions, A and B.

6. The superposition state can be written as $\alpha|0\rangle + \beta|1\rangle$. Find the amplitudes α and β assuming they are real and positive.

7. Use a basis change to show that the amplitudes α and β give the correct probabilities in both the x- and z- basis.

Answers

1. C. The output is indistinguishable in the z-basis

2. Superposition particles always have the same measurement outcome in the x-basis, while mixed particles have random spins in the x-basis.

3. Changing the superposition state from the z- to x-basis:

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

   so only $+x$ will be measured. Whereas in a mix of $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$ and $|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$, both $+x$ and $-x$ will be measured with 50/50 probability.

4. ? is the mixture since the x-basis measurements are 50/50, showing no correlation.

5. In the z-basis, we measure about 20% spin up and 80% spin down. Thus, $A = \frac{1}{5}$ and $B = \frac{4}{5}$.

6. In the z-basis, we measure about 20% spin up and 80% spin down. The probabilities are $\frac{1}{5}$ and $\frac{4}{5}$, but the amplitudes are the square root of the probability: $\alpha = \frac{1}{\sqrt{5}}$ and $\beta = \frac{2}{\sqrt{5}}$.

7. Changing the superposition state from the z to x-basis:

$$\alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{5}}\left(\frac{1}{\sqrt{2}}|-\rangle\right) + \frac{2}{\sqrt{5}}\left(\frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\right) = \frac{3}{\sqrt{10}}|+\rangle - \frac{1}{\sqrt{10}}|-\rangle,$$

   By squaring the amplitudes, we find 90% probability of $+x$ and 10% probability of $-x$.

10.6 ■ Measurement Basis Lab

Objectives

- Use the PHET Stern-Gerlach Simulator[7] to see how changing the orientation of the Stern-Gerlach Apparatus (SGA) affects the spin measurement.

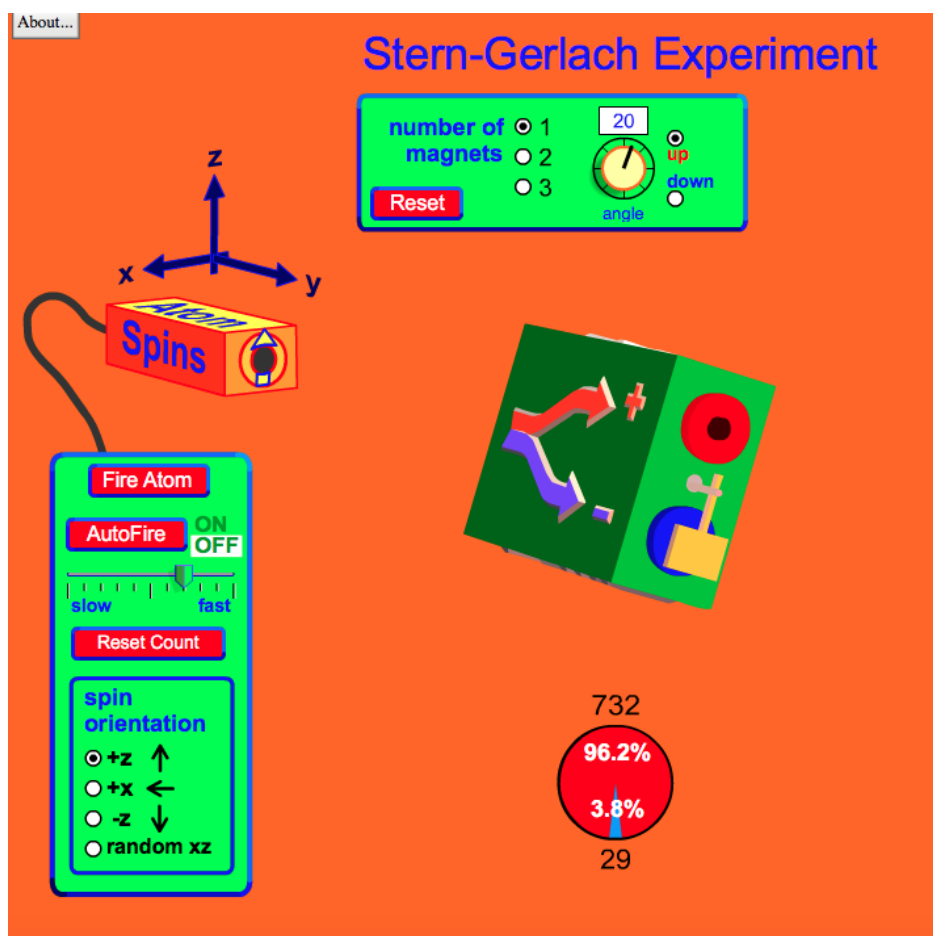- Perform calculations to write the spin in a different measurement basis.

Figure 10.15: Figure reproduced from the PHET Stern-Gerlach Simulator website, licensed under creative commons CC-BY.

---

[7]https://phet.colorado.edu/sims/stern-gerlach/stern-gerlach_en.html

Angle of SGA (θ_{SGA})	Probability of going through	Probability of being blocked
0°		
15°		
30°		
45°		
60°		
75°		
90°		
105°		
120°		
135°		
150°		
165°		
180°		

Questions

1. Send spin up electrons through a single SGA and record the measurement probabilities for different SGA angles.

2. Generate a scatter plot of the data.

3. What function describes the shape of the graph?

4. Write the state of the spin up electron as a superposition for an arbitrary SGA angle (θ_{SGA}). In other words, find α and β in $|\text{electron}\rangle = \alpha|\text{goes through}\rangle + \beta|\text{blocked}\rangle$. The diagram below may help, but note that $\theta \neq \theta_{SGA}$.
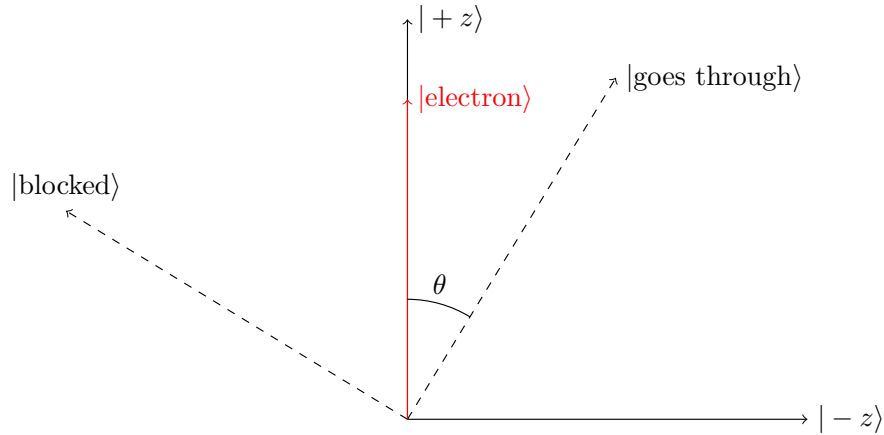
5. Do the theoretical probabilities match the simulated data?

Supplemental Questions

6. What would your scatter plot look like if you sent electrons through with the random *xz* spin option?

7. What is the theoretical probability of spin down electrons passing through a SGA angled at 45°?

8. What is the theoretical probability of spin +*x* electrons passing through a SGA angled at 45°?

Answers

2. Sample Data:
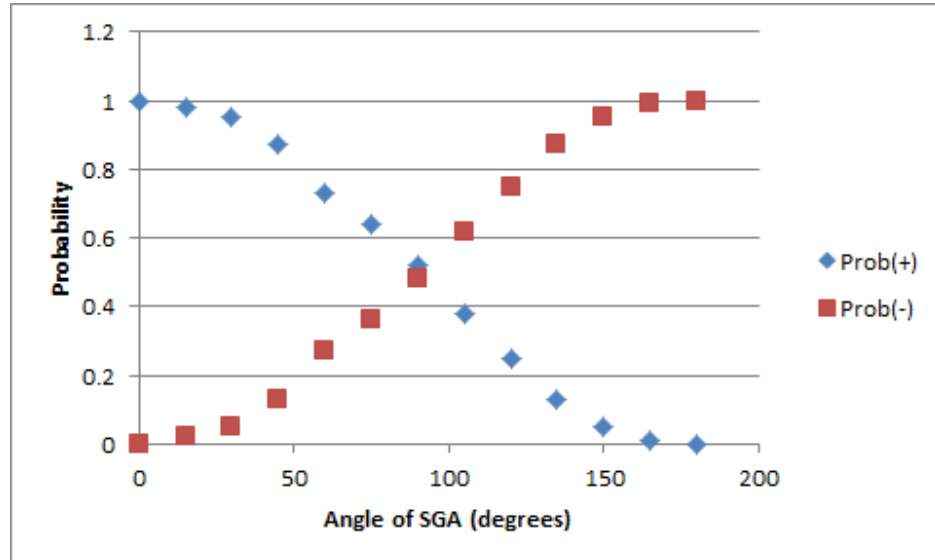
3. Cosine squared function

4. $\alpha = \cos\theta = \cos\frac{\theta_{SGA}}{2}, \quad \beta = \sin\frac{\theta_{SGA}}{2}$

6. 50/50 probability independent of angle. The graph would be constant at Probability=0.5.

7. Opposite of the probabaility for the spin up electron, so $1 - \cos^2(22.5°) = 0.146$.

8. $\sin^2(22.5°) = 0.146$

10.7 ● One-Time Pad (Alice)

Character	Binary Code
A	01000001
B	01000010
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111
P	01010000
Q	01010001
R	01010010
S	01010011
T	01010100
U	01010101
V	01010110
W	01010111
X	01011000
Y	01011001
Z	01011010

Table 10.1: One-time pad (Alice).

Before parting ways, you and Bob agree on a key. Using a coin with heads $= 0$ and tails $= 1$, randomly generate a key of the same length as the message. Make sure that you and Bob have the same key.

Shared Key:

Encoding:

1. Choose a secret letter to send to Bob in binary. Message:

2. Add the key to your message, bit by bit, to encode the message. In binary, $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, and $1 + 1 = 0$. For example, if the key $= 0110$ and the message $= 1101$, then the cipher text $= 0011$, as $0110 + 0101 = 0011$.

Cipher Text:

3. Send the cipher text to Bob.

Decoding

1. Write down the cipher received from Bob.

Cipher from Bob								
Shared Key								

2. Add the key to Bob's message, bit by bit, to decode the message.

Decoded Message							

3. What was the message?

Eavesdropping

1. Swap cipher texts with another group. How could you recover the original message?

2. How many different keys would you need to try?

3. If the original message had five letters instead of one letter, how many different keys would you need to try?

4. You intercept a five letter message and, by chance, find a key that decrypts it to read HELLO. What other words could it possibly be?

Questions

1. Why does adding the key to the cipher recover the original message?

2. Why is the one-time pad theoretically unbreakable?

3. What is the practical security flaw in the one-time pad?

10.8 ● One-Time Pad (Bob)

Character	Binary Code
A	01000001
B	01000010
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111
P	01010000
Q	01010001
R	01010010
S	01010011
T	01010100
U	01010101
V	01010110
W	01010111
X	01011000
Y	01011001
Z	01011010

Table 10.2: One-time pad (Bob).

Before parting ways, you and Alice agree on a key. Using a coin with heads $= 0$ and tails $= 1$, randomly generate a key of the same length as the message. Make sure that you and Alice have the same key.

Shared Key:

Encoding:

1. Choose a secret letter to send to Alice in binary. Message:

2. Add the key to your message, bit by bit, to encode the message. In binary, $0+0=0$, $0+1=1+0=1$, and $1+1=0$. For example, if the key $= 0110$ and the message $= 1101$, then the cipher text $= 0011$. $0110+0101=0011$.

Cipher Text:

3. Send the cipher text to Alice.

Decoding

1. Write down the cipher received from Alice.

Cipher from Alice								
Shared Key								

2. Add the key to Alice's message, bit by bit, to decode the message.

Decoded Message								

3. What was the message?

Eavesdropping

1. Swap cipher texts with another group. How could you recover the original message?

2. How many different keys would you need to try?

3. If the original message had five letters instead of one letter, how many different keys would you need to try?

4. You intercept a five-letter message and, by chance, find a key that decrypts it to read HELLO. What other words could it possibly be?

Questions

1. Why does adding the key to the cipher recover the original message?

2. Why is the one-time pad theoretically unbreakable?

3. What is the practical security flaw in the one-time pad?

10.9 ● BB84 Quantum Key Distribution (Alice)

No Eavesdropper

1. Randomly choose to prepare the electron in either the *x*- or *z*-basis.

2. The electron that's sent through your Stern-Gerlach apparatus will either be in a 0 or 1 state. You can randomize this by flipping a coin.

3. Pass the correct spin card to Bob face down.

$$\uparrow \ = 0 \qquad \downarrow \ = 1$$

$$\leftarrow \ = 0 \qquad \longrightarrow \ = 1$$
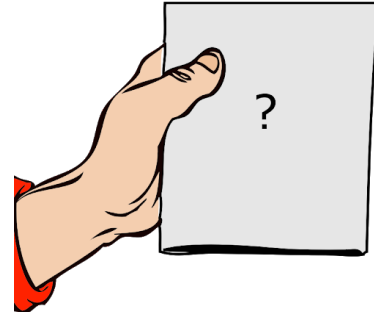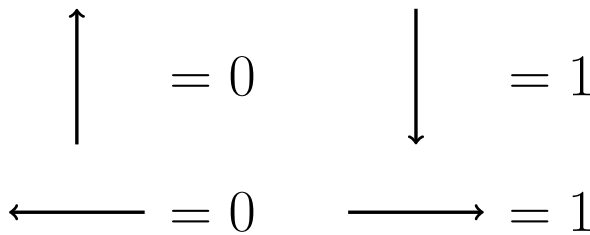
4. Once you have filled up the chart, tell Bob the basis used for each bit. If Bob tells you to "discard" the bit, cross it out on your chart.

5. Check to see that you and Bob end up with the same sifted key.

Basis: *x* or *z*								
Bit Value: 0 or 1								

SIFTED KEY: _____

With Eavesdropper

1. Repeat the procedure, but instead of passing the spin card directly to Bob, it will first pass through Eve.

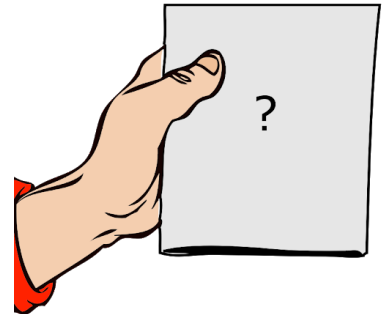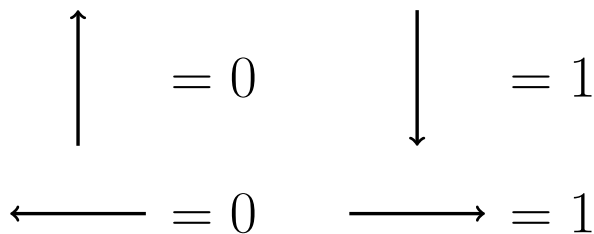2. Compare the sifted key bits one at a time. How can you tell if Eve intercepted the message?

SIFTED KEY: _____

Basis: x or z							
Bit Value: 0 or 1							

10.10 ● BB84 Quantum Key Distribution (Bob)

No Eavesdropper

1. Randomly choose between the *x*- or *z*-basis.

2. Receive the spin card from Alice and flip it over.

   - If your basis is the same as the card's, record the bit value.
   - If your basis is different, the output of your Stern-Gerlach apparatus will be random. Randomly pick 0 or 1.

$$\uparrow \quad = 0 \qquad \downarrow \quad = 1$$

$$\longleftarrow \quad = 0 \qquad \longrightarrow \quad = 1$$

3. Once you have filled up the chart, Alice will tell you the basis used for each bit. If you measured in a different basis, tell Alice to "discard" the bit and cross it out on your chart.

4. Check to see that you and Alice end up with the same sifted key.

Basis: *x* or *z*								
Bit Value: 0 or 1								

SIFTED KEY: _____

With Eavesdropper

1. Repeat the procedure, but instead of getting the spin card directly from Alice, it will first pass through Eve.

2. Compare the sifted key bits one at a time. How can you tell if Eve intercepted the message?

SIFTED KEY: _____

Basis: x or z							
Bit Value: 0 or 1							

10.11 ● BB84 Quantum Key Distribution (Eve)

<u>With Eavesdropper (You!)</u>

1. Randomly choose between the x- or z-basis.

2. Receive the spin card from Alice and flip it over.

   - If your basis is the same as the card's, record the bit value and pass it along to Bob.
   - If your basis is different, the output of your Stern-Gerlach apparatus will be random. Randomly pick a spin in your new basis, record the bit value, and pass it along to Bob.

3. Listen in as Alice and Bob compare their basis. If Bob says to "discard" the bit, cross it out on your chart.

4. Compare your sifted key to Alice and Bob's key. Was your eavesdropping successful?

SIFTED KEY: _____

Basis: x or z								
Bit Value: 0 or 1								

Acknowledgments

It is a pleasure to thank Marge Bardeen, Harry Cheung, and Spencer Pasero for helpful discussions on various aspects of this project, from inception to completion. We are grateful to Daniel Carney, William Jay, Yin Lin, Jim Simone, Julia Stadler and Anders Ellers Thomsen for reading and providing feedback on the draft document. It is also a pleasure to thank LaMargo Gill for her remarkably thorough proofreading of this document. We thank Heath O'Connell and Aaron Sauers for their useful advice regarding information content. We thank Olivia Vizcarra and the Fermilab theory group for facilitating this project.

Various sources were used as inspiration for building this course. We acknowledge IBM Q experience[8] for their useful web interface, and note that specific figures (as indicated in their captions) are owned by IBM as per their end-user license agreement.[9] We urge the reader to review this end-user license agreement before using the IBM Q web interface. Additionally, we would like to attribute the PhET Interactive Simulations for their useful interactive videos, and as per their license also acknowledge the University of Colorado Boulder and https://phet.colorado.edu. Furthermore, we credit the Quantum Mechanics Visualization Project (QuVis)[10], hosted by the University of St. Andrews, for useful interactive simulations. Finally, we thank Martin Laforest and the Communications and Strategic Initiatives Team at the Institute for Quantum Computing, University of Waterloo's outreach department[11] for supplying material which formed the inspiration for Chapters 3, 5 and 9 of this module.

---

[8]https://quantumexperience.ng.bluemix.net/qx

[9]https://quantumexperience.ng.bluemix.net/qx/terms

[10]https://www.st-andrews.ac.uk/physics/quvis/

[11]https://uwaterloo.ca/institute-for-quantum-computing/outreach