

A Quantum of Quantum Computing

Cora Barrett
Om Joshi
Hyo Sun Park
Ági Villányi
Matt Yeh

IAP 2025: MIT Quantum Winter School

Contents

Introduction	4
Superposition	6
Quantum vs. Classical Objects	6
Quantum Mechanics for Computation: DiVincenzo's Criteria	11
The Qubit	12
A Physical Qubit	15
BB84 Protocol for Quantum Key Distribution	21

Introduction

Quantum Computation. For thousands of years, humans have developed tools to aid in calculations. The abacus enabled people in the ancient world to count. In the 20th century, mathematicians and scientists formalized complex calculations under the concept of computation and built the first “useful” computers capable of more than simple addition and subtraction. The invention of the personal computer brought computational power to our fingertips, and today we are uncovering its vast potential to exceed human intelligence through artificial intelligence and machine learning. All of this is made possible by the physics of transistors, rooted in the fundamental laws of electricity and magnetism.

Despite their power, these “classical” computations are believed to have fundamental limits. For example, how can we simulate physical systems at the atomic level, which involve an exponential number of degrees of freedom? How can we address problems that lie beyond the capabilities of classical computers? Harnessing quantum mechanics for computation may provide the answer.

Quantum mechanics reveals a world that is difficult to perceive directly. The challenge of quantum computation lies in developing methods to leverage the unique properties of this quantum world as resources for solving complex computational problems. This is no easy task. Quantum mechanics, as you’ll discover throughout this course, defies intuition. The behavior of atoms does not align with the logic of our everyday experience, making it difficult to design them into computational devices. Nevertheless, many core engineering principles, such as finite control, scalability, and fault tolerance, remain relevant in the quantum realm. This makes the task of building quantum devices challenging but well-defined.

As we move “up the stack” from the physics of quantum devices to the realm of computation, we encounter the concept of a model of computation. A model of computation is an abstract machine defined by its states and the transitions between those states. An algorithm is a specific set of state-transition rules that solves a particular computational problem. In the quantum realm, models of computation have unique characteristics compared to their classical counterparts. The most widely used model of quantum computation is the Circuit Model, which you will explore extensively during this course.

Quantum computation is a rapidly evolving field, with groundbreaking innovation happening in academia, industry, and government organiza-

tions. There has never been a better time to dive into quantum computing, and we're very excited to have you here!

Learning Goals This mini-course provides a concise introduction to quantum computing. The goal is not to make students experts in quantum mechanics or quantum information theory but to help them understand the fundamental differences between classical and quantum computation. It also aims to highlight the unique challenges involved in building computational devices based on quantum mechanics and to introduce various quantum architectures. By the end of the course, students will leave with a "quantum of knowledge," which we hope will inspire them to further explore quantum computing through research and advanced coursework. The material in this textbook will be delivered through lectures and problem-solving sessions.

Outline The textbook—and this course—are divided into four sections: Superposition, Interference, Entanglement, and Applications. The first three days each focus on a specific quantum resource, exploring how that resource can be utilized for quantum computation. The final day provides an introduction to quantum algorithms and an overview of quantum error correction.

Superposition

You have to be careful.

-Mikhail Lukin, *Lectures on The Physics of Quantum Information*

This section focuses on superposition, which is a fundamental phenomenon in quantum mechanics and is a key resource for obtaining quantum advantage. Measurement is also introduced.

Quantum vs. Classical Objects

When you toss a football around with a friend, you are a direct witness to classical mechanics. Newton's equations of motion describe your every move. Arguably, these dynamics are intuitive: you can see the football, you can easily set the initial conditions of the throw by adjusting your shoulder and elbow and you can run to catch the ball if your partner's throw is a bit off the optimal trajectory. We experience the macroscopic world first-hand which means we can make sense of it through direct observation.

This applies to many areas of mechanics: the laws which govern a game of catch take on a distinct flavor when describing electricity and magnetism, for example, or when deriving the elliptical orbit of our planet around the sun. But our intuition is transferrable. Given the initial position and momentum of the system and all of the forces acting on the system, the final position and momentum can be predicted with certainty – whether the object is a tennis ball flying through the air, a cylinder rolling down a ramp or the Moon circling the Earth.

This intuition begins to diminish as you scale down the size of the object in motion to the atomic scale. At this scale, an analogue of a football or planet is an electron or photon or, more generally, a *quantum particle*. A quantum particle is any physical object which experiences the world according to quantum mechanics, which are a set of rules that have been discovered to accurately describe experimental observations of the atomic world. Quantum mechanics differs substantially from classical mechanics, with many beautifully weird phenomena often called “quantum effects”. But, in the limit of large objects, quantum mechanics in fact *becomes* classical mechanics. That is, classical mechanics can actually be derived from quantum mechanics! In this section, we will learn about some of the early observations physicists made that led to the discovery of quantum mechanics, as well as introduce three quantum principles: superposition, the uncertainty principle, and measurement.

A Brief History of Quantum Mechanics

Quantum mechanics evolved from a series of unexplainable experimental observations. The story begins in 1900, when Max Planck derived a formula for blackbody radiation by realizing that energy can only be emitted or absorbed in discrete integral multiples of some base unit of energy, which are called quanta. The classical theory was not reflecting experimental evidence, and therefore calculating the *blackbody curve* remained a major open problem, until Planck's insight. The idea that the energy of a physical object is not continuous, but rather is 'quantized' was revolutionary and formed some of the earliest insights into quantum mechanics. Later on in 1905, Albert Einstein proposed that certain materials, when shot at with light of sufficient energy, emitted electrons through a process called *photoemission*. He theorized that this was because light consists of individual energy packets, called photons, rather than being a continuous wave. As these interesting results began to emerge, a formal model for the structure of an atom was greatly sought after. In 1913, Niels Bohr described a new theory for the structure of the Hydrogen atom, which consists of a positively charged nucleus surrounded by a negatively charged electron cloud that comprised of *orbitals* which each correspond to discrete energy levels. This theory was later confirmed experimentally in 1922 by the Stern-Gerlach experiment, which is detailed below. Later that decade, physicists began to develop a formal theory for quantum mechanics. 1926, Schrödinger derived the Wave Equation, which formalized how quantum systems evolve through time and in 1927, Heisenberg stated the uncertainty principle, which says that a particle's position and momentum cannot both be known with certainty. The rest of the 20th century saw progress in both the theoretical and experimental verification of entanglement, and finally in 1981 Richard Feynman proposed that quantum mechanics could be harnessed for computation, potentially aiding in the simulation of quantum systems. And that was the birth of quantum computation.

The Stern-Gerlach Experiment

One of the first pieces of experimental evidence that our universe behaves in a "quantum" way was the trajectory of silver atoms bending under the influence of a nonuniform magnetic field. A foundational result which you may have derived in an electricity and magnetism course is that a nonuniform magnetic field deflects a magnetic dipole (i.e. a tiny magnet). The force on the dipole depends on the overlap of the magnetic dipole moment

with the magnetic field (i.e. dot product).

Many quantum objects act like magnetic dipoles due to intrinsic properties such as *spin* and *angular momentum*. We can think of a silver atom, which has non-zero angular momentum, as a magnetic dipole. A silver atom traveling in a nonuniform magnetic field will therefore be deflected. The amount of deflection depends upon the orientation of the dipole with respect to the magnetic field. If the dipole moment is perpendicular to the magnetic field, the deflection will be zero. If the dipole moment is aligned or anti-aligned with the magnetic field, the magnitude of the deflection will be maximal. For partial (anti-)alignment, the deflection will be somewhere in between.

Stern-Gerlach Experiment

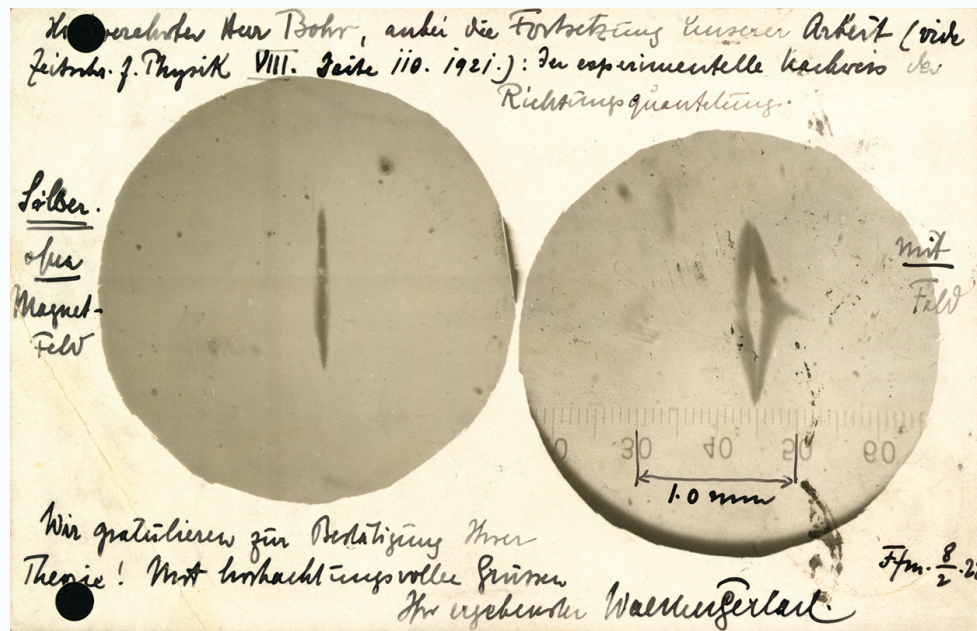


Fig. 1. Walther Gerlach sent this postcard to Niels Bohr, which says in German: “Attached is the experimental proof of spatial quantization (silver without and with field). We congratulate you on the confirmation of your theory.”.

In 1913, Niels Bohr predicted that the magnetic moment is quantized. In other words, the magnetic moment for an electron or a silver atom cannot be in an arbitrary orientation. Nine years later, in 1922, Otto Stern and Walter Gerlach performed a landmark experiment in the history of physics, which

is now referred to as the Stern-Gerlach experiment.

In the Stern-Gerlach experiment, they shot silver atoms through a nonuniform magnetic field. Classically, we would expect that the silver atom's magnetic moment could be anywhere from fully aligned to fully anti-aligned with the field, and there would be a distribution of silver atoms at all possible amounts of deflection. But instead, they observed that the silver atoms deflected only maximally up or down, indicating that the silver atom's magnetic moment could only be fully (anti-)aligned with the field. Niels Bohr was right — magnetic moments are indeed quantized.

The Wave Equation and Schrodinger

God does not play dice with the universe.

-Albert Einstein, in a letter to Max Born in 1926

Quantum objects do not have definite properties prior to measurement, even though we always find a single result when we perform a measurement. For instance, prior to measurement, an electron exists in a superposition of different locations. When we measure the electron's location, however, we find it to be in only one exact location. Essentially, before measuring an observable quantity like position or spin, we can only know the relative probabilities of each possible measurement outcome.

This probabilistic nature of measurement flies in the face of our intuition. It did not sit well with Einstein either, who initially was skeptical of quantum mechanics. Even though quantum theory describes the behavior of our universe on the smallest scales, the time evolution of quantum systems is not completely random like throwing dice. Similarly to how the motion of a football evolves deterministically with time, a quantum object also evolves deterministically with time in another sense.

Schrödinger Equation

Equation 1. For a quantum system with wavefunction $|\psi\rangle$ and Hamiltonian H , the wavefunction evolves according to

$$i\hbar \frac{d}{dt} |\psi\rangle = H |\psi\rangle \quad (1)$$

For a given quantum system, we can encapsulate all possible measurement outcomes and their probabilities in a *wavefunction*, often denoted $|\psi\rangle$.

We say that measurement *collapses* the wave function, yielding only one exact value. A quantum system is described by a Hamiltonian — total energy operator — H . The wave function evolves deterministically with time, governed by the Schrödinger equation. So before measurement, the quantum system is not behaving randomly at all.

The Uncertainty Principle and Heisenberg

One way in which quantum mechanics differs from classical mechanics is that there is no longer such a thing as definite properties of observables. For example, a soccer ball has – at all times – a well-defined position and a well-defined momentum. The same cannot be said for an electron.

The Heisenberg uncertainty principle tells us that for two quantum mechanical operators (operators correspond to observables) which do not commute, the uncertainty must be above a certain threshold. For example, for position and momentum: $\Delta x \Delta p \geq \frac{\hbar}{2}$.

A classic joke which illustrates this principle goes as follows:

Heisenberg is driving on the highway when he gets pulled over by the police.

The officer comes up to the window and says, “Did you know you were going 90 miles per hour?”

Heisenberg says “Damnit, now I don’t know where I am!”

Polarization Measurement Collapse

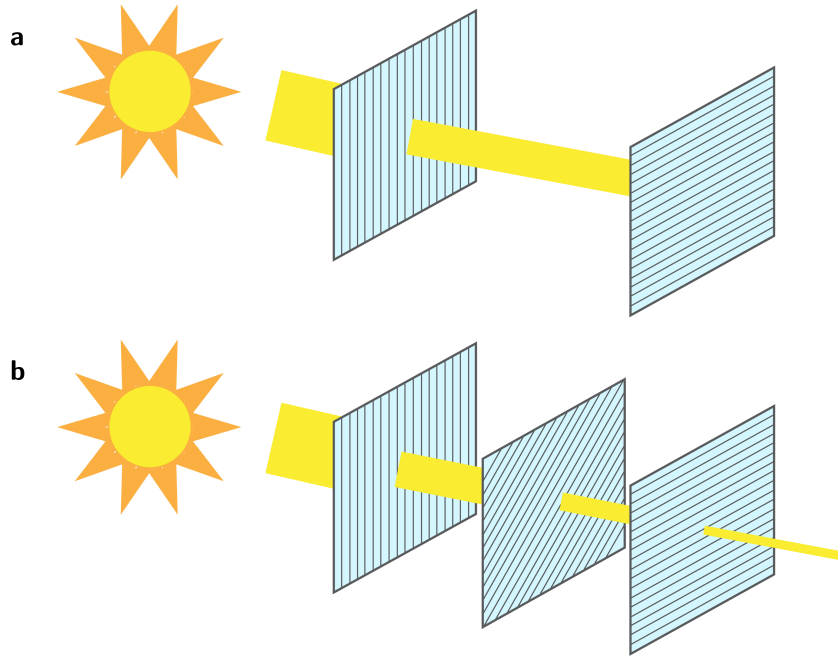


Fig. 2. A visual depiction of measurement based on the polarization of light.

Quantum Mechanics for Computation: DiVincenzo's Criteria

In the previous section, we introduced some of the physical differences between classical and quantum mechanics that played a vital role in the history of quantum mechanics. We mentioned that in 1981, Richard Feynman proposed that perhaps quantum mechanics could be used for computation. Over the next decade, modeling quantum computation both theoretically and physically building them became an exciting new challenge. As originally stated by David DiVincenzo in 1996, the conditions for constructing a useful quantum computer are as follows:

1. "The degrees of freedom required to hold data and perform computation should be available as dimensions of the Hilbert space of a quantum system."
2. "...It must be possible to place the quantum system in a fiducial starting quantum state."

3. "The quantum system to be used as a quantum computer must be to a high degree isolated from coupling to its environment. This isolation requirement is linked up with the precision required in quantum computation."
4. "It must be possible to subject the quantum system to a controlled sequence of unitary transformations. All of our quantum algorithms are expressed in terms of such sequences."
5. "...It is necessary that it be possible to subject the quantum system to a "strong" form of measurement."

These criteria are commonly summarized even more succinctly:

1. (Scalable qubits) The physical implementation should be scalable and have a well-defined qubit.
2. (Initialization) The qubits should be initializable to a well-defined state, typically $|0\rangle^{\otimes N}$.
3. (Coherence) The decoherence times (i.e., how long it takes for the qubit system to lose its "quantumness") should be long relevant to the gate times.
4. (Universality) The quantum gates available should be able to construct any possible unitary transformation on the qubit system.
5. (Measurement) The physical implementation should have the capability for projective qubit measurement.

The Qubit

In this section, we will begin to explore the first item in DiVincenzo's criteria: The Qubit. This section will give a more mathematical and computer science perspective, while the following section will give a physical perspective.

To specify a computation, we first need to define a *model of computation*, which is a set of rules that abstract away the physical device that is executing the computations. Some common models of computation that you may have already encountered are finite automata, Turing machines, the RAM model, or pointer machines. In general, a model of computation consists of defining the *states* of the system (that is, the form that each intermediate

step of the computation takes) and *transitions* between them (that is, how to get from one state to the next). In this section, we will define a *qubit*, which describes the simplest type of quantum state. This is the first step in defining a complete model of quantum computation, which we will gradually build-up to over the next few days.

We will first define a qubit formally, and then carefully explore all of its parts in detail, providing the necessary mathematical background as we go. In particular, we will explain the strange angle brackets used in the definition, $|\cdot\rangle$, which is called *Dirac* or *braket* notation.

A Qubit

Definition 2. For $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$, a qubit is a vector $|\psi\rangle \in \mathbb{C}^2$ that takes the following form:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2)$$

Let's now dive-in to understanding this definition. First, we will describe the notation. The angular brackets $|\cdot\rangle$ denote a column vector. Although it may seem unnecessary, this short-hand will prove to be extremely helpful later on for making calculations more succinct. For example, $|0\rangle$ in the above definition corresponds to the column vector $(1, 0)^T$. That is:

$$\begin{aligned} |0\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned} \quad (3)$$

Therefore, another way of writing $|\psi\rangle$ in Definition 2 is:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (4)$$

In later lectures, we will describe special properties of quantum states that can be defined using Dirac notation. For now, the above understanding is sufficient. We will now go through a small tutorial on vectors and complex numbers.

A vector is a mathematical object that is specified by a magnitude and a direction. For example, an element (a, b) in \mathbb{R}^2 can be made into a vector by thinking about it as an *arrow* rather than a *point*.¹ Vectors may also

¹The notation \mathbb{R}^2 denotes the Real numbers with dimension 2. The reader can think of

be defined using complex entries, as is the case in Definition 2. Complex numbers were discovered to deal with the previously undefined value of $\sqrt{-1}$. A complex number, $\alpha \in \mathbb{C}$, is specified by two real numbers $a, b \in \mathbb{R}$ and is written as $\alpha = a + b \cdot i$, where $i = \sqrt{-1}$. Its magnitude, denoted by $|\cdot|$, is defined as: $|\alpha| = \sqrt{a^2 + b^2}$. For a more complete overview of vectors and complex numbers with some great exercises, we refer the reader to Chapter 1 of [Ax15].

Importantly, Definition 2 specifies the condition that $|\alpha|^2 + |\beta|^2 = 1$, that is, quantum states are always normalized.

Examples of Quantum States

A classical bit is a scalar quantity $b \in \{0, 1\}$. It is the basic unit of classical computation and specifies the simplest type of *state* in most models of classical computation. It is possible to encode a classical bit b into a quantum state $|\psi\rangle$ by setting $\alpha_b = 1$. For example, the following is an encoding of the bit $b = 0$ as a quantum state:

$$|\psi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (5)$$

And the following is an encoding of the bit $b = 1$ as a quantum state:

$$|\psi\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (6)$$

Note that these are both valid quantum states because $|\alpha|^2 + |\beta|^2 = 1$. Another common quantum state is when the state corresponding to $\alpha = \beta = 1/\sqrt{2}$, commonly denoted by $|+\rangle$:

$$|+\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \quad (7)$$

Bloch Circle.

The Bloch sphere is a geometric visualization of a single qubit quantum state, and will be covered in the next lecture. The Bloch circle is a "slice" of the Bloch sphere and represents

this as the 2-dimensional Cartesian plane.

Bloch Circle

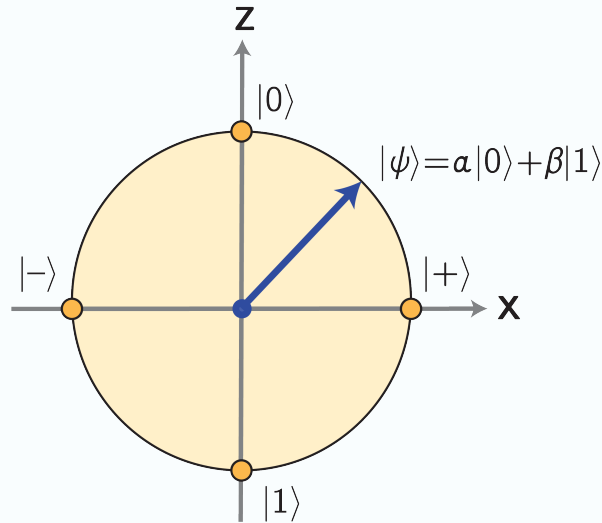


Fig. 3. This is a "slice" of the Bloch sphere, which we will learn about on day 2.

A Physical Qubit

Photon Polarization: A Visual Qubit

A photon is what makes my photon detector go "click".

-Peter Mosley, PhD Thesis

It might be surprising to some that light, a seemingly everyday presence, can be used as a qubit. In fact, light, or more precisely electromagnetic radiation, was the original progenitor of quantum theory. It was the study of blackbody radiation, e.g. the spectrum of light emitted by a hot object, that originally broke down classical theories and led Max Planck to quantize energy with his celebrated constant "h bar" (\hbar):

$$E = \hbar\omega \quad (8)$$

Light is inescapable in our daily life. We see it when we open our eyes, feel it when we stand near a fire. But how can we describe light? If we were to look at a rainbow, we might say the color (or equivalently, the frequency

and wavelength) is the best descriptor. But if we were to just split a beam into two beams, maybe the path (spatial distribution) would be better. Put on a pair of polarized sunglasses, and now polarization (whatever that is) is best.

As the opening quote sardonically alludes to, it can be complicated to describe light completely. Even the sense of a “photon” is subtle. The name suggests a “quantum” of light, an indivisible unit. Clearly a photon is just one unit of these indivisible excitations. And yet, using “photon number” as our descriptor loses all the other possible degrees of freedom (What color is it? What shape does it occupy in space?).

Fine, we were just being sloppy. Properly, we should have said “one quantum of light of frequency ω with spatial profile $\psi(x)$ with polarization σ with ...” and so forth. But even this sense leads to confusion. Heisenberg says that frequency and time have an uncertainty relation. So if our photon really is a “single” frequency ω , it extends infinitely in time. Does that really make sense? A single quantum electromagnetic excitation that extends forever?

We will not dive deep into these subtleties in this short course. However, these kind of questions lie at the foundation of a rich field of study known as *quantum optics*. Indeed, the fact that light has so many degrees of freedom is often seen as an opportunity, a means to encode qubits in whatever degree of freedom is most convenient.

For illustrative purposes, we consider encoding the qubits in *polarization*. Think of each photon as a flying arrow [Fig. 4]. Polarization then is analogous to the orientation of the arrow fletching, defining an “orientation” of the oscillations of the electromagnetic field. The two qubit states can then be mapped to the “horizontal” (H) and “vertical” (V) orientations,

$$|H\rangle = |0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (9)$$

$$|V\rangle = |1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (10)$$

which conveniently correspond to the x and y axes of a 2D Cartesian plane. In this encoding, the quantum superposition of the polarization states very literally corresponds to the mathematical superposition of two Euclidean vectors!

Polarization conceptually

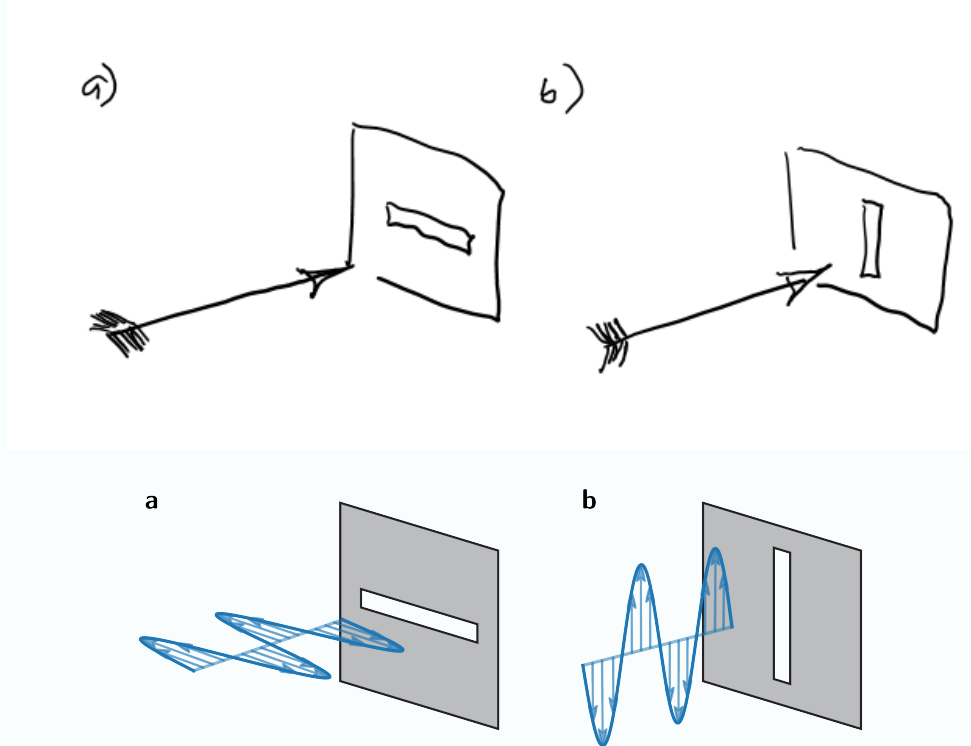


Fig. 4. Polarization refers to the orientation of the field oscillations, specifically of the electric field. Horizontal (H) and Vertical (V) polarization can be thought of as the orientation of fletching on an arrow, determining if the arrow (photon) can pass through a slit (polarizer).

Electromagnetic Waves

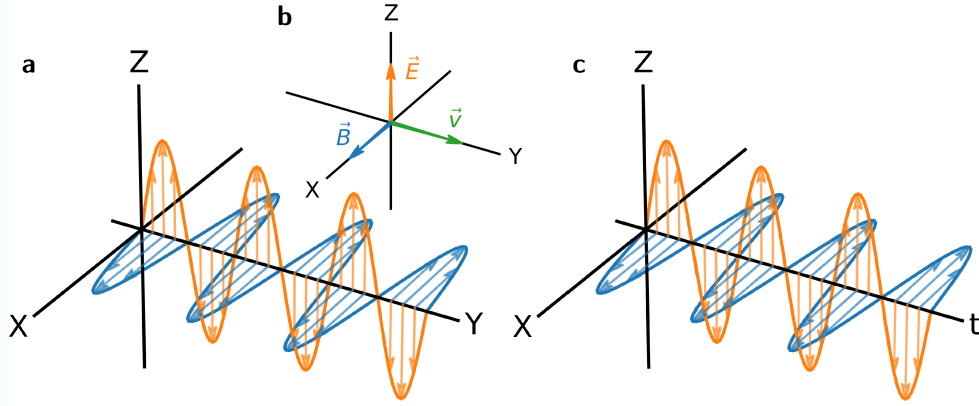


Fig. 5. Light (and single photons) are electromagnetic waves, comprised of oscillating electric (\vec{E}) and magnetic (\vec{B}) fields. **(a)** At a given point in time, the field oscillates in space. **(b)** The direction of propagation \vec{v} is determined by the cross product $\vec{E} \times \vec{B}$. **(c)** We can also think of the wave as oscillating in time at a fixed location. The *polarization* of the light is the orientation of the electric field \vec{E} . For the wave drawn here, the wave is polarized in the z -direction, which we can call vertically polarized and represent by the state $|V\rangle$.

Change of Basis

It is worth noting that the set of vectors $\{|0\rangle, |1\rangle\}$ is not the only way we can decompose an arbitrary state $|\psi\rangle$! $\{|0\rangle, |1\rangle\}$ happens to be convenient – they map to the xy axes in our usual Cartesian space. But one can imagine that you could pick any other pair of vectors (supposing they are not just rescaled versions of the same vector, i.e. they are *linearly independent*) and decompose $|\psi\rangle$ in terms of those as well.

Let's illustrate this graphically, in Cartesian (not Bloch!) coordinates [Fig. 6].

The state

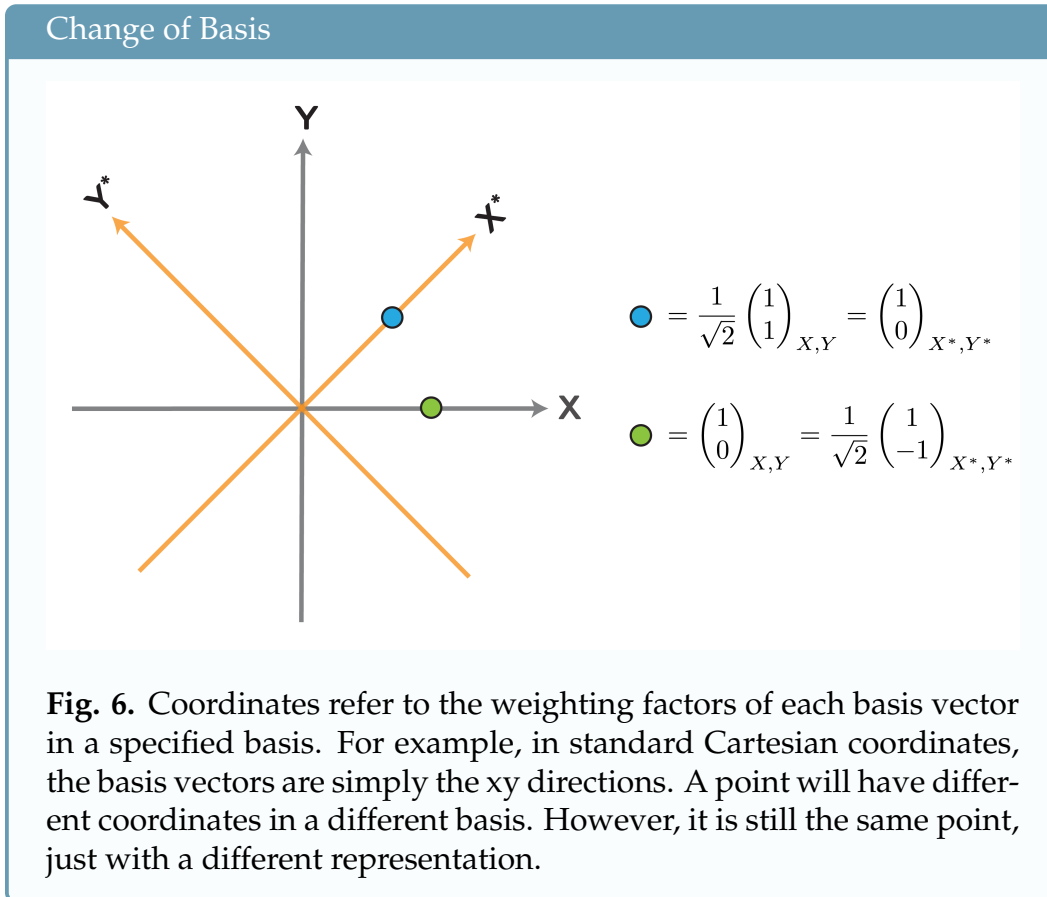
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (11)$$

means that we “walk” $1/\sqrt{2}$ in the “ x ” ($|0\rangle$) direction and $1/\sqrt{2}$ in the “ y ” ($|1\rangle$) direction. But we could equivalently just walk 1 in the $|\psi\rangle$ direction,

which we will now give the special label $|+\rangle$. This is the sense of a change of basis. The point (state) is the same – but the coordinate representation has changed, i.e.

$$|\psi\rangle = 1 \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} + 0 \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}_+ \quad (12)$$

where the subscript $+$ indicates that these are the coordinates in the $+$ basis.



Different Polarizations

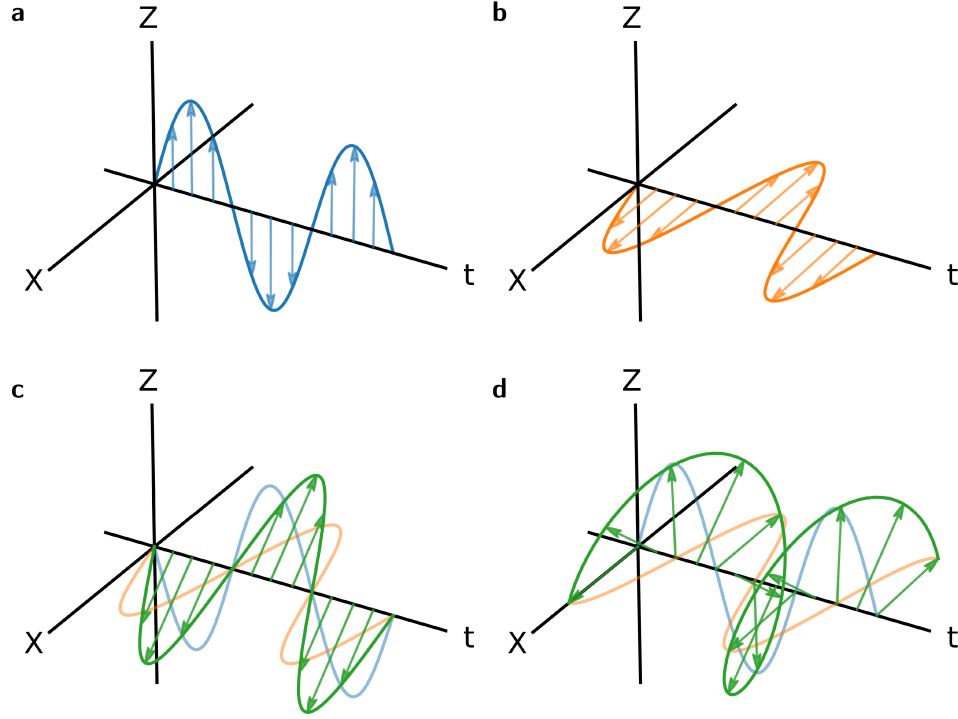


Fig. 7. (a) Vertically polarized light, represented by $|V\rangle$. (b) Horizontally polarized light, represented by $|H\rangle$. (c) Diagonally polarized light is a linear combination of $|V\rangle$ and $|H\rangle$. (d) Circularly polarized light is a linear combination of $|V\rangle$ and $|H\rangle$ with a 90° phase shift between them.

Note that we have implicitly added a second “direction” (basis vector) $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Intuitively, for a two dimensional coordinate system we want two basis vectors, and in this case we have chosen the two basis vectors to be orthogonal. Conveniently in quantum mechanics, our bases will typically come out to be orthogonal (perpendicular) and normalized (to preserve probability). Some common bases we will encounter are given special names:

$$Z = \{|0\rangle, |1\rangle\} \rightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

$$X = \{|+\rangle, |-\rangle\} \rightarrow \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

Here we have written the coordinate representations in the Z basis.

BB84 Protocol for Quantum Key Distribution

With superposition alone, we already can start exploring *information* applications not possible in classical physics. In fact, although we often think about information in terms of how we process it (“Big Data”, computers, and the like), one of the core ideas in information is how to transmit it efficiently and securely. This is the field of *communications*.

Quantum communications encodes transmitted information in quantum systems. These are typically photons, or “flying qubits”. Photons are nice! They travel at the speed of light, and *really* don’t like interacting with the environment. Combined with existing fiber optic infrastructure for the internet that spans across the globe (<https://www.submarinecablemap.com/>), this means photons can transmit quantum information over 10s of kilometres with minimal loss of the information!

Core idea: We can detect eavesdroppers because eavesdropping is a measurement, and measurement of a quantum system perturbs it.

This follows directly from the measurement collapse postulate, and is the basis of quantum-secured communication.

For example, we may consider the problem of how to transmit encryption keys securely. The first quantum version of such a key distribution protocol was developed by Bennett and Brassard in 1984 (hence, BB84...very imaginative naming).

























BB84				
Alice's bit	Alice's basis	Initial state	Bob's basis	Bit added to shared key?
0				yes
1				yes
0				no
1				no
0				no
1				no
0				yes
1				yes

Fig. 8. Table of BB84 outcomes.

Let us describe the situation. Consider two parties, Alice and Bob, who want to communicate securely. They have access to a classical communication channel (e.g. internet fibre) and a quantum communication channel over which quantum states can be transmitted. In practice, this may just be another optical fiber transmitting single photons instead of laser pulses.

1. Alice wants to send Bob a bit string $a = 101101...01$.
2. For each bit $a_i \in \{0, 1\}$ they pick either the Z or X basis to encode the information in. That is,

$$a_{i,Z} = 0 \rightarrow |0\rangle$$

$$a_{i,Z} = 1 \rightarrow |1\rangle$$

$$a_{i,X} = 0 \rightarrow |+\rangle$$

$$a_{i,X} = 1 \rightarrow |-\rangle$$

3. This basis choice can also be encoded in a separate bitstring $b = 010010...10$ where $b_i = 0$ indicates the Z basis was chosen, and $b_i = 1$ indicates the X basis was chosen.

4. Bitstring a is then transmitted over the quantum channel to Bob. Bob does not get bitstring b saying which basis to choose yet! Instead, they just randomly pick to measure in X or Z for each bit a_i .
5. Once Bob has finished measuring all the information in the quantum channel, Alice can transmit the actual basis string a which Bob can use to compare. Wherever both parties measured in the same basis, that information is kept; the mismatched ones are tossed.

The protocol is not secure yet! What if an eavesdropper Eve were stealing bits? The key idea here is that Eve measuring and then sending along a random bit to spoof an unintercepted communication introduces randomness from the measurement, which can be detected. Consider if Alice and Bob encoded and measured in the same basis, e.g. Alice sent $|+\rangle$ and Bob measured in the X basis. Then Bob would get $|+\rangle$ *deterministically*. But if Eve got the basis wrong and measured in Z instead, then they would get $|0\rangle$ or $|1\rangle$, each with 50% probability. Sending that along to Bob would then result in Bob measuring the wrong result (i.e. $|-\rangle$) half the time, even though Alice said the basis was correct!

Exercise for the reader: Check that $p(+) = 1/2$ for the above situation.

We thus add an extra final step:

6. Alice and Bob publicly announce k of the basis-matched bits to check they match. If more than some security threshold are mismatched, then they have detected the presence of Eve!

Of course, the natural question is how many bits k should be compared?

For this, we need to return to the rules of probability. As suggested by the exercise, the probability of Bob measuring $|-\rangle$ is $1/2$ – assuming that Eve got the basis wrong. But actually, Eve has a $1/2$ chance of picking the right basis. So the *unconditioned* probability of Bob measuring $|-\rangle$ is actually

$$\begin{aligned} p(-) &= p(-|Z_E)p(Z_E) \\ &= 1/2 \times 1/2 \\ &= 1/4 \end{aligned}$$

In words, “the overall probability of Bob measuring $|-\rangle$ is equal to the probability of Bob measuring $|-\rangle$ conditioned on Eve measuring in the wrong (Z) basis, times the probability that Eve actually chose the Z basis.”

Similar conditions can be found for all the other cases. Therefore, in general the probability that Bob measures the wrong state even though both Alice and Bob agreed their basis choices were the same is $1/4$. So if they compared just $k = 1$ bit, the probability they would actually find a mismatched bit indicating the presence of an eavesdropper is only 25%. Alice and Bob can do better. And they will!

If k bits are compared, then the probability of detecting Eve is the same as the probability that at least 1 bit out of k is mismatched. One might consider adding all the probabilities,

$$\begin{aligned} p(\text{at least 1 bit mismatched in } k) &= p(\text{exactly 1 bit mismatched in } k) \\ &\quad + p(\text{exactly 2 bits mismatched in } k) \\ &\quad + \dots \\ &\quad + p(\text{exactly } k \text{ bits mismatched in } k) \end{aligned}$$

This is a bit cumbersome. Instead, we can note that the probability that at least 1 bit is corrupted and the probability that 0 bits are corrupted make up the entire span of possibilities. So their probabilities should add to 1! Mathematically,

$$p(\text{at least 1 bit mismatched in } k) = 1 - p(0 \text{ bits mismatched in } k)$$

Each bit has a 75% chance of being uncorrupted. Moreover, each bit is *independent* from the others (the outcome of one bit measurement doesn't affect the probabilities of the others). And so,

$$p(\text{at least 1 bit mismatched in } k) = 1 - (3/4)^k$$

We can set this expression to any arbitrary detection threshold. For example, if we wanted to detect Eve 90% of the time, Alice and Bob should compare $k = 8$ bits.

No-cloning Theorem

One might ask if the eavesdropper could simply measure the qubit, but then send an identical copy of the information so no one would be the wiser. This is a subtle point – but in fact, also disallowed by the laws of quantum mechanics!

Theorem: There is no quantum operation that can duplicate an arbitrary quantum state.

Proof: Suppose there were an operation U that can clone an arbitrary state $|\psi\rangle$, i.e.

$$U |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle$$

Because $|\psi\rangle$ is arbitrary, then it could be a superposition of some basis states, i.e.

$$\begin{aligned} U |\psi\rangle |0\rangle &= U(a |\alpha\rangle + b |\beta\rangle) |0\rangle \\ &= (a |\alpha\rangle + b |\beta\rangle)(a |\alpha\rangle + b |\beta\rangle) \end{aligned}$$

However, we could alternately use the linearity of U to write:

$$\begin{aligned} U |\psi\rangle |0\rangle &= (aU |\alpha\rangle + bU |\beta\rangle) |0\rangle \\ &= a |\alpha\rangle |\alpha\rangle + b |\beta\rangle |\beta\rangle \end{aligned}$$

Some FOIL to expand the binomials will quickly show these are not equivalent – proof by contradiction!

Bibliography

[Axl15] Sheldon Axler. Linear Algebra Done Right. Springer, 3rd edition, 2015.