# Introduction to Quantum Computing

**George Voutsadakis**[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

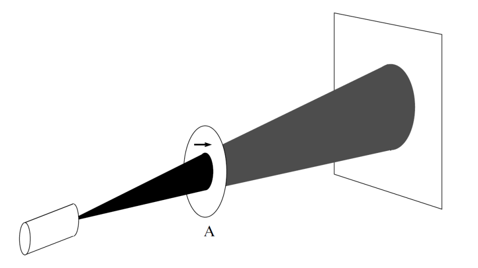
1. Single-Qubit Quantum Systems
   - The Quantum Mechanics of Photon Polarization
   - Single Quantum Bits
   - Single-Qubit Measurement
   - A Quantum Key Distribution Protocol
   - The State Space of a Single-Qubit System

Subsection 1

## The Quantum Mechanics of Photon Polarization

# An Experiment

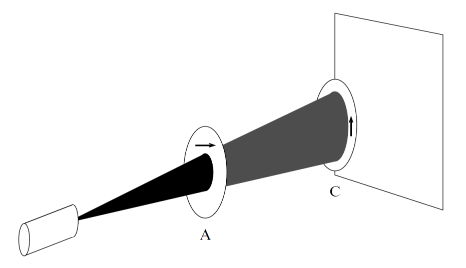
- Shine a beam of light on a projection screen.
- Suppose polaroid $A$ is placed between the light source and the screen.



- Then the intensity of the light reaching the screen is reduced.
- Suppose that the polarization of polaroid $A$ is horizontal

# An Experiment (Cont'd)

- Next, place polaroid $C$ between polaroid $A$ and the projection screen.



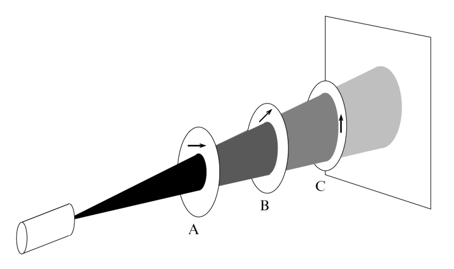
- Suppose polaroid $C$ is rotated so that its polarization is orthogonal (vertical) to the polarization of $A$.
- Then no light reaches the screen.

# An Experiment (Cont'd)

- Place polaroid $B$ between polaroids $A$ and $C$.
- One might expect that adding another polaroid will not make any difference.
- The presumption may be that if no light got through two polaroids, then surely no light will pass through three!
- Surprisingly, at most polarization angles of $B$, light shines on the screen.

# An Experiment (Cont'd)

- The intensity of the light will be maximal if the polarization of $B$ is at 45 degrees to both $A$ and $C$.



- Clearly the polaroids cannot be acting as simple sieves.

# Light: Waves and Quanta

- For a bright beam of light, there is a classical explanation of the experiment in terms of waves.
- Versions of the experiment described here, using light so dim that only one photon at a time interacts with the polaroid, have been done with more sophisticated equipment.
- The results of these single photon experiments can be explained only using quantum mechanics.
- The classical wave explanation no longer works.

# Quantum Mechanical Explanation

- The quantum mechanical explanation of the experiment consists of two parts.
    - A model of a photon's polarization state;
    - A model of the interaction between a polaroid and a photon.
- The description of this experiment, and the definition of a qubit, use basic notions of linear algebra such as *vector*, *basis*, *orthonormal* and *linear combination*.

# Photon's Polarization State (Vectors)

- Quantum mechanics models a photon's polarization state by a unit vector, a vector of length 1, pointing in the appropriate direction.
- We write $|\uparrow\rangle$ for the unit vector that represents vertical polarization.
- We write $|\rightarrow\rangle$ for the unit vectors that represents horizontal polarization.
- Think of $|v\rangle$ as a vector with some arbitrary label $v$.
- In quantum mechanics, the standard notation for a vector representing a quantum state is $|v\rangle$, just as $\overrightarrow{v}$ or $\mathbf{v}$ are notations used for vectors in other settings.
- This notation is part of a more general notation, Dirac's notation, explained in more detail later.

# Photon's Polarization State (Linear Combinations)

- An arbitrary polarization can be expressed as a linear combination

  $$|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$$

  of the two basis vectors $|\uparrow\rangle$ and $|\rightarrow\rangle$.
- For example,

  $$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$$

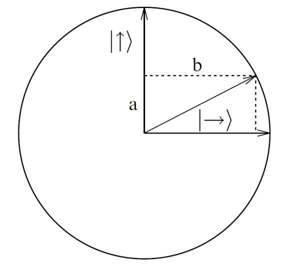
  is a unit vector representing polarization of 45 degrees.

# Amplitudes and Superposition

- The coefficients $a$ and $b$ in

$$|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$$

are called the **amplitudes** of $|v\rangle$ in the directions $|\uparrow\rangle$ and $|\rightarrow\rangle$, respectively.



- When $a$ and $b$ are both non-zero,

$$|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$$

is said to be a **superposition** of $|\uparrow\rangle$ and $|\rightarrow\rangle$.

# Interaction Between a Photon and a Polaroid

- The polaroid has a preferred axis, its polarization.
- Suppose a photon has polarization $|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$.
- When it meets a polaroid with preferred axis $|\uparrow\rangle$, the photon:
  - Will get through with probability $|a|^2$;
  - Will be absorbed with probability $|b|^2$.
- In words:
  - The probability that a photon passes through the polaroid is the square of the magnitude of the amplitude of its polarization in the direction of the polaroid's preferred axis.
  - The probability that the photon is absorbed by the polaroid is the square of the magnitude of the amplitude in the direction perpendicular to the polaroid's preferred axis.
- Furthermore, any photon that passes through the polaroid will now be polarized in the direction of the polaroid's preferred axis.

# Remark

- The preceding features of the interaction hold more generally.
- In all interactions between qubits and measuring devices, no matter what their physical realization:
  - The nature of the interaction is probabilistic;
  - There is a resulting change of state in the observed qubit.

# Explanation of the Photon Experiment (Polaroids $A$ and $C$)

- In the experiment, any photons that pass through polaroid $A$ will leave polarized in the direction of polaroid $A$'s preferred axis, in this case horizontal, $|\rightarrow\rangle$.
- A horizontally polarized photon has no amplitude in the vertical direction, so it has no chance of passing through polaroid $C$, which was given a vertical orientation.
- For this reason, no light reaches the screen.
- Had polaroid $C$ been in any other orientation, a horizontally polarized photon would have some amplitude in the direction of polaroid $C$'s preferred axis, and some photons would reach the screen.

# Explanation of the Experiment (Insertion of Polaroid $B$)

- Suppose polaroid $B$ has preferred axis $|\nearrow\rangle$.
- Write the horizontally polarized photon's polarization state $|\rightarrow\rangle$ as

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle.$$

- Any photon that passes through polaroid $A$ becomes horizontally polarized.
- So the amplitude of any such photon's state $|\rightarrow\rangle$ in the direction $|\nearrow\rangle$ is $\frac{1}{\sqrt{2}}$.
- A horizontally polarized photon will pass through polaroid $B$ with probability $\frac{1}{2} = |\frac{1}{\sqrt{2}}|^2$.

# Explanation of the Experiment (Cont'd)

- A horizontally polarized photon will pass through polaroid $B$ with probability $\frac{1}{2} = |\frac{1}{\sqrt{2}}|^2$.
- Any photons that have passed through polaroid $B$ now have polarization $|\nearrow\rangle$.
- When these photons hit polaroid $C$, they do have amplitude in the vertical direction.
- So some of them (half) will pass through polaroid $C$ and hit the screen.
- In this way, quantum mechanics explains how more light can reach the screen when the third polaroid is added.
- Moreover, it provides a means to compute how much light will reach the screen.

Subsection 2

## Single Quantum Bits

# Qubits

- The space of possible polarization states of a photon is an example of a **quantum bit**, or **qubit**.
- Any state represented by a unit vector
$$a|\uparrow\rangle + b|\rightarrow\rangle$$
is a legitimate qubit value.
- So a qubit has a continuum of possible values.
- The amplitudes *a* and *b* can be complex numbers, even though complex amplitudes were not needed for the explanation of the experiment.

# State Space

- In general, the set of all possible states of a physical system is called the **state space** of the system.
- Any quantum mechanical system that can be modeled by a two-dimensional complex vector space can be viewed as a qubit.
- There is redundancy in this representation.
- Any vector multiplied by a modulus one [unit length] complex number represents the same quantum state.
- This redundancy is discussed carefully later.

# Two-State Quantum Systems

- Qubits are also called **two-state quantum systems**.
- They include:
  - Photon polarization;
  - Electron spin;
  - The ground state together with an excited state of an atom.
- The **two-state** label for these systems does not mean that the state space has only two states - it has infinitely many.
- It rather means that all possible states can be represented as a linear combination, or superposition, of just two states.

# Remarks

- For a two-dimensional complex vector space to be viewed as a qubit, two linearly independent states, labeled $|0\rangle$ and $|1\rangle$, must be distinguished.
- For the theory of quantum information processing, all two-state systems, whether they be electron spin or energy levels of an atom, are equally good.
- From a practical point of view, it is as yet unclear which two-state systems will be most suitable for physical realizations of quantum information processing devices such as quantum computers.

# Dirac's Bra/ket Notation

- Dirac's bra/ket notation is used throughout quantum physics to represent quantum states and their transformations.
- We introduce the part of Dirac's notation used for quantum states.
- We defer Dirac's notation for quantum transformations for later.
- Familiarity and fluency with this notation will help greatly in understanding all subsequent material.
- In Dirac's notation, a **ket** such as $|x\rangle$, where $x$ is an arbitrary label, refers to a vector representing a state of a quantum system.
- A vector $|v\rangle$ is a **linear combination** of vectors $|s_1\rangle, |s_2\rangle, \ldots, |s_n\rangle$ if there exist complex numbers $a_i$, such that

$$|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \cdots + a_n|s_n\rangle.$$

# Span

- A set of vectors $S$ **generates** a complex vector space $V$ if every element $|v\rangle$ of $V$ can be written as a complex linear combination of vectors in the set.
- That is, every $|v\rangle \in V$ can be written as

  $$|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \cdots + a_n|s_n\rangle,$$

  for some elements $|s_i\rangle \in S$ and complex numbers $a_i$.
- Given a set of vectors $S$, the subspace of all linear combinations of vectors in $S$ is called the **span** of $S$ and denoted $\text{span}(S)$.

# Basis

- A set of vectors $B$ for which every element of $V$ can be written uniquely as a linear combination of vectors in $B$ is called a **basis** for $V$.
- In a two-dimensional vector space, any two vectors that are not multiples of each other form a basis.
- In quantum mechanics, bases are usually required to be *orthonormal*, (to be explained shortly).
- The two distinguished states, $|0\rangle$ and $|1\rangle$ are required to be orthonormal.

# Inner Product

- Suppose $\overline{z}$ denotes the complex conjugate

$$\overline{z} = a - \boldsymbol{i}b$$

of a complex number $z = a + \boldsymbol{i}b$.

- An **inner product**, or **dot product**,

$$\langle v_2 | v_1 \rangle$$

on a complex vector space $V$ is a complex function defined on pairs of vectors $|v_1\rangle$ and $|v_2\rangle$ in $V$, satisfying:
    - $\langle v|v\rangle$ is non-negative real;
    - $\langle v_2|v_1\rangle = \overline{\langle v_1|v_2\rangle}$;
    - $(a\langle v_2| + b\langle v_3|)|v_1\rangle = a\langle v_2|v_1\rangle + b\langle v_3|v_1\rangle$.

# Orthogonality and Norm

- Two vectors $|v_1\rangle$ and $|v_2\rangle$ are said to be **orthogonal** if

$$\langle v_1|v_2\rangle = 0.$$

- A set of vectors is **orthogonal** if all of its members are orthogonal to each other.
- The **length**, or **norm**, of a vector $|v\rangle$ is

$$||v\rangle| = \sqrt{\langle v|v\rangle}.$$

- Since all vectors $|x\rangle$ representing quantum states are of unit length,

$$\langle x|x\rangle = 1, \quad \text{for any state vector } |x\rangle.$$

# Orthonormality

- A set of vectors is said to be **orthonormal** if all of its elements are of length one and orthogonal to each other.
- That is, a set of vectors

  $$B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_n\rangle\}$$

  is orthonormal if, for all $i, j$,

  $$\langle \beta_i | \beta_j \rangle = \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

- In quantum mechanics we are mainly concerned with bases that are orthonormal.
- So, whenever we say basis, we mean *orthonormal basis*, unless stated otherwise.

# Qubit Representation

- For the state space of a two-state system to represent a quantum bit, two orthonormal states, labeled $|0\rangle$ and $|1\rangle$, must be specified.
- Apart from the requirement that $|0\rangle$ and $|1\rangle$ be orthonormal, the states may be chosen arbitrarily.
- In the case of photon polarization, we may choose $|0\rangle$ and $|1\rangle$ to correspond to the states $|\uparrow\rangle$ and $|\rightarrow\rangle$, or to $|\nearrow\rangle$ and $|\nwarrow\rangle$.
- We follow the convention that

$$|0\rangle = |\uparrow\rangle \quad \text{and} \quad |1\rangle = |\rightarrow\rangle.$$

- This choice implies that

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

# Standard Basis

- When talking about qubits, a **standard basis**

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

  with respect to which all statements are made must be chosen in advance and remain fixed throughout the discussion.
- In quantum information processing, classical bit values of 0 and 1 will be encoded in the distinguished states $|0\rangle$ and $|1\rangle$.
- This encoding enables a direct comparison between bits and qubits.
  - Bits can take only two values, 0 and 1;
  - Qubits can take not only the values $|0\rangle$ and $|1\rangle$ but also any superposition of these values,

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

    where $a$ and $b$ are complex numbers, such that $|a|^2 + |b|^2 = 1$.

# Vector Representation in Bra/ket Notation

- Vectors and linear transformations can be written using matrix notation once a basis has been specified.
- If basis $\{|\beta_1\rangle, |\beta_2\rangle\}$ is specified, a ket

$$|v\rangle = a|\beta_1\rangle + b|\beta_2\rangle$$

  can be written $\begin{pmatrix} a \\ b \end{pmatrix}$.
- A ket $|v\rangle$ corresponds to a column vector $v$, where $v$ is simply a label, a name for this vector.

# Vector Representation in Bra/ket Notation (Cont'd)

- The conjugate transpose $v^\dagger$ of a vector $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ is
$$v^\dagger = (\overline{a_1}, \ldots, \overline{a_n}).$$
- In Dirac's notation, the conjugate transpose of a ket $|v\rangle$ is called a **bra** and is written $\langle v|$.
- So
$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{and} \quad \langle v| = (\overline{a_1}, \ldots, \overline{a_n}).$$
- A bra $\langle v|$ corresponds to a row vector $v^\dagger$.

# Inner Product Representation

- Let $|a\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ and $|b\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ be two complex vectors.
- The standard **inner product** $\langle a|b\rangle$ is defined to be the scalar obtained by multiplying the conjugate transpose $\langle a| = (\overline{a_1}, \ldots, \overline{a_n})$ with $|b\rangle$,

$$\langle a|b\rangle = \langle a||b\rangle = (\overline{a_1}, \ldots, \overline{a_n}) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} \overline{a_i} b_i.$$

- When $\vec{a} = |a\rangle$ and $\vec{b} = |b\rangle$ are real vectors, this inner product is the same as the standard dot product on the $n$ dimensional real vector space $\mathbb{R}^n$,

$$\langle a|b\rangle = a_1 b_1 + \cdots + a_n b_n = \vec{a} \cdot \vec{b}.$$

# Inner Product Representation and Bra/ket

- Dirac's choice of *bra* and *ket* arose as a play on words.
- An inner product $\langle a|b\rangle$ of a bra $\langle a|$ and a ket $|b\rangle$ is sometimes called a **bracket**.
- The following relations hold, where $v = a|0\rangle + b|1\rangle$.
  - $\langle 0|0\rangle = 1$;
  - $\langle 1|1\rangle = 1$;
  - $\langle 1|0\rangle = \langle 0|1\rangle = 0$;
  - $\langle 0|v\rangle = a$, and $\langle 1|v\rangle = b$.

# The Standard Basis

- In the standard basis, with ordering $\{|0\rangle, |1\rangle\}$, the basis elements $|0\rangle$ and $|1\rangle$ can be expressed as $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- A complex linear combination $|v\rangle = a|0\rangle + b|1\rangle$ can be written $\begin{pmatrix} a \\ b \end{pmatrix}$.
- This choice of basis and order of the basis vectors are by convention.
- Representing $|0\rangle$ as $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle$ as $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ or representing $|0\rangle$ as $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ and $|1\rangle$ as $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ would be equally good as long as it is done consistently.
- Unless otherwise specified, all vectors and matrices in these notes will be written with respect to the standard basis $\{|0\rangle, |1\rangle\}$ in this order.

# Superposition

- A quantum state $|v\rangle$ is a **superposition** of basis elements $\{|\beta_1\rangle, |\beta_2\rangle\}$ if it is a nontrivial linear combination of $|\beta_1\rangle$ and $|\beta_2\rangle$.
- That is, if
$$|v\rangle = a_1|\beta_1\rangle + a_2|\beta_2\rangle,$$
where $a_1$ and $a_2$ are non-zero.
- For the term **superposition** to be meaningful, a basis must be specified.
- If we say "superposition" without explicitly specifying the basis, we implicitly mean with respect to the standard basis.

# Vector versus Bra/ket Notation

- Initially the vector/matrix notation may appear easier to use because it is familiar.
- Sometimes matrix notation is convenient for performing calculations.
- It always requires the choice of a basis and an ordering of that basis.
- The bra/ket notation has the advantage of being independent of basis and the order of the basis elements.
- It is also more compact and suggests correct relationships, as we saw for the inner product.
- So once it becomes familiar, bra/ket notation is easier to read and faster to use.

# Qudits

- Instead of qubits, physical systems with states modeled by three- or $n$-dimensional vector spaces could be used as fundamental units of computation.
- Three-valued units are called **qutrits**.
- $n$-valued units are called **qudits**.
- Qudits can be modeled using multiple qubits.
- So a model of quantum information based on qudits has the same computational power as one based on qubits.
- For this reason we do not consider qudits further, just as in the classical case most people use a bit-based model of information.

Subsection 3

## Single-Qubit Measurement

# Measurement

- Quantum theory postulates that any device that measures a two-state quantum system must have two preferred states whose representative vectors,
$$\{|u\rangle, |u^\perp\rangle\},$$
form an orthonormal basis for the associated vector space.
- Measurement of a state transforms the state into one of the measuring device's associated basis vectors $|u\rangle$ or $|u^\perp\rangle$.
- The probability that the state is measured as basis vector $|u\rangle$ is the square of the magnitude of the amplitude of the component of the state in the direction of the basis vector $|u\rangle$.

# Example

- Consider a device for measuring the polarization of photons with associated basis

  $$\{|u\rangle, |u^{\perp}\rangle\}.$$

  Consider the state

  $$|v\rangle = a|u\rangle + b|u^{\perp}\rangle.$$

  $|v\rangle$ is measured as:

  - $|u\rangle$ with probability $|a|^2$;
  - $|u^{\perp}\rangle$ with probability $|b|^2$.

# Device Bases

- If quantum mechanics is correct:
  - All devices that measure single qubits must have associated bases;
  - The measurement outcome is always one of the two basis vectors.
- For this reason, whenever anyone says “measure a qubit”, they must specify with respect to which basis the measurement takes place.
- When we say “measure a qubit” without further elaboration, we mean that the measurement is with respect to the standard basis

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

# Quantum Measurements Change the State

- Measurement of a quantum state changes the state.
- If a state

$$|v\rangle = a|u\rangle + b|u^{\perp}\rangle$$

  is measured as $|u\rangle$, then the state $|v\rangle$ changes to $|u\rangle$.
- A second measurement with respect to the same basis will return $|u\rangle$ with probability 1.
- Thus, unless the original state happens to be one of the basis states, a single measurement will change that state, making it impossible to determine the original state from any sequence of measurements.

# Superposition and Basis Dependence

- The notion of superposition is basis-dependent.
- All states are superpositions with respect to some bases and not with respect to others.

  Example: Consider the state

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

  It is a superposition with respect to the basis $\{|0\rangle, |1\rangle\}$.

  It is not a superposition with respect to $\{a|0\rangle + b|1\rangle, \overline{b}|0\rangle - \overline{a}|1\rangle\}$.

# Meaning of Superposition

- The result of measuring a superposition is probabilistic.
- However, the state $|v\rangle = a|0\rangle + b|1\rangle$ is not a probabilistic mixture of $|0\rangle$ and $|1\rangle$.
- In particular, it is not true that the state is really either $|0\rangle$ or $|1\rangle$ and that we simply do not happen to know which.
- Rather, $|v\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results.

# Example

- Consider a photon with polarization

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

It behaves deterministically when measured with respect to the Hadamard basis $\{|\nearrow\rangle, |\nwarrow\rangle\}$.

It gives random results when measured with respect to the standard basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$.

# Meaning of Superposition (Cont'd)

- It is okay to think of a superposition $|v\rangle = a|0\rangle + b|1\rangle$ as in some sense being in both state $|0\rangle$ and state $|1\rangle$ at the same time.
- However, that statement should not be taken too literally.
- Consider states that are combinations of $|0\rangle$ and $|1\rangle$ in similar proportions but with different amplitudes.
- E.g., consider

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad \frac{1}{\sqrt{2}}(|0\rangle + \boldsymbol{i}|1\rangle).$$

- These represent distinct states that behave differently in many situations.

# Extracting Information from a Qubit

- Qubits can take on any one of infinitely many states.
- Consequently, one might hope that a single qubit could store lots of classical information.
- However, the properties of quantum measurement severely restrict the amount of information that can be extracted from a qubit.
    1. Information about a quantum bit can be obtained only by measurement.
       Any measurement results in one of only two states, namely, the two basis states associated with the measuring device.
       Thus, a single measurement yields at most a single classical bit of information.

# Extracting Information from a Qubit

2. Measurement changes the state.
   So one cannot make two measurements on the original state of a qubit.
3. An unknown quantum state cannot be cloned.
   So it is not possible to measure a qubit's state in two ways, even indirectly by copying the qubit's state and measuring the copy.

- In summary:
  - A quantum bit can be in infinitely many different superposition states.
  - However, it is possible to extract only a single classical bit's worth of information from a single quantum bit.

Subsection 4

## A Quantum Key Distribution Protocol

# Keys

- Keys provide the security for most cryptographic protocols.
- Keys are binary strings or numbers chosen randomly from a sufficiently large set.
- Two general classes of keys exist.
  - Symmetric keys;
  - Public-private key pairs.
- Public-private key pairs consist of:
  - A public key, knowable by all;
  - A corresponding private key whose secrecy must be carefully guarded by the owner.
- Symmetric keys consist of a single key (or a pair of keys easily computable from one another) that are known to all of the legitimate parties and no one else.
- In the symmetric key case, multiple parties are responsible for guarding the security of the key.

# Quantum Key Distribution Protocols

- Quantum key distribution protocols establish a symmetric key between two parties.
- The parties are generally known in cryptography as Alice and Bob.
- Quantum key distribution protocols can be used securely anywhere classical key agreement protocols can be used.
- The security of quantum key distribution rests on fundamental properties of quantum mechanics.
- On the other hand, classical key agreement protocols rely on the computational intractability of a certain problem.

# Example

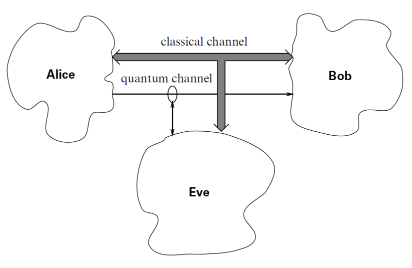
- An example showcasing the difference is the Diffie-Hellman classical key agreement protocol.
- It remains secure against all known classical attacks.
- However, the problem on which it is based, the discrete logarithm problem, is tractable on a quantum computer.

# Introducing the BB84 Protocol

- The earliest quantum key distribution protocol is known as BB84 after its inventors (Charles Bennett and Gilles Brassard), and the year.
- The aim of the BB84 protocol is to establish a secret key, a random sequence of bit values 0 and 1, known only to the two parties.
- The parties may use this key to support a cryptographic task such as exchanging secret messages or detecting tampering.
- The BB84 protocol enables Alice and Bob to be sure that, if they detect no problems while attempting to establish a key, then with high probability it is secret.
- The protocol does not guarantee, however, that they will succeed in establishing a private key.

# The Communication Setup

- Suppose Alice and Bob are connected by two public channels.
  - An ordinary bidirectional classical channel;
  - A unidirectional quantum channel.



- The quantum channel allows Alice to send a sequence of single qubits to Bob.
- Suppose the qubits are encoded in the polarization states of individual photons.
- Both channels can be observed by an eavesdropper Eve.

# Alice's Quantum Message to Bob

- Alice and Bob aim at establishing a private key.
- Alice uses quantum or classical means to generate a random sequence of classical bit values.
- A random subset of this sequence will be the final private key.
- Alice then randomly encodes each bit of this sequence in the polarization state of a photon by randomly choosing for each bit one of the following two agreed-upon bases in which to encode it.
    - The standard basis,
    $$0 \mapsto |\uparrow\rangle, \qquad 1 \mapsto |\rightarrow\rangle;$$
    - The Hadamard basis,
    $$0 \mapsto |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \quad 1 \mapsto |\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle).$$
- She sends this sequence of photons to Bob through the quantum channel.

# Bob and Alice Communication

- Bob measures the state of each photon he receives by randomly picking either basis.
- Over the classical channel, Alice and Bob check that Bob has received a photon for every one Alice has sent.
- Only then do Alice and Bob tell each other the bases they used for encoding and decoding (measuring) each bit.
  - When the choice of bases agree, Bob's measured bit value agrees with the bit value that Alice sent.
  - When they chose different bases, the chance that Bob's bit matches Alice's is only 50 percent.

# Bob and Alice Communication (Cont'd)

- Without revealing the bit values themselves, which would also reveal the values to Eve, there is no way for Alice and Bob to figure out which of these bit values agree and which do not.
- So they discard all the bits on which their choice of bases differed.
- An average of 50 percent of all bits transmitted remain.
- Then, depending on the level of assurance they require, Alice and Bob compare a certain number of bit values to check that no eavesdropping has occurred.
- These bits will also be discarded, and only the remaining bits will be used as their private key.

# Eve's Possible Attack

- We describe one sort of attack that Eve can make.
- We see how quantum aspects of the protocol guard against it.
- On the classical channel, Alice and Bob discuss only the choice of bases and not the bit values themselves.
- So Eve cannot gain any information about the key from listening to the classical channel alone.
- To gain information, Eve must intercept the photons transmitted by Alice through the quantum channel.
- Eve must send photons to Bob before knowing the choice of bases made by Alice and Bob, because they compare bases only after Bob has confirmed receipt of the photons.
- If she sends different photons to Bob, Alice and Bob will detect that something is wrong when they compare bit values.
- If she sends the original photons to Bob without doing anything, she gains no information.

# Means of Eve's Intervention

- To gain information, Eve makes a measurement before sending the photons to Bob.
- Instead of using a polaroid to measure, she can use a *calcite crystal* and a *photon detector*.
    - A beam of light passing through a calcite crystal is split into two spatially separated beams.
        - One polarized in the direction of the crystal's optic axis;
        - The other polarized in the direction perpendicular to the optic axis.
    - A photon detector placed in one of the beams performs a quantum measurement.

      The probability with which a photon ends up in one of the beams can be calculated as described previously.

# Problems with Eve's Intervention

- Alice has not yet told Bob her sequence of bases.
- So Eve does not know in which basis to measure each bit.
- If she randomly measures the bits, she will measure using the wrong basis approximately half of the time.
- When she uses the wrong basis to measure, the measurement changes the polarization of the photon before it is resent to Bob.
- As a consequence, even if Bob measures the photon in the same basis as Alice used to encode the bit, he will get the correct bit value only half the time.

# Alice and Bob's Security Assurance

- Overall, for each of the qubits Alice and Bob retain, if the qubit was measured by Eve before she sent it to Bob, there will be a 25 percent chance that Bob measures a different bit value than the one Alice sent.
- Thus, this attack on the quantum channel is bound to introduce a high error rate that Alice and Bob detect by comparing a sufficient number of bits over the classical channel.
- If these bits agree, they can confidently use the remaining bits as their private key.

# Alice and Bob's Security Assurance (Cont'd)

- Summarizing the outcomes of the attack:
  - It is likely that 25 percent of Eve's version of the key is incorrect;
  - The fact that someone is eavesdropping can be detected by Alice and Bob.
- So Alice and Bob run little risk of establishing a compromised key.
- Either they succeed in creating a private key or they detect that eavesdropping has taken place.

# Impossibility of Copying with Unknown Basis

- Eve does not know in which basis to measure the qubits.
- This property is crucial to the security of this protocol.
- It is ensured as Alice and Bob share information about which bases they used only after Bob has received the photons.
- If Eve knew in which basis to measure the photons, her measurements would not change the state.
- So she could obtain the bit values without Bob and Alice noticing anything suspicious.

# No-Cloning Principle

- What if Eve could overcome this obstacle by copying the qubit, keeping a copy for herself while sending the original on to Bob?
- Then she can measure her copy later after learning the correct basis from listening in on the classical channel.
- Such a protocol is defeated by an important property of quantum information.
- The No-Cloning Principle of quantum mechanics means that it is impossible to reliably copy quantum information unless a basis in which it is encoded is known.
- Copying with the wrong machine not only does not produce an accurate copy, but it also changes the original in much the same way measuring in the wrong basis does.
- So Bob and Alice would detect attempts to copy with high probability.

# Additional Precautions Needed

- The security of this protocol, like other pure key distribution protocols such as Diffie-Hellman, is vulnerable to a **man-in-the-middle attack** in which Eve impersonates Bob to Alice and Alice to Bob.
- To guard against such an attack, Alice and Bob need to combine it with an authentication protocol, be it recognizing each other's voices or a more mathematical authentication protocol.
- More sophisticated versions of this protocol exist that support quantum key distribution through noisy channels and stronger guarantees about the amount of information Eve can gain.

Subsection 5

## The State Space of a Single-Qubit System

# State Space for Qubits

- The **state space** of a classical or quantum physical system is the set of all possible states of the system.
- When we are considering only polarization states of a single photon, the state space is all possible polarizations.
- The state space for a single qubit, no matter how it is realized, is the set of possible qubit values,

  $$\{a|0\rangle + b|1\rangle\},$$

  where $|a|^2 + |b|^2 = 1$.
- Moreover, $a|0\rangle + b|1\rangle$ and $a'|0\rangle + b'|1\rangle$ are considered the same qubit value if

  $$a|0\rangle + b|1\rangle = c(a'|0\rangle + b'|1\rangle),$$

  for some complex number $c$, with $|c| = 1$.

# The Global Phase

- That the same quantum state is represented by more than one vector means that there is a critical distinction between:
  - The complex vector space in which we write our qubit values;
  - The quantum state space itself.
- We have reduced the ambiguity by requiring that vectors representing quantum states be unit vectors, but some ambiguity remains.
- Unit vectors equivalent up to multiplication by a complex number of modulus one represent the same state.

# The Global Phase (Cont'd)

- The multiple by which two vectors representing the same quantum state differ is called the **global phase** and has no physical meaning.
- We write $|v\rangle \sim |v'\rangle$ to indicate that $|v\rangle = c|v'\rangle$, for some complex global phase $c = e^{\boldsymbol{i}\phi}$.
- $\sim$ is an equivalence relation.
- The space in which two two-dimensional complex vectors are considered equivalent if they are multiples of each other is called **complex projective space** of dimension one.

# The Quotient Space

- This **quotient space**, a space obtained by identifying sets of equivalent vectors with a single point in the space, is expressed with the compact notation used for quotient spaces:

$$\mathbf{CP}^1 = \{a|0\rangle + b|1\rangle\}/\sim.$$

- So the quantum state space for a single-qubit system is in one-to-one correspondence with the points of the complex projective space $\mathbf{CP}^1$.
- We will make no further use of $\mathbf{CP}^1$.
- However, it is used in the quantum information literature.

# Working in the Vector Space

- The linearity of vector spaces makes them easier to work with than projective spaces.
- E.g., in vector spaces, we know how to add vectors, but there is no corresponding way of adding points in projective spaces.
- So we generally perform all calculations in the vector space corresponding to the quantum state space.
- The multiplicity of representations of a single quantum state in this vector space representation, however, may cause some confusion.

# Relative Phase

- A physically important quantity is the *relative phase* of a single-qubit state $a|0\rangle + b|1\rangle$.
- The relative phase (in the standard basis) of a superposition $a|0\rangle + b|1\rangle$ is a measure of the angle in the complex plane between the two complex numbers $a$ and $b$.
- More precisely, the **relative phase** of $a|0\rangle + b|1\rangle$ is the modulus one complex number $e^{\boldsymbol{i}\phi}$ satisfying

$$\frac{a}{b} = e^{\boldsymbol{i}\phi}\frac{|a|}{|b|}.$$

- Two superpositions $a|0\rangle + b|1\rangle$ and $a'|0\rangle + b'|1\rangle$ whose amplitudes have the same magnitudes but that differ in a relative phase represent different states.

# Relative versus Global Phase

- The physically meaningful relative phase and the physically meaningless global phase should not be confused.
- While multiplication with a unit constant does not change a quantum state vector, relative phases in a superposition do represent distinct quantum states.

  Example: Even though $|v_1\rangle \sim e^{\boldsymbol{i}\phi}|v_1\rangle$, the vectors

  $$\frac{1}{\sqrt{2}}(e^{\boldsymbol{i}\phi}|v_1\rangle + |v_2\rangle) \text{ and } \frac{1}{\sqrt{2}}(|v_1\rangle + |v_2\rangle)$$

  do not represent the same state.
- We must always be careful of the $\sim$ equivalence when we interpret the results of our computations as quantum states.

# Specially Named Single-Qubit States

- A few single-qubit states will be referred to often enough that we give them special labels.

$$\begin{array}{rcl} |+\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\ |\boldsymbol{i}\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle + \boldsymbol{i}|1\rangle), \\ |-\boldsymbol{i}\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle - \boldsymbol{i}|1\rangle). \end{array}$$

- The basis $\{|+\rangle, |-\rangle\}$ is referred to as the **Hadamard basis**.
- We sometimes use the notation $\{|\nwarrow\rangle, |\nearrow\rangle\}$ for the Hadamard basis when discussing photon polarization.

# Geometric Model: Extended Complex Plane $\mathbb{C} \cup \{\infty\}$

- A correspondence between the set of all complex numbers and single-qubit states is given by

$$a|0\rangle + b|1\rangle \mapsto \frac{b}{a} = \alpha$$

- Its inverse is

$$\alpha \mapsto \frac{1}{\sqrt{1+|\alpha|^2}}|0\rangle + \frac{\alpha}{\sqrt{1+|\alpha|^2}}|1\rangle.$$

- The preceding mapping is not defined for the state with $a = 0$ and $b = 1$.
- To make this correspondence one-to-one we need to add a single point, which we label $\infty$, to the complex plane and define $\infty \leftrightarrow |1\rangle$.

# Example

- Consider the correspondence

$$a|0\rangle + b|1\rangle \mapsto \frac{b}{a} = \alpha,$$

with $\infty \leftrightarrow |1\rangle$.

We then have

$$\begin{array}{ll} |0\rangle \mapsto 0, & |1\rangle \mapsto \infty, \\ |+\rangle \mapsto +1, & |-\rangle \mapsto -1, \\ |\boldsymbol{i}\rangle \mapsto \boldsymbol{i}, & |-\boldsymbol{i}\rangle \mapsto -\boldsymbol{i}. \end{array}$$

# Geometric Model: Bloch Sphere

- Start with the previous representation.
- Consider a state represented by the complex number $\alpha = s + \boldsymbol{i}t$.
- The unit sphere in three real dimensions consists of the points $(x, y, z) \in \boldsymbol{C}$ satisfying $|x|^2 + |y|^2 + |z|^2 = 1$.
- We map $\alpha$ onto the sphere via the standard **stereographic projection**,

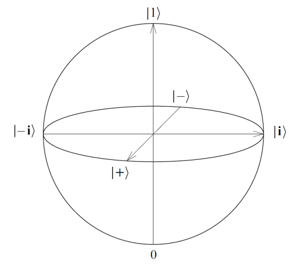
$$(s, t) \mapsto \left( \frac{2s}{|\alpha|^2 + 1}, \frac{2t}{|\alpha|^2 + 1}, \frac{1 - |\alpha|^2}{|\alpha|^2 + 1} \right).$$

Additionally, we require that $\infty \mapsto (0, 0, -1)$.

# Example

- We picture

$$(s,t) \mapsto \left(\frac{2s}{|\alpha|^2+1}, \frac{2t}{|\alpha|^2+1}, \frac{1-|\alpha|^2}{|\alpha|^2+1}\right).$$



Then we have

$$|0\rangle \mapsto (0,0,1), \quad |1\rangle \mapsto (0,0,-1),$$
$$|+\rangle \mapsto (1,0,0), \quad |-\rangle \mapsto (-1,0,0),$$
$$|\boldsymbol{i}\rangle \mapsto (0,1,0), \quad |-\boldsymbol{i}\rangle \mapsto (0,-1,0).$$

# Representations of the State Space

- We have given three representations of the quantum state space for a single-qubit system.
  1. Vectors written in ket notation: $a|0\rangle + b|1\rangle$ with complex coefficients $a$ and $b$, subject to $|a|^2 + |b|^2 = 1$, where $a$ and $b$ are unique up to a unit complex factor.

     Because of this global phase, this representation is not one-to-one.
  2. Extended complex plane: A single complex number $\alpha \in \mathbb{C}$ or $\infty$.

     This representation is one-to-one.
  3. Bloch sphere: Points $(x, y, z)$ on the unit sphere.

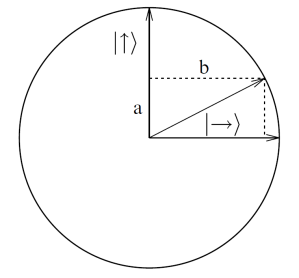
     This representation is also one-to-one.
- For historical reasons, the entire ball, including the interior, is called the **Bloch sphere**, instead of just the states on the surface, which truly form a sphere.
- For this reason, we refer to the state space of a single-qubit system as the **surface of the Bloch sphere**.

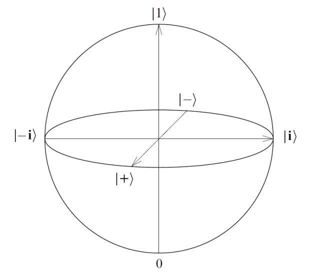
# Bases in Bloch Sphere

- One of the advantages of the Bloch sphere representation is that it is easy to read off all possible bases from the model.
  - Orthogonal states correspond to antipodal points of the Bloch sphere.
  - In particular, every diameter of the Bloch sphere corresponds to a basis for the single-qubit state space.

# Angles in Plane versus Bloch Sphere

- The representations





  differ in that the angles are half in the first than those in the Bloch sphere.

- The angle between two states on the plane has the usual relation to the inner product.
- In the Bloch sphere representation the angle is twice that of the angle in the inner product formula.