Quantum Computing

- Lecture 2 (April 24, 2025)

- Today:
  - Quantum state, qubit, and their linear algebra formulation

Qubit

- A **qubit** describes the quantum state of a quantum system
- Abstracted as a mathematical object (i.e., ignore their physical meanings…)

- Two "basic" states $|0\rangle$, $|1\rangle$
  - Dirac (Bra-ket) notations
  - In some research papers, $|\ \rangle$ is also called a quantum register

- We describe the **superposition** state of the system using the qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The numbers α and β are **complex number** and $|\alpha|^2 + |\beta|^2 = 1$

Qubit

- We describe the state of a system using the **single** qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The numbers α and β are **complex number** and $|\alpha|^2 + |\beta|^2 = 1$

Qubit

- We describe the state of a system using the **single** qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The numbers α and β are **complex number** and $|\alpha|^2 + |\beta|^2 = 1$

Superposition (for single qubit, informal): $|\boldsymbol{\phi}\rangle$ **cannot be written as either** $|\mathbf{0}\rangle$ **or** $|\mathbf{1}\rangle$

Qubit

- We describe the state of a system using the **single** qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The numbers α and β are **complex number** and $|\alpha|^2 + |\beta|^2 = 1$

A quick recap of complex numbers $\mathbb{C}$:

- A complex number $\alpha \in \mathbb{C}$ can be written as $\boldsymbol{\alpha = a + bi}$, where a, b are real numbers, and $i = \sqrt{-1}$
- If $\alpha \in \mathbb{C}$ and $\alpha = a + bi$, then we write its **conjugate** as $\boldsymbol{\alpha^* = a - bi}$
- We write α's **norm** as $|\alpha| = \left|\sqrt{a^2 + b^2}\right|$. We always have $|\alpha| = |\alpha^*| = \left|\sqrt{\alpha\alpha^*}\right|$

- If $|\boldsymbol{\alpha}| = 1$, then $\boldsymbol{\alpha}$ can also be written as $\boldsymbol{\alpha} = \cos\boldsymbol{\theta} + \boldsymbol{i}\sin\boldsymbol{\theta}$ for some $\boldsymbol{\theta}$.
- By Euler's formula, $\boldsymbol{\alpha} = \cos\boldsymbol{x} + \boldsymbol{i}\sin\boldsymbol{x} = \boldsymbol{e^{ix}}$, and $|\boldsymbol{e^{ix}}| = \boldsymbol{1}$

Qubit

- We describe the state of a system using the **single** qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The numbers α and β are **complex number** and $|\alpha|^2 + |\beta|^2 = 1$

- **Examples:**

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad \cos\theta\,|0\rangle + e^{i\psi}\sin\theta\,|1\rangle$$

Qubit as a unit vector

- We describe the state of a system using the **single** qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The numbers α and β are **complex number** and $|\alpha|^2 + |\beta|^2 = 1$

- **Relation between $|0\rangle$ and $|1\rangle$:**
  - They should be **"easy" to distinguish**
  - Linear algebra representation:

$$|0\rangle \coloneqq \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Qubit as a unit vector

Some linear algebra:

- Focus on vector spaces over $\mathbb{C}$
- Linear (in)dependence, basis, orthonormal basis, transpose, adjoint, …

$|0\rangle \coloneqq \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\langle 0| \coloneqq [1^* \quad 0^*] (= [1 \quad 0])$, or more generally, if $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, then $\langle \psi| = [\alpha^* \quad \beta^*]$

- We call $|\psi\rangle$ a **"ket"** and $\langle\psi|$ a **"bra"**
- Inner product using Dirac (Bra-ket) notations: $\langle\phi|\psi\rangle$
- Easy to see $\langle 0|1\rangle = \langle 1|0\rangle = 0$ and $\langle 0|0\rangle = 1 = \langle 1|1\rangle$

Qubit as a unit vector

- We describe the state of a system using the **single** qubit:
  - The numbers α and β are **complex numbers**

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$= \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2$$

  - A single qubit is a **unit vector over** $\mathbb{C}^2$

$$\| |\phi\rangle \| = \sqrt{\langle\phi|\phi\rangle} = \sqrt{|\alpha|^2 + |\beta|^2} = 1$$

- Change basis:

$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ is a basis of $\mathbb{C}^2$ (known as **computational basis**)

$\left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$ is also a basis of $\mathbb{C}^2$

Qubit in Different Bases

- Single qubit: $|\phi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \in \mathbb{C}^2, \| |\phi\rangle \| = 1$
- Change basis: $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$ is a basis of $\mathbb{C}^{\mathbf{2}}$ (known as the **computational basis**)

  $\left\{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right\}$ is also a basis of $\mathbb{C}^{\mathbf{2}}$.

- Let $|\nearrow\rangle \coloneqq \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ and $|\searrow\rangle \coloneqq \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$, then:

$$|\phi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}\,|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|\searrow\rangle$$

Qubit in Different Bases

- Single qubit: $|\phi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \in \mathbb{C}^2, \||\phi\rangle\| = 1$

- Described by different bases:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

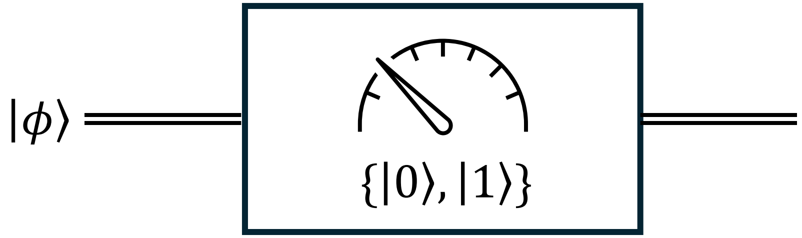
$$|\phi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}|\searrow\rangle$$

- What do they mean? **Depends on measurement** (will be introduced later)

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \in \mathbb{C}^2$

- If we measure $|\phi\rangle$ **in the computational basis** $\{|0\rangle, |1\rangle\}$:

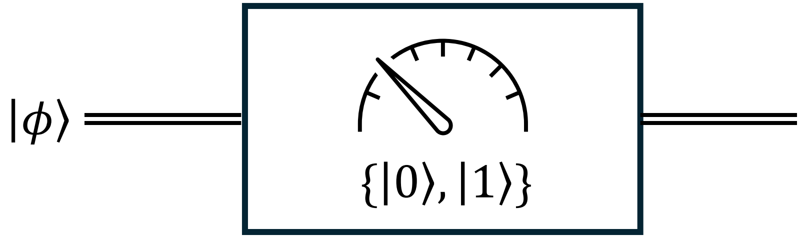


$$b = \begin{cases} 0 & \text{with probability } \alpha^2 \\ 1 & \text{with probability } \beta^2 \end{cases}$$

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}|\searrow\rangle$

- If we measure $|\phi\rangle$ **in the computational basis** $\{|0\rangle, |1\rangle\}$:



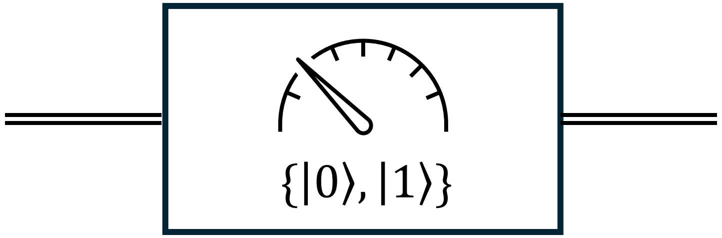
$$b = \begin{cases} 0 & \text{with probability } \alpha^2 \\ 1 & \text{with probability } \beta^2 \end{cases}$$

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}|\searrow\rangle$

- If we measure $|\phi\rangle$ **in the computational basis** $\{|0\rangle, |1\rangle\}$:

$|\phi\rangle$



$$b = \begin{cases} 0 & \text{with probability } \alpha^2 \\ 1 & \text{with probability } \beta^2 \end{cases}$$

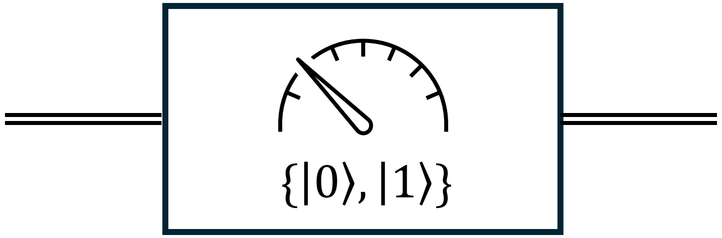
- If we measure $|\phi\rangle$ **in the basis** $\{|\nearrow\rangle, |\searrow\rangle\}$:

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}\,|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|\searrow\rangle$

- If we measure $|\phi\rangle$ **in the computational basis** $\{|0\rangle, |1\rangle\}$:

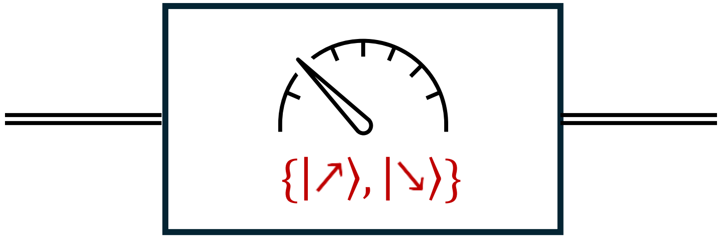
$|\phi\rangle$



$$b = \begin{cases} 0 & \text{with probability } \alpha^2 \\ 1 & \text{with probability } \beta^2 \end{cases}$$

- If we measure $|\phi\rangle$ **in the basis** $\{|\nearrow\rangle, |\searrow\rangle\}$:

$|\phi\rangle$



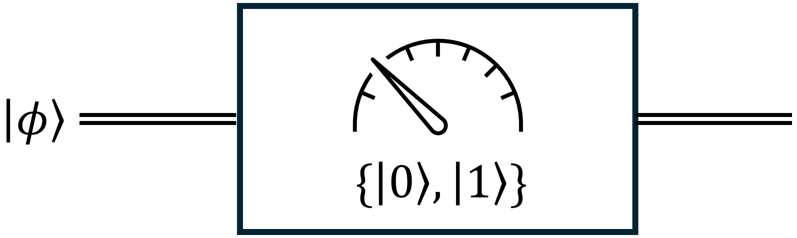
$$b = \begin{cases} \nearrow & \text{with probability } \left|\left(\frac{\alpha+\beta}{\sqrt{2}}\right)\right|^2 \\ \searrow & \text{with probability } \left|\left(\frac{\alpha-\beta}{\sqrt{2}}\right)\right|^2 \end{cases}$$

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}|\searrow\rangle$

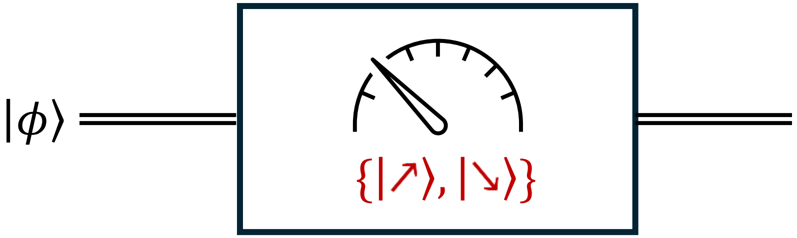
It depends on how you define 0, 1, ↗, ↘, … (i.e., how you encode the information and define its measurement)

- If we measure $|\phi\rangle$ **in the computational basis** $\{|0\rangle, |1\rangle\}$:



$$b = \begin{cases} 0 & \text{with probability } \alpha^2 \\ 1 & \text{with probability } \beta^2 \end{cases}$$

- If we measure $|\phi\rangle$ **in the basis** $\{|\nearrow\rangle, |\searrow\rangle\}$:



$$b = \begin{cases} \nearrow & \text{with probability } \left|\left(\frac{\alpha+\beta}{\sqrt{2}}\right)\right|^2 \\ \searrow & \text{with probability } \left|\left(\frac{\alpha-\beta}{\sqrt{2}}\right)\right|^2 \end{cases}$$

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Notes:

1. We may also call α and β as amplitudes
2. Why complex numbers? A natural way for describing waves (amplitude + phase)

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Wrong: The qubit is $|0\rangle$ with probability $|\alpha|^2$ and is $|1\rangle$ with probability $|\beta|^2$

Correct: The qubit is in a superposition before measurement – in both $|0\rangle$ and $|1\rangle$ at once

Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Can we estimate α and β by measuring $|\phi\rangle$ many times?

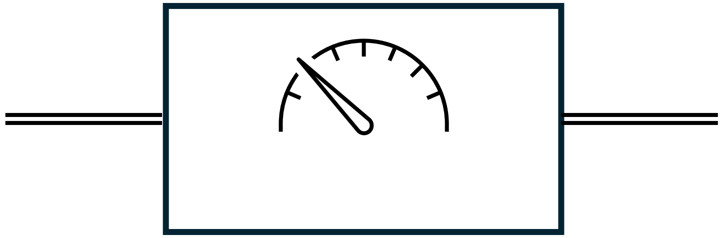
Single qubit measurement

- Single qubit: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Can we estimate α and β by measuring $|\phi\rangle$ many times?

No. Because of collapse and no-cloning...

$|\phi\rangle$



$$b = \begin{cases} 0 & \text{with probability } \alpha^2 \\ 1 & \text{with probability } \beta^2 \end{cases}$$

$|\phi\rangle$ becomes $|b\rangle$ after measurement...

Inner/Outer Product

- Let $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a qubit
- Inner product (to see adjoint and linearity):

$$\langle\phi|\phi\rangle = \langle\phi| \cdot |\phi\rangle = (\alpha^*\langle 0| + \beta^*\langle 1|) \cdot (\alpha|0\rangle + \beta|1\rangle) = \cdots = 1$$

- Outer product: $|\phi\rangle\langle\phi|$

$$|\phi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}, \langle\phi| = [\alpha^* \quad \beta^*], |\phi\rangle\langle\phi| = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \cdot [\alpha^* \quad \beta^*] = \text{(a 2 x 2 matrix)}$$

Inner/Outer Product

- Let $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a qubit
- Inner product (to see adjoint and linearity):

$$\langle\phi|\phi\rangle = \langle\phi| \cdot |\phi\rangle = (\alpha^*\langle 0| + \beta^*\langle 1|) \cdot (\alpha|0\rangle + \beta|1\rangle) = \cdots = 1$$

- Outer product: $|\phi\rangle\langle\phi|$

$$|\phi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}, \langle\phi| = [\alpha^* \quad \beta^*], |\phi\rangle\langle\phi| = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \cdot [\alpha^* \quad \beta^*] = \text{(a 2 x 2 matrix)}$$

What does $|\phi\rangle\langle\phi|$ represents? A **projector** that project a vector onto the “line” (one-dimension linear space) spanned by $|\phi\rangle$.

Tensor Product

- Let $\mathbf{A}$ $(n_1 \times m_1)$ and $\mathbf{B}$ $(n_2 \times m_2)$ be two arbitrary complex matrices, where

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m_1} \\ \vdots & \ddots & \vdots \\ a_{n_1,1} & \cdots & a_{n_1,m_1} \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} b_{1,1} & \cdots & b_{1,m_2} \\ \vdots & \ddots & \vdots \\ b_{n_2,1} & \cdots & b_{n_2,m_2} \end{bmatrix}$$

- Then the **tensor product** of $\mathbf{A}$ and $\mathbf{B}$, denoted as $\mathbf{A} \otimes \mathbf{B}$, is defined by

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{1,1}\mathbf{B} & \cdots & a_{1,m_1}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{n_1,1}\mathbf{B} & \cdots & a_{n_1,m_1}\mathbf{B} \end{bmatrix}$$, which is a $\boldsymbol{n_1 n_2} \times \boldsymbol{m_1 m_1}$ matrix

Tensor Product

- Let $\mathbf{A}$ $(n_1 \times m_1)$ and $\mathbf{B}$ $(n_2 \times m_2)$ be two arbitrary complex matrices, where

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m_1} \\ \vdots & \ddots & \vdots \\ a_{n_1,1} & \cdots & a_{n_1,m_1} \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} b_{1,1} & \cdots & b_{1,m_2} \\ \vdots & \ddots & \vdots \\ b_{n_2,1} & \cdots & b_{n_2,m_2} \end{bmatrix}$$

- Then the **tensor product** of $\mathbf{A}$ and $\mathbf{B}$, denoted as $\mathbf{A} \otimes \mathbf{B}$, is defined by

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{1,1}\mathbf{B} & \cdots & a_{1,m_1}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{n_1,1}\mathbf{B} & \cdots & a_{n_1,m_1}\mathbf{B} \end{bmatrix}$$, which is a $\boldsymbol{n_1 n_2} \times \boldsymbol{m_1 m_1}$ matrix

- One can define **tensor product for vectors** in a natural way.
- We use tensor product to define **multiple qubits**

Multiple Qubits

- In the classical world, an n-bit string has 2^n possibilities (i.e., 2^n basic states)
- We define multiple qubits (in the **computational basis**) by an analogous way.

Multiple Qubits

- Multiple (n) qubits **in the computational basis.**

- 2^n basic states: $|00\cdots00\rangle, |00\cdots01\rangle, |00\cdots10\rangle, |00\cdots11\rangle, \ldots, |11\cdots11\rangle$, where

$$|b_{n-1}b_{n-2}\cdots b_1 b_0\rangle \coloneqq |b_{n-1}\rangle \otimes |b_{n-2}\rangle \otimes \cdots \otimes |b_1\rangle \otimes |b_0\rangle$$

- More compact representation:

$$|0\rangle, |1\rangle, |2\rangle, |3\rangle, \ldots, |2^n - 1\rangle$$

- An ***n*-qubit states**: A **superposition** of the 2^n basic states (also a **unit vector over** $\mathbb{C}^{\boldsymbol{2^n}}$)

$$|\boldsymbol{\phi}\rangle = \sum_{i=0}^{2^n-1} \alpha_i \, |i\rangle,$$

where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Multiple Qubits

- Multiple qubits **in an arbitrary orthonormal basis:** $|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_{N-1}\rangle$

- A more general representation:

$$|\boldsymbol{\phi}\rangle = \sum_{i=0}^{N-1} \alpha_i \, |\phi_i\rangle,$$

where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{N-1} |\alpha_i|^2 = 1$

Next Topic

- Linear Operators, Unitaries, Quantum Gates, Entanglement, …
- More linear algebra

- Next Wednesday: **~50min lecture** + **40min exercise & explanation**
  - **Bring your pen and paper** (and also your laptop/iPad to check the lecture notes)

References

- **[NC00]** *Quantum Computation and Quantum Information.* Michael **N**ielsen and Isaac **C**huang
  - Section 1.2 (**Bloch sphere representation** of a qubit)
  - Sections 2.1.1 – 2.1.3
- **[KLM07]** *An Introduction to Quantum Computing.* Phillip **K**aye, Raymond **L**aflamme, Michele **M**osca
  - Sections 2.1, 2.2, and 2.6
- **[RP11]** *Quantum Computing: A Gentle Introduction.* Eleanor **R**ieffel and Wolfgang **P**olak
  - Sections 2.1-2.2, 3.1
- Professor Mark Zhandry's lecture note.
- Professor Henry Yuen's lecture note.