Mathematical Tools for Quantum Computing

CPSC 4470/5470

Introduction to Quantum Computing

Instructor: Prof. **Yongshan Ding**

Computer Science, Applied Physics, Yale Quantum Institute

Mathematical Model of Quantum Systems

Four Principles to model quantum systems mathematically:

1. **Superposition:**
   The state of a qubit is a unit complex vector in the two-dimensional *Hilbert Space*.
2. **Composition:**
   The joint state of many (independent) quantum systems is the *tensor product* of component states.
3. **Transformation:**
   Time evolution of a quantum system is a *unitary process*.
4. **Measurement:**
   Measuring a quantum state causes its superposition to *collapse/project* to one of its basis states randomly.

Von Neumann: *“In mathematics, you don’t understand things. You just get used to them.”*

Superposition State of A Qubit

The **state of a qubit** is represented by a unit vector in the two-dimensional complex vector space (**Hilbert Space** $\mathbb{C}^2$). In the Dirac notation:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

where $\alpha, \beta \in \mathbb{C}$, satisfying that its 2-norm: $|\alpha|^2 + |\beta|^2 = 1$.

Here, α and β are called the **probability amplitudes** on the (classical) basis, $|0\rangle$ and $|1\rangle$, respectively.

(can be negative, even complex numbers)

$$|\psi\rangle = 0.6|0\rangle - 0.8|1\rangle = \begin{bmatrix}0.6\\ -0.8\end{bmatrix}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix}$$

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

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

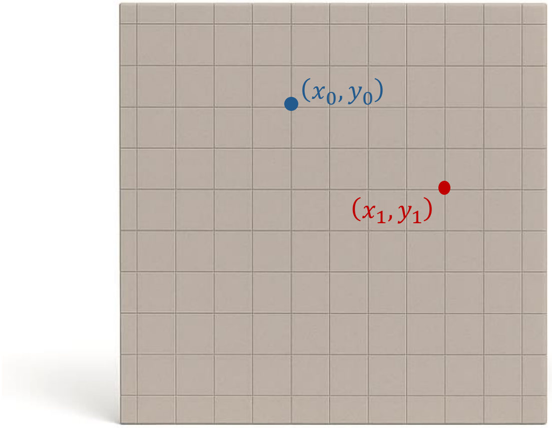
Not valid: $\frac{1}{4}|0\rangle + \frac{i}{2}|1\rangle = \begin{bmatrix}1/4\\ i/2\end{bmatrix}$

Vector Spaces

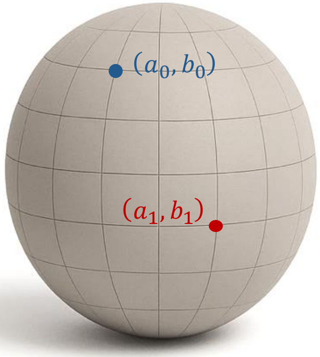
Vector space: a (special) set of vectors.

Example: Position vectors for points on a 2D surface.
$\mathbb{R}^2$: Two-dimensional real vector space

Position on a flat surface: X-y plane



Surface of a sphere: Longitude-latitude



Two real-valued coordinates.

Algebra: that allows us to take linear combinations.

- Scalar multiplication: $c \cdot \vec{a} = \begin{bmatrix} ca_0 \\ ca_1 \end{bmatrix}$ for some $c \in \mathbb{R}$
- Vector addition: $\vec{a} + \vec{b} = \begin{bmatrix} a_0 + b_0 \\ a_1 + b_1 \end{bmatrix}$

"Vectors after algebra remain in the same space."

$\mathbb{R}^n$: n-dimensional real vector space:

all vectors with n real components: $\vec{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \in \mathbb{R}^n$

More about Vectors

$\vec{a}^T$: Transpose of $\vec{a}$

Properties (<u>derive on board</u>):

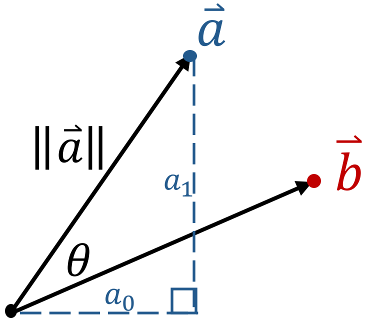
- **Length** of a vector (as in ℓ_2-norm or Euclidean norm): $\vec{a} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$

$$\|\vec{a}\|_2^2 = \vec{a}^T\vec{a}$$

- **Angle** between two vectors: $\vec{a} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$ and $\vec{b} = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$

$$\|\vec{a}\| \cdot \|\vec{b}\| \cos\theta = \vec{a}^T\vec{b}$$

Inner product of $\vec{a}$ and $\vec{b}$: $\vec{a}^T\vec{b}$



Origin: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$

Hilbert space: inner-product vector space.

- Well-defined “geometry” (incl. length and angle).

Do they work for complex vectors?

What about Complex Vectors?

A **complex number** $\alpha \in \mathbb{C}$ is of form:

$$\alpha = \underbrace{a_0}_{\text{Real component}} + \overbrace{a_1}^{\text{Imaginary component}} i$$

Where $a_0, a_1 \in \mathbb{R}$ and $i^2 = -1$.

A vector in a two-dimensional complex vector space:

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \in \mathbb{C}^2$$

Can we use the same definition for length and angle?

- Length:

$$\vec{a}^T \vec{a} = \|\vec{a}\|_2^2$$

- Angle:

$$\vec{a}^T \vec{b} = \|\vec{a}\| \cdot \|\vec{b}\| \cos\theta$$

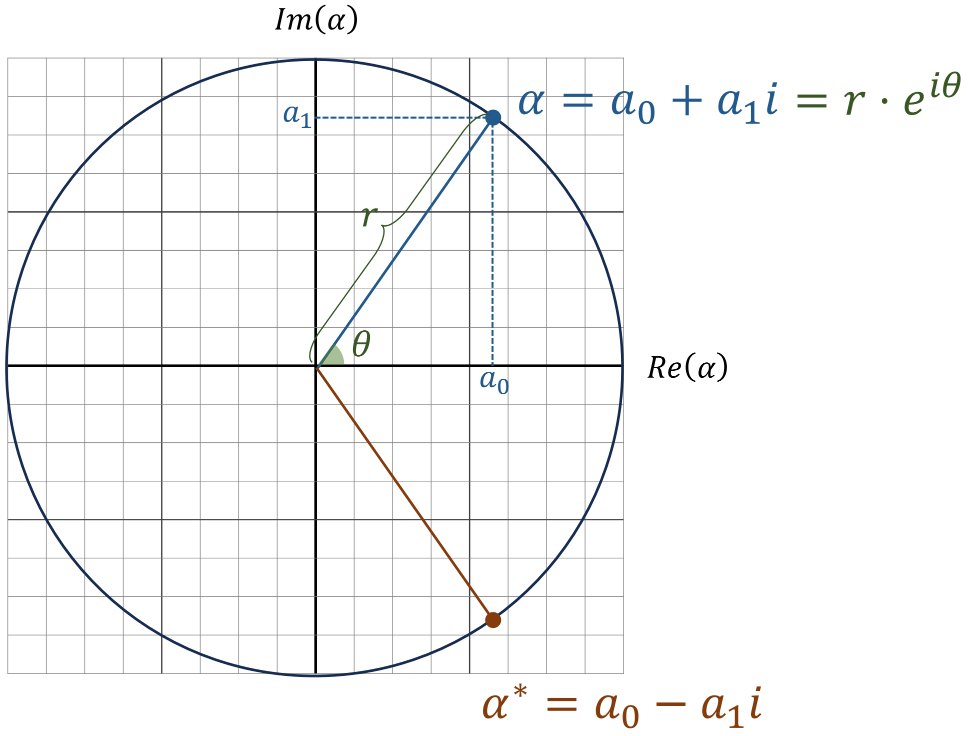
What could be problematic?

Example: Length of $|\psi\rangle = \begin{bmatrix} 1 \\ i \end{bmatrix}$?

Complex Numbers

A **complex number** $\alpha \in \mathbb{C}$ is of form: $\alpha = a_0 + a_1 i$, where $a_0, a_1 \in \mathbb{R}$ and $i^2 = -1$.

Complex Plane:



Cartesian coordinate (a_0, a_1) : (real, imaginary)

$$\alpha = a_0 + a_1 i$$

Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$

Polar coordinate (r, θ) : (magnitude, phase)

$$\alpha = r\cos\theta + r\sin\theta\, i = r \cdot e^{i\theta}$$

"length" "angle"

"Length": Magnitude $r = |\alpha| = \sqrt{a_0^2 + a_1^2} = \sqrt{\alpha^*\alpha}$

"Angle": Complex phase $\theta = \arctan\frac{a_1}{a_0}$

Notation: α^* is the complex conjugate of α

$$\alpha^* = a_0 - a_1 i = r \cdot e^{-i\theta}$$

Back to Complex Vectors

For a **quantum state** $|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$:

What are $\langle\psi|\psi\rangle$, $\langle 0|\psi\rangle$ and $\langle 1|\psi\rangle$?

Algebra:

- Scalar multiplication: $c \cdot |\psi\rangle = \begin{bmatrix} c\alpha_0 \\ c\alpha_1 \end{bmatrix}$ for some $c \in \mathbb{C}$
- Vector addition: $|\psi\rangle + |\varphi\rangle = \begin{bmatrix} \alpha_0 + \beta_0 \\ \alpha_1 + \beta_1 \end{bmatrix}$

Properties (derive on board):

“Ket”

- Length of a vector: $|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$

$$\| |\psi\rangle \|_2^2 = [\alpha_0^* \quad \alpha_1^*] \cdot \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

Example: Length of $|\psi\rangle = \begin{bmatrix} 1 \\ i \end{bmatrix}$

- Angle between two vectors: $|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$ and $|\varphi\rangle = \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix}$

$$\cos\theta = [\alpha_0^* \quad \alpha_1^*] \cdot \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix}$$

Dirac Notation:

$$\langle\psi| = (|\psi\rangle)^\dagger = (|\psi\rangle^*)^T = [\alpha_0^* \quad \alpha_1^*]$$

“Bra”

Adjoint of a vector: conjugate transpose

$$\langle\psi| \cdot |\psi\rangle = \langle\psi|\psi\rangle$$

Inner product: “Bra-ket”

$$\langle\psi| \cdot |\varphi\rangle = \langle\psi|\varphi\rangle$$

What about more qubits?

Two coins:

$$\Pr(0_A) = 0.36\,,\Pr(1_A) = 0.64 \qquad \Pr(0_B) = 0.5\,,\Pr(1_B) = 0.5$$

Assuming they are independent: $\Pr(0_A 0_B) = \Pr(0_A) \cdot \Pr(0_B)$

$$\begin{aligned} \Pr(0_A 0_B) &= 0.36 \cdot 0.5, & \Pr(0_A 1_B) &= 0.36 \cdot 0.5, \\ \Pr(1_A 0_B) &= 0.64 \cdot 0.5, & \Pr(1_A 1_B) &= 0.64 \cdot 0.5, \end{aligned}$$

We use a “joint state” to fully characterize the system:

Tensor product:

$$\begin{bmatrix} 0.36 \\ 0.64 \end{bmatrix} \otimes \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix} = \begin{bmatrix} 0.36 \cdot \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix} \\ 0.64 \cdot \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix} \end{bmatrix} = \begin{array}{cl} \begin{bmatrix} 0.36 \cdot 0.5 \\ 0.36 \cdot 0.5 \\ 0.64 \cdot 0.5 \\ 0.64 \cdot 0.5 \end{bmatrix} & \begin{matrix} \Pr(0_A 0_B) \\ \Pr(0_A 1_B) \\ \Pr(1_A 0_B) \\ \Pr(1_A 1_B) \end{matrix} \end{array}$$

Two qubits:

$$|\psi_A\rangle = 0.6|0\rangle + 0.8|1\rangle \qquad |\psi_B\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Assuming they are independent: $\langle 0_A 0_B | \psi_{AB} \rangle = \langle 0_A | \psi_A \rangle \cdot \langle 0_B | \psi_B \rangle$

$$|\psi_{AB}\rangle = 0.6 \cdot \frac{1}{\sqrt{2}}|00\rangle - 0.6 \cdot \frac{1}{\sqrt{2}}|01\rangle + 0.8 \cdot \frac{1}{\sqrt{2}}|10\rangle - 0.8 \cdot \frac{1}{\sqrt{2}}|11\rangle$$

$$\begin{bmatrix} 0.6 \\ 0.8 \end{bmatrix} \otimes \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} = \begin{array}{cl} \begin{bmatrix} 0.6 \cdot 1/\sqrt{2} \\ -0.6 \cdot 1/\sqrt{2} \\ 0.8 \cdot 1/\sqrt{2} \\ -0.8 \cdot 1/\sqrt{2} \end{bmatrix} & \begin{matrix} |0_A 0_B\rangle \\ |0_A 1_B\rangle \\ |1_A 0_B\rangle \\ |1_A 1_B\rangle \end{matrix} \end{array}$$

High-Dimensional Complex Hilbert Space

The **joint state of n qubit** is a 2^n-dimensional complex vector in the **Hilbert Space** $\mathcal{H}$, described by complex numbers, $\alpha_i \in \mathbb{C}$, for $i \in \{0,1\}^n$, satisfying that its 2-norm: $\sum_{i\in\{0,1\}^n} |\alpha_i|^2 = 1$. In the Dirac notation:

$$|\psi\rangle = \alpha_{00\ldots0}|00\ldots0\rangle + \alpha_{00\ldots1}|00\ldots1\rangle + \cdots + \alpha_{11\ldots1}|11\ldots1\rangle = \begin{bmatrix} \alpha_{00\ldots0} \\ \alpha_{00\ldots1} \\ \vdots \\ \alpha_{11\ldots1} \end{bmatrix} \in \mathcal{H} = \mathbb{C}^{2^n}$$

Inner product: $\langle\psi|\psi\rangle = \begin{bmatrix} \alpha^*_{00\ldots0} & \alpha^*_{00\ldots0} & \ldots & \alpha^*_{00\ldots0} \end{bmatrix} \begin{bmatrix} \alpha_{00\ldots0} \\ \alpha_{00\ldots1} \\ \vdots \\ \alpha_{11\ldots1} \end{bmatrix} = \sum_{i\in\{0,1\}^n} \alpha_i^* \alpha_i = 1$ Normalized. ✅

This is a linear combination over 2^n basis states: $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$.

Change of Basis?

$$|\psi\rangle = 0.6|0\rangle + 0.8|1\rangle$$

Standard basis: $\begin{cases} |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \\ |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \end{cases}$

Derive on board:

$$|\psi\rangle = \;?\,|+\rangle + \;?\,|-\rangle$$

Define an alternative basis:

$$\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{cases}$$

What about the following basis for $|\psi\rangle$?

$$\begin{cases} |v\rangle = |0\rangle + i|1\rangle \\ |w\rangle = |0\rangle - i|1\rangle \end{cases}$$

What are the criteria for a “good” basis?

Orthonormal Basis

Span: A set of vectors $|v_0\rangle, |v_1\rangle, \dots, |v_{n-1}\rangle$ *spans* the vector space S, if for any vector $|w\rangle \in S$, there exists $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{C}$:

$$|w\rangle = \underbrace{\alpha_0|v_0\rangle + \alpha_1|v_1\rangle + \cdots + \alpha_{n-1}|v_{n-1}\rangle}_{\text{Linear combination (with complex coefficients)}}$$

Linear dependence: A set of (non-zero) vectors are *linearly dependent* if there exists $\alpha_0, \dots, \alpha_{n-1}$ not all zero:

$$0 = \alpha_0|v_0\rangle + \alpha_1|v_1\rangle + \cdots + \alpha_{n-1}|v_{n-1}\rangle$$

Basis: *linearly independent* vectors *spans* the vector space S.

Orthonormal basis:

- Length: A set of unit vectors
- Angle: mutually orthogonal

$$\langle v_j|v_k\rangle = \begin{cases} 1, \text{ if } j = k \text{ (unit length)} \\ 0, \text{ if } j \neq k \text{ (orthogonal)} \end{cases}$$

Examples: two-qubit basis

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$|++\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}, |+-\rangle = \frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix}, |-+\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix}, |--\rangle = \frac{1}{2}\begin{bmatrix}1\\-1\\-1\\1\end{bmatrix}$$

$|+\rangle \otimes |+\rangle$

The Process of Evolving a Probabilistic State

A **Markov Process** is a stochastic process over a state space S such that:

$$\Pr[S_{t+1} = s' | S_t = s, S_{t-1} = s_{t-1}, \ldots, S_0 = s_0] = \Pr[S_{t+1} = s' | S_t = s]$$

For all state $s_t \in S$ at time t.

Transition probability (from s to s'):

$$\Pr[S_{t+1} = s' | S_t = s]$$

Example:
A 3-bit Markov Model for CPSC 4470 student:

Ⓟ Phone out? (0 = away, 1 = out)

Ⓓ Discussing? (0 = quiet, 1 = participating)

Ⓤ Understanding now? (0 = lost, 1 = get)

Eight possible states ($s \in S$):

0	Ⓟ Ⓓ Ⓤ	Silently lost
1	Ⓟ Ⓓ Ⓤ	Zen absorber
2	Ⓟ Ⓓ Ⓤ	Eager-but-lost
3	Ⓟ Ⓓ Ⓤ	Classroom king
4	Ⓟ Ⓓ Ⓤ	Doomscrolling
5	Ⓟ Ⓓ Ⓤ	Overconfident texter
6	Ⓟ Ⓓ Ⓤ	Clueless chaos
7	Ⓟ Ⓓ Ⓤ	Mythical Multitasker

A **transition matrix** to fully characterize the process.

FROM

TO

$$\begin{array}{c|cccccccc|}
 & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\
000 & 0.5 & 0.2 & & & 0.25 & & & \\
001 & 0.3 & 0.5 & & 0.3 & & 0.25 & & \\
010 & 0.2 & & 0.5 & 0.2 & & & 0.25 & \\
011 & & 0.3 & 0.5 & 0.5 & & & & 0.3 \\
100 & & & & & 0.5 & & & \\
101 & & & & & & 0.5 & & 0.2 \\
110 & & & & & 0.15 & & 0.5 & \\
111 & & & & & 0.1 & 0.25 & 0.25 & 0.5
\end{array}$$

Col-k, Row-j of the matrix:

$$T[k, j] = \Pr[S_{t+1} = k | S_t = j]$$

- Non-negative elements.
- Columns sum to 1.

The Process of Evolving a Probabilistic State

Probabilistic mixture of possible states:

0	P D U	Silently lost
1	P D U	Zen absorber
2	P D U	Eager-but-lost
3	P D U	Classroom king
4	P D U	Doomscrolling
5	P D U	Overconfident texter
6	P D U	Clueless chaos
7	P D U	Mythical Multitasker

$$\vec{p_t} = \begin{bmatrix} \Pr[S_t = 0] \\ \Pr[S_t = 1] \\ \Pr[S_t = 2] \\ \Pr[S_t = 3] \\ \Pr[S_t = 4] \\ \Pr[S_t = 5] \\ \Pr[S_t = 6] \\ \Pr[S_t = 7] \end{bmatrix}$$

Evolution of probabilistic state:

$$\vec{p_{t+1}} = T \cdot \vec{p_t}$$

Transition matrix

Three stages of the class:

Output state

Input state

T_0: “Staying engaged”

$$\begin{bmatrix} 0.2 \\ 0.5 \\ \\ 0.3 \\ \\ \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 0.5 & 0.2 & & & 0.25 & & & \\ 0.3 & 0.5 & & 0.3 & & 0.25 & & \\ 0.2 & & 0.5 & 0.2 & & & 0.25 & \\ & 0.3 & 0.5 & 0.5 & & & & 0.3 \\ & & & & 0.5 & & & \\ & & & & & 0.5 & & 0.2 \\ & & & & 0.15 & & 0.5 & \\ & & & & 0.1 & 0.25 & 0.25 & 0.5 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

T_1: “Drifting”

$$\begin{bmatrix} 0.22 \\ 0.46 \\ 0.1 \\ 0.17 \\ 0.05 \\ \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 0.6 & 0.2 & 0.2 & & 0.2 & & & \\ 0.2 & 0.6 & & 0.4 & & 0.2 & & \\ 0.2 & & 0.6 & 0.2 & & & 0.2 & \\ & 0.1 & 0.2 & 0.4 & & & & 0.2 \\ & 0.1 & & & 0.7 & 0.2 & & \\ & & & & & 0.4 & & 0.2 \\ & & & & 0.1 & & 0.6 & 0.2 \\ & & & & & 0.2 & 0.2 & 0.4 \end{bmatrix} \cdot \begin{bmatrix} 0.2 \\ 0.5 \\ 0 \\ 0.3 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

T_2: “Fatigue + bounce back”

$$\begin{bmatrix} 0.1925 \\ 0.4475 \\ 0.128 \\ 0.207 \\ 0.02 \\ 0.005 \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 0.4 & 0.2 & & & 0.25 & & & \\ 0.4 & 0.6 & 0.2 & 0.3 & 0.25 & 0.25 & & \\ 0.2 & & 0.5 & 0.2 & & & 0.1 & \\ & 0.2 & 0.3 & 0.5 & & & & 0.3 \\ & & & & 0.4 & & 0.15 & \\ & & & & 0.1 & 0.5 & & 0.2 \\ & & & & & & 0.5 & \\ & & & & & 0.25 & 0.25 & 0.5 \end{bmatrix} \cdot \begin{bmatrix} 0.22 \\ 0.46 \\ 0.1 \\ 0.17 \\ 0.05 \\ \\ \\ \\ \end{bmatrix}$$

The Process of Evolving a Superposition State

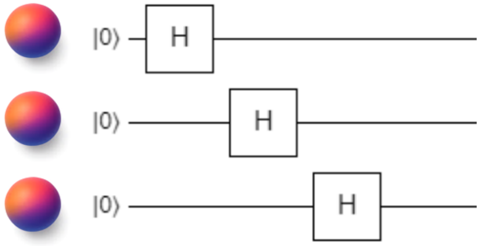
Superposition of possible states:

$$|\psi_t\rangle = \begin{bmatrix} \alpha_{00\ldots0} \\ \alpha_{00\ldots1} \\ \vdots \\ \alpha_{11\ldots1} \end{bmatrix}$$

Evolution of superposition state:

$$|\psi_{t+1}\rangle = U \cdot |\psi_t\rangle$$

Unitary matrix



Apply three quantum gates:

Output state

Input state

$$U_0 = H \otimes I \otimes I$$

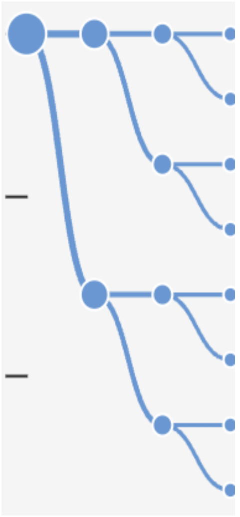
$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ \\ \\ \\ 1 \\ \\ \\ \\ \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & & & & 1 & & & \\ & 1 & & & & 1 & & \\ & & 1 & & & & 1 & \\ & & & 1 & & & & 1 \\ 1 & & & & -1 & & & \\ & 1 & & & & -1 & & \\ & & 1 & & & & -1 & \\ & & & 1 & & & & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$U_1 = I \otimes H \otimes I$$

$$\frac{1}{2}\begin{bmatrix} 1 \\ \\ 1 \\ \\ 1 \\ \\ 1 \\ \\ \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & & 1 & & & & & \\ & 1 & & 1 & & & & \\ 1 & & -1 & & & & & \\ & 1 & & -1 & & & & \\ & & & & 1 & & 1 & \\ & & & & & 1 & & 1 \\ & & & & 1 & & -1 & \\ & & & & & 1 & & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ \\ \\ \\ 1 \\ \\ \\ \\ \end{bmatrix}$$

$$U_2 = I \otimes I \otimes H$$

$$\frac{1}{2\sqrt{2}}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & & & & & & \\ 1 & -1 & & & & & & \\ & & 1 & 1 & & & & \\ & & 1 & -1 & & & & \\ & & & & 1 & 1 & & \\ & & & & 1 & -1 & & \\ & & & & & & 1 & 1 \\ & & & & & & 1 & -1 \end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix} 1 \\ \\ 1 \\ \\ 1 \\ \\ 1 \\ \\ \end{bmatrix}$$



Geometry-Preserving Transformations

Inner product gives the length and angle of vectors:

Real vectors: $\overrightarrow{v_j}^T \overrightarrow{v_k}$ Complex vectors: $\langle v_j | v_k \rangle$

Transformations that preserves "geometry": lengths and angles.

- Orthonormal basis stays orthonormal.
- Shapes don't get stretched.

	Orthogonal Matrix	**Unitary Matrix**
Definition	$Q^T Q = I$	$U^\dagger U = I$
Inverse	$Q^{-1} = Q^T$	$U^{-1} = U^\dagger$
Columns	Real orthonormal vectors	Complex orthonormal vectors
Example	2D rotation matrix	Quantum gates

Principle #3: Transformation

(More details in Lecture 5.)

Understanding Projections

Derive on board:

$\Pi_0 = \frac{|0\rangle\langle 0|}{\langle 0|0\rangle}$, What is $\Pi_0|\psi\rangle$?

Principle #4: Measurements

(More details in Lecture 6.)

Projection (as a “linear operator”: mapping from one vector space to another)

Example:
3D object casting shadows onto 2D plane.

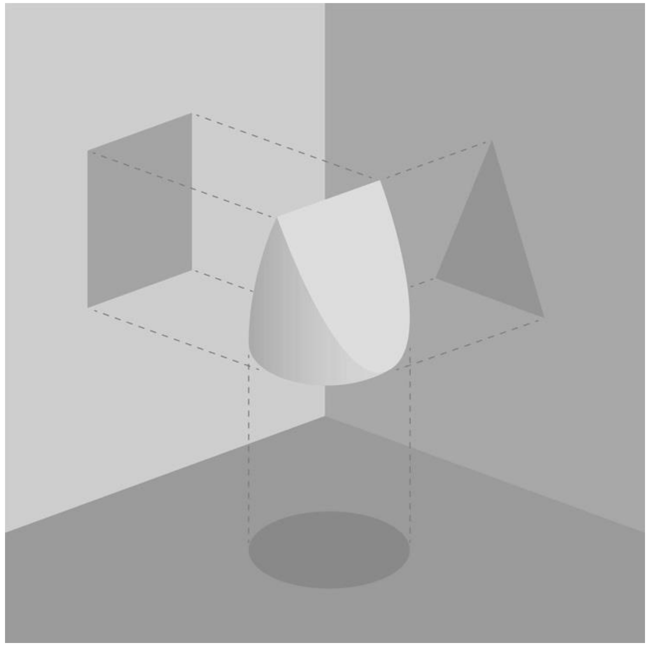
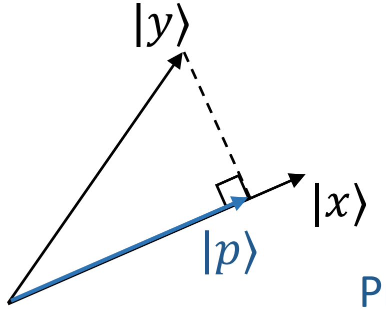


Image credit: Peter Hermes Furian / Alamy Stock

Projecting $|y\rangle$ onto the line direction of $|x\rangle$.



Projected state: $|p\rangle = ?$

Projection is a matrix:

$$|p\rangle = \Pi_x|y\rangle, \Pi_x = \frac{|x\rangle\langle x|}{\langle x|x\rangle}$$

Outer product: a matrix

Inner product: a scalar

Properties:

1. Π is symmetric. (Hermitian: $\Pi^\dagger = \Pi$)
2. Project twice is the same as once. ($\Pi^2 = \Pi$)

Hermitian Matrix in QM

Symmetric matrix (real):

$$S^T = S$$

Hermitian matrix (complex):

$$H^\dagger = H$$

- Hermitian matrix has **real eigenvalues.**
- Corresponding to *physical observable* with real-valued quantity.

Why?

Eigenvalue equation for a linear operator A:

$$A|v_j\rangle = \lambda_j|v_j\rangle$$

where $|v_j\rangle$ is the (non-zero) **eigenvector**,
and λ_j is a complex number known as the **eigenvalue**.

Derive on board (Pauli Matrices):

"Pauli Z operator" $\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

- Eigenvalues: $\lambda_0 = 1$ and $\lambda_1 = -1$
- Eigenvectors: $|v_0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|v_1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Standard basis! $\{|0\rangle, |1\rangle\}$

"Pauli Y operator" $\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

- Eigenvalues: $\lambda_0 = 1$ and $\lambda_1 = -1$
- Eigenvectors: $|v_0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}$ and $|v_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}$

$\{|+i\rangle, |-i\rangle\}$ basis!

"Pauli X operator" $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

- Eigenvalues: $\lambda_0 = 1$ and $\lambda_1 = -1$
- Eigenvectors: $|v_0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $|v_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$

$\{|+\rangle, |-\rangle\}$ basis!

Spectral Theorem

For a linear operator that is normal ($A^\dagger A = AA^\dagger$), we can write it in the **spectral decomposition**:

$$A = \sum_j \lambda_j |v_j\rangle\langle v_j|$$

where λ_j are the eigenvalues, and $|v_j\rangle$ are the corresponding (orthonormal) eigenvectors.

Examples:

$$\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = (+1)|0\rangle\langle 0| + (-1)|1\rangle\langle 1| \qquad \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = (+1)|+\rangle\langle +| + (-1)|-\rangle\langle -|$$

Applications:

- Power of a matrix:

$$A^8 = \left(\sum_j \lambda_j |v_j\rangle\langle v_j|\right)^8 = \sum_j \lambda_j^8 |v_j\rangle\langle v_j|$$

- Exponential of a matrix:

$$e^A \equiv \sum_{k=0}^{\infty} \frac{1}{k!} A^k = \sum_j e^{\lambda_j} |v_j\rangle\langle v_j|$$

Example:

$$e^{i\theta\sigma_z} = e^{i\theta}|0\rangle\langle 0| + e^{-i\theta}|1\rangle\langle 1| = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix}$$