From classical to quantum

Jaikumar Radhakrishnan

ICTS-TIFR, Bengaluru

Workshop, FSTTCS 2025
BITS Pilani, KK Birla Goa Campus
14 Dec 2025

Syllabus

- Mathematical preliminaries
  - Complex Euclidean spaces
  - Relevant matrix operations (decompositions, Kronecker product, etc.)
  - Positive semidefinite matrices and their properties
  - ~~Basics of linear and semidefinite programming~~
- Basics of quantum information
  - Representations of quantum states (pure and mixed)
  - Superposition and Entanglement
  - Quantum operations (unitaries, POVMs, general measurements, partial trace, etc.)
  - Quantum state discrimination

Plan for this talk

- Classical probability in quantum notation: states, events, evolution
- Quantum registers and their states
- Gates and the evolution of quantum states
- Quantum measurements
- Telling classical and quantum states apart

Classical probability in quantum notation: *states*

- The state of a random bit is a probability distribution over $\{0,1\}$, given by a probabilty vector $|\pi\rangle\!\rangle = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}$.
- We write $|0\rangle\!\rangle$ for $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle\!\rangle$ for $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. So $|\pi\rangle\!\rangle = p_0 |0\rangle\!\rangle + p_1 |1\rangle\!\rangle$.
- When describing the probabilistic state of n registers, we have a probability vector with 2^n components:

$$|\pi\rangle\!\rangle = \begin{bmatrix} p_{0\ldots00} \\ p_{0\ldots01} \\ \vdots \\ p_{1\ldots11} \end{bmatrix} = \sum_{x\in\{0,1\}^n} p_x |x\rangle\!\rangle.$$

Classical probability in quantum notation: *evolution*

- In each step of a randomized computer with n registers, a new state is obtained from the old state.
- The change in state is described by a $2^n \times 2^n$ stochastic matrix: the columns add up to 1.

The Toffoli gate acts on three bits:

$$|x, y, z\rangle\!\rangle \mapsto |x, y, z \oplus xy\rangle\!\rangle.$$

- The Toffoli gate corresponds to the 8×8 permuation matrix

$$\begin{bmatrix} \mathrm{I}_{2\times 2} & & & \\ & \mathrm{I}_{2\times 2} & & \\ & & \mathrm{I}_{2\times 2} & \\ & & & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{bmatrix}.$$

- The dollar gate corresponds to the matrix $\begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$.

Classical probability in quantum notation: *events*

- Events are subsets of basis states. They are represented by the their characteristic vector.
- The probability of the event $\langle\!\langle \mathcal{E}|$ when the registers are in state $|\pi\rangle\!\rangle$ is $\langle\!\langle \mathcal{E}|\pi\rangle\!\rangle$.
- The matrix $(p_{i|j} : i, j \in [N])$ can be written as $\sum_{i,j} p_{i|j} |i\rangle\!\rangle\langle\!\langle j|$, that is

$$|j\rangle\!\rangle \mapsto \sum_i p_{i|j} |i\rangle\!\rangle.$$

- For example, $\langle\!\langle \mathrm{EQ}| = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$ corresponds to to the observation that the two registers have identical values.
- Similarly, the event $\langle\!\langle \mathrm{OR}| = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}$ corresponds to the observation that at least one of the registers contains a 1.
- What is the probability of the event $\langle\!\langle \mathrm{EQ}|$ when the state is $|\pi\rangle\!\rangle = \begin{bmatrix} 0.4 \\ 0.1 \\ 0.2 \\ 0.3 \end{bmatrix}$?

Classical probability in quantum notation: *events*

- Events are subsets of basis states. They are represented by the their characteristic vector.
- The probability of the event $\langle\!\langle\mathcal{E}|$ when the registers are in state $|\pi\rangle\!\rangle$ is $\langle\!\langle\mathcal{E}|\pi\rangle\!\rangle$.
- The matrix $(p_{i|j} : i,j \in [N])$ can be written as $\sum_{i,j} p_{i|j} |i\rangle\!\rangle\langle\!\langle j|$, that is

$$|j\rangle\!\rangle \mapsto \sum_i p_{i|j} |i\rangle\!\rangle.$$

- For example, $\langle\!\langle \mathrm{EQ}| = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$ corresponds to to the observation that the two registers have identical values.
- Similarly, the event $\langle\!\langle \mathrm{OR}| = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}$ corresponds to the observation that at least one of the registers contains a 1.
- What is the probability of the event $\langle\!\langle \mathrm{EQ}|$ when the state is $|\pi\rangle\!\rangle = \begin{bmatrix} 0.4 \\ 0.1 \\ 0.2 \\ 0.3 \end{bmatrix}$?

Classical probability in quantum notation: *events*

- Events are subsets of basis states. They are represented by the their characteristic vector.
- The probability of the event $\langle\!\langle\mathcal{E}|$ when the registers are in state $|\pi\rangle\!\rangle$ is $\langle\!\langle\mathcal{E}|\pi\rangle\!\rangle$.
- The matrix $(p_{i|j} : i, j \in [N])$ can be written as $\sum_{i,j} p_{i|j} |i\rangle\!\rangle\langle\!\langle j|$, that is

$$|j\rangle\!\rangle \mapsto \sum_i p_{i|j} |i\rangle\!\rangle.$$

- For example, $\langle\!\langle \mathrm{EQ}| = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$ corresponds to to the observation that the two registers have identical values.
- Similarly, the event $\langle\!\langle \mathrm{OR}| = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}$ corresponds to the observation that at least one of the registers contains a 1.
- What is the probability of the event $\langle\!\langle \mathrm{EQ}|$ when the state is $|\pi\rangle\!\rangle = \begin{bmatrix} 0.4 \\ 0.1 \\ 0.2 \\ 0.3 \end{bmatrix}$?

Classical probability in quantum notation: *events*

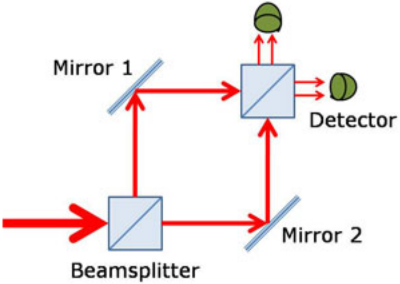
- Events are subsets of basis states. They are represented by the their characteristic vector.
- The probability of the event $\langle\!\langle \mathcal{E}|$ when the registers are in state $|\pi\rangle\!\rangle$ is $\langle\!\langle \mathcal{E}|\pi\rangle\!\rangle$.
- The matrix $(p_{i|j} : i, j \in [N])$ can be written as $\sum_{i,j} p_{i|j} |i\rangle\!\rangle\langle\!\langle j|$, that is

$$|j\rangle\!\rangle \mapsto \sum_i p_{i|j} |i\rangle\!\rangle.$$

- For example, $\langle\!\langle \mathrm{EQ}| = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$ corresponds to to the observation that the two registers have identical values.
- Similarly, the event $\langle\!\langle \mathrm{OR}| = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}$ corresponds to the observation that at least one of the registers contains a 1.
- What is the probability of the event

$$\langle\!\langle \mathrm{EQ}| \text{ when the state is } |\pi\rangle\!\rangle = \begin{bmatrix} 0.4 \\ 0.1 \\ 0.2 \\ 0.3 \end{bmatrix}?$$

Quantum probability



Internet: C. Orzel/Union College

The Mach-Zender apparatus

- When the top beam is blocked, either detector may receive the photon.
- When the bottom beam is blocked, either detector may receive the photon.
- When both beams are allowed, only one detector receives the photon.

Classical versus quantum probability

- The state of a random bit

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix}; \quad p_0 + p_1 = 1.$$

- When n bits are involved, the state is a probability vector with 2^n components.
- Operations correspond to stochastic matrix.

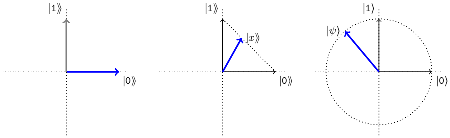
- The state of a qubit

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \quad |\alpha|^2 + |\beta|^2 = 1.$$

$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ Negative numbers are allowed!

- When n qubits are involved, the state is a unit vector with 2^n amplitudes.
- Operations correspond to unitary matrices.

Where do the states live?



- Deterministic register

$$|0\rangle\rangle,\ |1\rangle\rangle$$

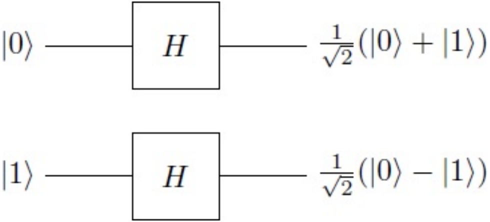
- Randomized register

$$p|0\rangle\rangle + q|1\rangle\rangle; \quad p + q = 1.$$

- Quantum register

$$\alpha|0\rangle + \beta|1\rangle; \quad |\alpha|^2 + |\beta|^2 = 1$$

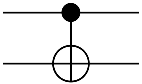
Quantum circuits: The Hadamard gate



Internet: Daniel Ciocîrlan

- We allow 2×2 and 4×4 unitary operations that act on two registers at a time.
- An important operation is the Hadamard operation *H*.
- It is like a coin toss, but it remembers its input; *H* is its own inverse. Much can be done with it.

Quantum circuits: The CNOT gate



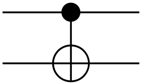
https://commons.wikimedia.org/wiki/File:CNOT_gate.svg

- $|x, y\rangle \mapsto |x, x \oplus y\rangle$
- $\begin{bmatrix} I_{2\times 2} & \\ & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{bmatrix}$
- The first register remains the same; the second register flips if the first contains a 1.

- What happens if the input is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$?
- What happens if the input is $\frac{1}{\sqrt{2}}|0\rangle\,(|0\rangle + |1\rangle)$?
- What happens if the input is $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$?

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}}|0\rangle\,(|0\rangle + |1\rangle)$
- $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$

Quantum circuits: The CNOT gate



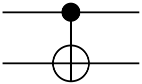
https://commons.wikimedia.org/wiki/File:CNOT_gate.svg

- $|x, y\rangle \mapsto |x, x \oplus y\rangle$
- $\begin{bmatrix} I_{2\times 2} & & \\ & 0 & 1 \\ & 1 & 0 \end{bmatrix}$
- The first register remains the same; the second register flips if the first contains a 1.

- What happens if the input is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$?
- What happens if the input is $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$?
- What happens if the input is $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$?

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$
- $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$

Quantum circuits: The CNOT gate



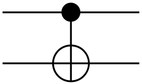
https://commons.wikimedia.org/wiki/File:CNOT_gate.svg

- $|x, y\rangle \mapsto |x, x \oplus y\rangle$
- $\begin{bmatrix} I_{2\times 2} & & \\ & 0 & 1 \\ & 1 & 0 \end{bmatrix}$
- The first register remains the same; the second register flips if the first contains a 1.

- What happens if the input is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$?
- What happens if the input is $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$?
- What happens if the input is $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$?

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$
- $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$

Quantum circuits: The CNOT gate



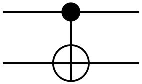
https://commons.wikimedia.org/wiki/File:CNOT_gate.svg

- $|x, y\rangle \mapsto |x, x \oplus y\rangle$
- $\begin{bmatrix} I_{2\times 2} & \\ & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{bmatrix}$
- The first register remains the same; the second register flips if the first contains a 1.

- What happens if the input is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$?
- What happens if the input is $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$?
- What happens if the input is $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$?

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$
- $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$

Quantum circuits: The CNOT gate



https://commons.wikimedia.org/wiki/File:CNOT_gate.svg

- $|x, y\rangle \mapsto |x, x \oplus y\rangle$
- $\begin{bmatrix} I_{2\times 2} & \\ & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{bmatrix}$
- The first register remains the same; the second register flips if the first contains a 1.

- What happens if the input is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$?
- What happens if the input is $\frac{1}{\sqrt{2}}|0\rangle\,(|0\rangle + |1\rangle)$?
- What happens if the input is $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$?

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}}|0\rangle\,(|0\rangle + |1\rangle)$
- $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$

Quantum probability: *measurements*

- When the registers are measured, the state collapses to one of the basis states.
- If the registers were originally in the state $|\psi\rangle = \sum_x \alpha_x |x\rangle$, then the probability that the state $|x\rangle$ results is $|\alpha_x|^2$.
- If a register is measured, then the state of that register collapses to either $|0\rangle$ or $|1\rangle$; the state of the remaining registers also collapses consistently.
- Suppose two registers are in state $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.
- If the first register is measured, then the probability of observing 0 is $p_0 = |\alpha_{00}|^2 + |\alpha_{01}|^2$. If zero is observed, the state of the second register becomes $\frac{1}{\sqrt{p_0}}(\alpha_{01}|01\rangle + \alpha_{10}|10\rangle)$.

Mixed states

An ensemble of states

- Suppose we prepare a state in a register A by performing a classical probabilistic experiment:

$$\begin{pmatrix} p_1 & p_2 & p_3 & \cdots & p_t \\ |\psi_1\rangle & |\psi_2\rangle & |\psi_3\rangle & \cdots & |\psi_t\rangle \end{pmatrix}.$$

- What is the state of the register A?
- Can different ensembles lead to the same state?

The state of a subsystem

- Suppose two registers A and B are in a joint state

$$|\psi\rangle_{AB} = \sum_{i=1}^{t} \alpha_i |a_i\rangle_A |b_i\rangle_B .$$

- Does it then makes sense to talk about the state of the register A?
- Is the state of register A an ensemble?
- What if we measure B? Does the basis of measurement matter?

The density matrix

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & t \\ |\psi_1\rangle & |\psi_2\rangle & |\psi_3\rangle & \cdots & |\psi_t\rangle \end{pmatrix}.$$

- Question: Suppose we perform an orthogonal measurement in a basis $\{|m_j\rangle : j = 1, 2, \ldots, d\}$ What is the probability of the j-th outcome?
- Answer:

$$\sum_{i=1}^{d} p_i \langle m_j | |\psi_i\rangle \langle psi_i | |m_j\rangle = \langle m_j | \left(\sum_{i=1}^{d} p_i |\psi_i\rangle \langle \psi_j | \right) |m_i\rangle = \langle m_j | \rho | m_j\rangle .$$

  The same ρ irrespective of j.
- All the information about the ensemble has been *compiled* in ρ; it is the density matrix of the state of the ensemble.

The density matrix

- The density matrix is positive semidefinite.
- It can be written as
$$\rho = \sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle\phi_i|,$$
where $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$.
- The density matrix is positive semidefinite, and has trace 1.
- Suppose the density matrix ρ_{AB} describes the joint state of a pair of registers (A, B); to obtain the state ρ_A of the register A, we perform a partial trace
$$\rho_A = \mathrm{Tr}_B \rho_{AB}.$$

State discrimination

- Suppose there are two registers X and Y; X is quantum, but Y is classical (random) bit.
- Alice first prepares Y such that $\Pr[Y = 0] = \lambda$ and $\Pr[Y = 1] = 1 - \lambda$. Then, she prepares X in state ρ_0 if $Y = 0$ and in state ρ_1 if $Y = 1$.
- Alice sends X to Bob, and asks him to guess Y.
- What is the best strategy for Bob?

The optimal strategy

- Consider the classical analog with P_0 and P_1 instead of ρ_0 and ρ_1. In the optimal strategy,

$$\Pr[error] = \frac{1}{2} + \frac{1}{2}\|\lambda P_0 - (1-\lambda)P_1\|_1.$$

- The quantum bound is similar (Holevo-Helstrom theorem). In the best quantum strategy,

$$\Pr[error] = \frac{1}{2} + \frac{1}{2}\|\lambda \rho_0 - (1-\lambda)\rho_1\|_1 = \frac{1}{2} + \|\lambda \rho_0 - (1-\lambda)\rho_1\|_{\mathrm{Tr}}.$$

Thank you.