VERIFICATION OF QUANTUM CIRCUITS

Lecture 1: Introduction to Quantum states and transformations

Reference: Chapter 3 of the text book:

"Quantum computing for Computer Scientists"

– by Yanofsky & Mannucci

Some preliminary notions that we will be using:

– please refer to Chapters 1 & 2 of the textbook

- Complex numbers
- Complex vector space, $\mathbb{C}^n$
- Matrices over complex numbers
- Adjoint operation
- Hermitian matrix
- Unitary matrix

Plan for the lecture:

– 1. An example of a classical deterministic system

– 2. A probabilistic system

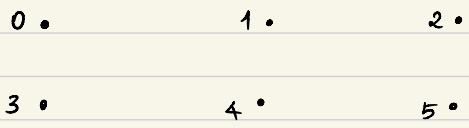
– 3. Quantum systems – differences from probabilistic systems

↳ some examples

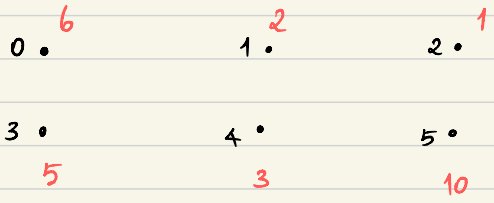
Part 1: classical deterministic systems

Here is an example of a classical system and its state-transformation dynamics.

Consider a graph with six vertices:



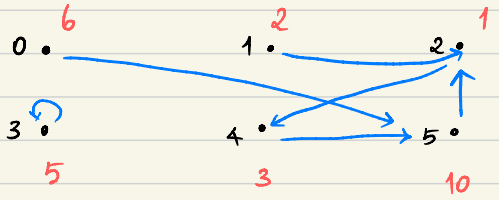
27 marbles are divided and placed on the vertices in the following way:



State: $[6, 2, 1, 5, 3, 10]^T$

↳ state can be succinctly represented as a column vector.

How do the marbles change position? Here are the edges of the graph, with the condition that every vertex has exactly one outgoing edge.



$M[i,j] = 1$ if $j \longrightarrow i$

Adjacency matrix M:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	0	0	0	0	0
2	0	1	0	0	0	1
3	0	0	0	1	0	0
4	0	0	1	0	0	0
5	1	0	0	0	1	0

Transitions: $M \cdot X$

X → current state at 't'

$M \cdot X$ → state at $t+1$

So if $X = [6, 2, 1, 5, 3, 10]^T$ is state at 't',

state at $t+1$ will be

$$M \cdot X = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 6 \\ 2 \\ 1 \\ 5 \\ 3 \\ 10 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 12 \\ 5 \\ 1 \\ 9 \end{bmatrix}$$

→ State after 'k' steps would be $M^k X$

Bottomline: - states represented as column vectors

- dynamics corresponds to matrices
  - ↳ one step transformation obtained by multiplying state with a matrix
    - ↳ Multi step dynamics by repeated matrix multiplication.

Part 2: Probabilistic systems

→ Assume a graph as before.

→ There is a single marble.

↳ there is a probability associated to each vertex

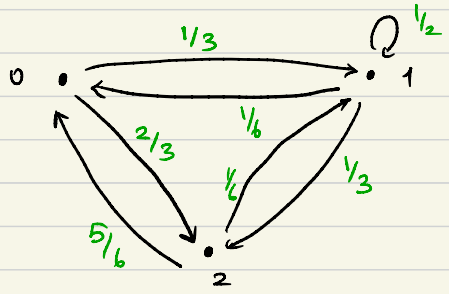
for example, if we have a 3-vertex graph, a state could be:

$$\begin{bmatrix} \frac{1}{5}, & \frac{2}{5}, & \frac{1}{5} \end{bmatrix}^T$$

sum should be 1.

State: vectors whose values sum up to 1. Give a probability for the marble to be at each node.

– Transitions are now probabilistic.



At each vertex: - sum of outgoing edges is 1.

- sum of incoming edges is 1.

→ marble must go and come from someplace.

Adjacency matrix: $M = \begin{bmatrix} 0 & 1/6 & 5/6 \\ 1/3 & 1/2 & 1/6 \\ 2/3 & 1/3 & 0 \end{bmatrix}$ → doubly stochastic matrix

sum of columns = sum of rows = 1

Evolution of a system in k steps: $M^k \cdot X$ ⤷ give probability that the marble is present in each state.

→ Transpose M^T : corresponds to graph with edge reversed.

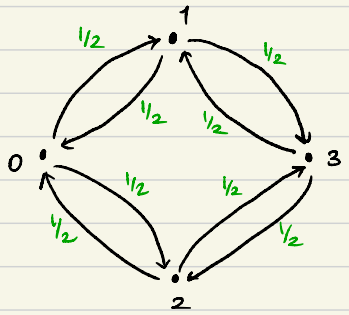
Suppose W is a row vector with sum of entries $= 1$.

$$M^T W^T = (W M)^T$$

multiplying a state to the left of M takes W from t to $t-1$.

Example: Stochastic billiard ball

Consider the graph:



Starting state: $[1, 0, 0, 0]^T$ initially marble at 0.

Transition matrix = $M = \begin{bmatrix} 0 & 1/2 & 1/2 & 0 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{bmatrix}$

After 1 click, state would be $[0, 1/2, 1/2, 0]^T$

After 2 clicks, —— $[1/2, 0, 0, 1/2]^T$

Then, this repeats. The marble bounces back and forth between (1,2) and (0,3)

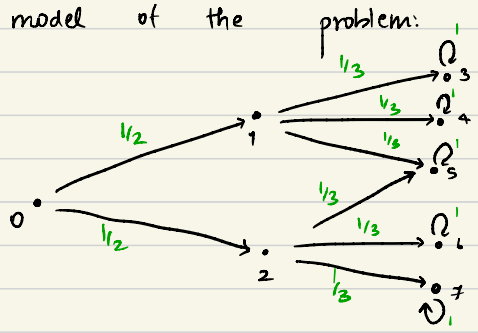
Example: Probabilistic double-slit experiment



Bullet being shot. 50% chance the bullet travels through top slit, 50% chance it goes through bottom slit

→ once a bullet is through a slit, there are 3 targets to the right of each slit that the bullet can hit with equal probability.

Graph model of the problem:



Matrix $B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1/3 & 1/3 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1/3 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1/3 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Computing B^2, we will see that $B^2[5,0] = 1/6 + 1/6 = 1/3$

→ there are two ways for the bullet to reach position 5, hence they get added up.

Bottom line: - states are vectors whose values sum to 1
- transitions are given by stochastic matrices.

Part 3: Quantum Systems

States:

Now, a state would be a vector of complex numbers:

$$X = \begin{bmatrix} x_1, & x_2, & \dots, & x_n \end{bmatrix}^T$$

s.t. the sum of the moduli is 1.

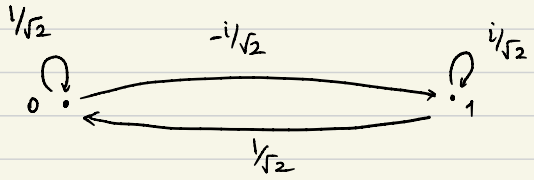
i.e., $\sum_{i=1}^{n} x_i^2$

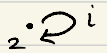
For example: $\begin{bmatrix} \frac{1}{\sqrt{3}}, & \frac{2i}{\sqrt{15}}, & \sqrt{\frac{2}{5}} \end{bmatrix}^T$

→ An interpretation: the square of the modulus represents some probability.

→ Using this representation allows to cancel out numbers leading to smaller probabilities on adding (we will see an example later)

Transition dynamics: Transitions will be specified using graphs having complex number weights.





Matrix $U = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ -i/\sqrt{2} & i/\sqrt{2} & 0 \\ 0 & 0 & i \end{bmatrix}$ → a unitary matrix

i.e., $U^\dagger \cdot U = U \cdot U^\dagger = I$ ($U^\dagger$: adjoint)

Matrices will have special properties:

Consider the matrix representing the modulus of the square of each cell. We denote it as $|U[i,j]|^2$

$$|U[i,j]|^2 = \begin{vmatrix} 1/2 & 1/2 & 0 \\ 1/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

↳ will be a doubly stochastic matrix.

Fact: For any unitary matrix, the modulus squared of each of its entries forms a doubly stochastic matrix.

→ Suppose X is a state, U is a unitary matrix:

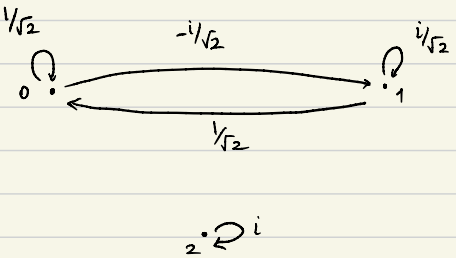
$$UX = Y$$

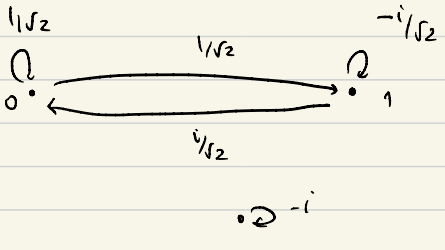
↳ will also preserve property that sum of modulus squared is 1.

Graph interpretation of unitary matrices:

For $U = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ -i/\sqrt{2} & i/\sqrt{2} & 0 \\ 0 & 0 & i \end{bmatrix}$

$U^\dagger = \begin{bmatrix} 1/\sqrt{2} & +i/\sqrt{2} & 0 \\ 1/\sqrt{2} & -i/\sqrt{2} & 0 \\ 0 & 0 & -i \end{bmatrix}$





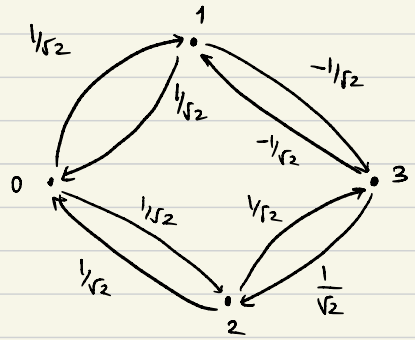
U takes from t to $t+1$

$U^\dagger$ takes from t to $t-1$

reversing a computation.

Notice that $U^\dagger \cdot U = U \cdot U^\dagger = I_3$ (identity).

Example: Quantum billiard ball



Matrix $A = \begin{bmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ 1/\sqrt{2} & 0 & 0 & -1/\sqrt{2} \\ 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \\ 0 & -1/\sqrt{2} & 1/\sqrt{2} & 0 \end{bmatrix}$ → unitary matrix.

Initial state: $[1, 0, 0, 0]^T$ → single marble on vertex 0.

→ After one click system will be in $[0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0]^T$

50% in 1, 50% in 2

→ After two clicks, state comes to $[1, 0, 0, 0]^T$ again

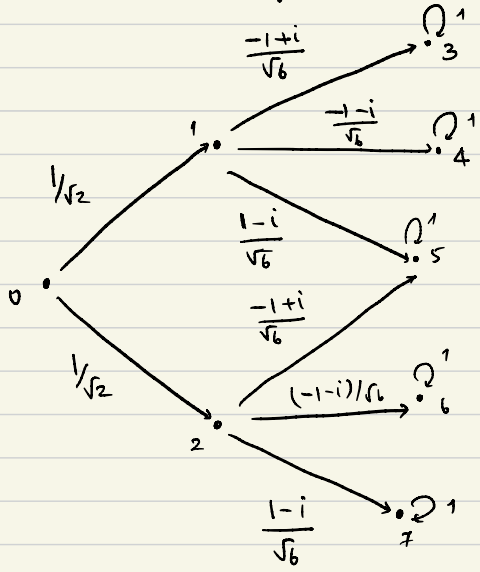
$$\begin{bmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ 1/\sqrt{2} & 0 & 0 & -1/\sqrt{2} \\ 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \\ 0 & -1/\sqrt{2} & 1/\sqrt{2} & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1/2 + 1/2 = 0 \end{bmatrix}$$

cancel out

models a physical phenomenon called interference

Example: Double-slit experiment with photons

Here is a graph model:



→ There is a 50-50 chance of photon passing through each slit

↳ this explains the $\frac{1}{\sqrt{2}}$ out of 0 since $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$

- Similarly $\left|\frac{\pm 1 \pm i}{\sqrt{6}}\right|^2 = \frac{2}{6} = \frac{1}{3}$

there is a $\frac{1}{3}$ probability to hit any of the three measuring devices.

→ However notice the prob. of going to 5:

it will be $|c|^2$ where

$$c = \frac{1}{\sqrt{2}} \cdot \left(\frac{1-i}{\sqrt{6}}\right) + \frac{1}{\sqrt{2}} \left(\frac{-1+i}{\sqrt{6}}\right) = 0$$

→ the numbers cancel out leading to smaller probability of hitting 5.

↳ models the notion of interference.

↓

This is quite a deviation from "probabilistic systems" that we saw in Part 2.

Note: refer to the book for an explanation of the physics behind.

→ Same experiment can be carried out with a single photon.
Similar "canceling out" of probabilities happens.

→ Refer to book for an interpretation of the state

→ Photon is not in a single position, it is simultaneously in all positions in some sense

↳ hence it is in a superposition.

Briefly:

A system is in a state $X = [c_0, c_1, \dots c_{n-1}]^T$ means that after measuring it it will be found in position i with probability $|c_i|^2$.

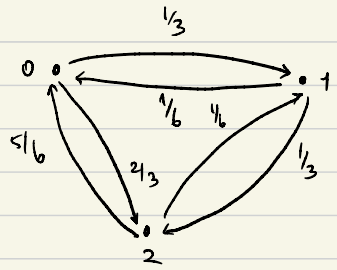
Bottom line:

- Quantum states are represented by column vectors of complex numbers whose sum of moduli squared is 1.
- Dynamics represented by unitary matrices and is therefore reversible.

Part 4: Combining systems

Suppose there is a red marble whose dynamics is given by:

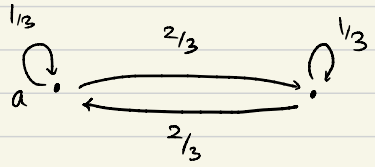
G_M:



$$M = \begin{bmatrix} 0 & 1/6 & 5/6 \\ 1/3 & 1/2 & 1/6 \\ 2/3 & 1/3 & 0 \end{bmatrix}$$

and there is a blue marble whose dynamics is given as:

G_N:



$$N: \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix}$$

A state of the "two-marble" system can be seen as:

$$X = \begin{matrix} 0a \\ 0b \\ 1a \\ 1b \\ 2a \\ 2b \end{matrix} \begin{bmatrix} 1/18 \\ 0 \\ 2/18 \\ 1/3 \\ 0 \\ 1/2 \end{bmatrix}$$

→ prob. that red marble is in '1' & blue marble is in 'a'

→ dynamics of the combined system is given by the tensor product of M, N.

$$M \otimes N = \begin{bmatrix} 0 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} & 1/6 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} & 5/6 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} \\ 1/3 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} & 1/2 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} & 1/6 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} \\ 2/3 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} & 1/3 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} & 0 \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix} \end{bmatrix}$$

$$M \otimes N = \begin{array}{c} \\ 0a \\ 0b \\ 1a \\ 1b \\ 2a \\ 2b \end{array} \begin{array}{c} \begin{array}{cccccc} 0a & 0b & 1a & 1b & 2a & 2b \end{array} \\ \begin{bmatrix} 0 & 0 & 1/18 & 2/18 & 5/18 & 10/18 \\ 0 & 0 & 2/18 & 1/18 & 10/18 & 5/18 \\ 1/9 & 2/9 & 1/6 & 2/6 & 1/18 & 2/18 \\ 2/9 & 1/9 & 2/6 & 1/6 & 2/18 & 1/18 \\ 2/9 & 4/9 & 1/9 & 2/9 & 0 & 0 \\ 4/9 & 2/9 & 2/9 & 1/9 & 0 & 0 \end{bmatrix} \end{array}$$

The graph corresponds to a Cartesian product of G_M & G_N.

Entangled States:

- Sometimes a combined state (a vector) can be written as tensor product of two vectors.
- If we cannot write it as a tensor product, we call it an entangled state.

for example: $\begin{bmatrix} 8 \\ 12 \\ 6 \\ 12 \\ 18 \\ 9 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \otimes \begin{bmatrix} 4 \\ 6 \\ 3 \end{bmatrix}$

↳ not entangled (called separable)

$\begin{bmatrix} 8 \\ 0 \\ 0 \\ 0 \\ 0 \\ 18 \end{bmatrix}$ cannot be written as a tensor product of a vector from $\mathbb{C}^2$ and $\mathbb{C}^3$.

↳ an entangled state.

Summary of the lecture:

- → Quantum states, dynamics
- → Tensor product, entangled states
- → Ideas of interference, superposition, measurement.