Discrete Probability :

→ Distributions over n bits :

$$x \in \{0,1\}^n \qquad (p_x)_{x \in \{0,1\}^n}$$

$$\mathcal{D} \equiv \text{vector } v \in (\mathbb{R}^+)^{2^n}$$

$$\|v\|_1 = 1$$

eg. $n = 3$ $\qquad \mathcal{D}$: $p_{000} : 1/2$

$p_{101} : 1/6$

$p_{110} : 1/3$

$$\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \begin{bmatrix} 1/2 \\ \\ \\ \\ \\ 1/6 \\ 1/3 \\ \\ \end{bmatrix} \equiv |\mathcal{D}\rangle \in (\mathbb{R}^+)^8$$

↑ represents the 'state' of the system.

→ Two independent distributions

$\mathcal{D}_1$: distribution over n_1 bits ←

$\mathcal{D}_2$: " " n_2 bits ←

We have $n_1 + n_2$ bits, where first n_1 are sampled from $\underline{\mathcal{D}_1}$, remaining sampled **independently** from $\underline{\mathcal{D}_2}$.

eg. $n_1 = 2$ $\quad \mathcal{D}_1$: P^1_{00} : $1/2$ $\quad \mathcal{D}_2$: P^2_0 : $2/3$

$n_2 = 1$ $\quad P^1_{10}$: $1/6$ $\quad P^2_1$: $1/3$

P^1_{11} : $1/3$

$$\begin{bmatrix} 2/3 \\ 1/3 \end{bmatrix}$$

$$\begin{bmatrix} 1/2 \\ 0 \\ 1/6 \\ 1/3 \end{bmatrix}$$

$$|\mathcal{D}\rangle = \begin{bmatrix} 1/3 \\ 1/6 \\ 0 \\ 0 \\ 1/9 \\ 1/18 \\ 2/9 \\ 1/9 \end{bmatrix} \begin{array}{l} -000 \\ -001 \\ \\ \\ \\ \\ \\ \\ \end{array}$$

State of combined system is given by TENSOR PRODUCT of $|\psi_1\rangle$ and $|\psi_2\rangle$

$$\underset{(\mathbb{R}^+)^{2^{n_1+n_2}}}{|\psi\rangle} = \underset{(\mathbb{R}^+)^{2^{n_1}}}{|\psi_1\rangle} \otimes \underset{(\mathbb{R}^+)^{2^{n_2}}}{|\psi_2\rangle}$$

Tensor Product : $\underset{n_{11} \times n_{12}}{M_1}$, $\underset{n_{21} \times n_{22}}{M_2}$

$$\underbrace{M_1 \otimes M_2}_{n_{11} n_{21} \times n_{12} n_{22}} = \begin{bmatrix} M_1[0,0]\, M_2 & M_1[0,1]\, M_2 & \cdots \\ M_1[1,0] \cdot M_2 & M_1[1,1]\, M_2 & \cdots \\ & & \ddots \end{bmatrix}$$

$A \otimes (B + C) = A \otimes B + A \otimes C$ $\qquad A \otimes B \neq B \otimes A.$

$A \otimes (B \otimes C) = (A \otimes B) \otimes C$

Q1 : $\|v_1\|_p = z_1$ $\qquad \|v_2\|_p = z_2$

$$\|v_1 \otimes v_2\|_p = ?$$

NOTE : There exist states that cannot be decomposed as tensor product of two smaller states.

$$\begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix} \neq |v_1\rangle \otimes |v_2\rangle$$

→ Mixture of two distributions

$\mathcal{D}_1$, $\mathcal{D}_2$: distⁿ over n bits.

$$\mathcal{D} \equiv \begin{cases} \mathcal{D}_1 & \text{w.p. } p_1 \\ \mathcal{D}_2 & \text{w.p. } p_2 \end{cases} \qquad \begin{matrix} p_1 \geq 0 \\ p_2 \geq 0 \end{matrix} \qquad p_1 + p_2 = 1.$$

$$|\mathcal{D}\rangle = p_1 |\mathcal{D}_1\rangle + p_2 |\mathcal{D}_2\rangle$$

→ Operations over n- bit system :

maps n bits to m bits

$n = 2$

$$D = \begin{bmatrix} 1/2 \\ 0 \\ 1/4 \\ 1/4 \end{bmatrix}$$

AND :

$00 \longrightarrow 0$

$01 \longrightarrow 0$

$10 \longrightarrow 0$

$11 \longrightarrow 1$

$$M_{AND} = \begin{array}{cccc} \left[\begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}\right] \\ \begin{matrix} \uparrow & \uparrow & \uparrow & \uparrow \\ 00 & 01 & 10 & 11 \end{matrix} \end{array}$$

$$M_{AND} \cdot |D\rangle$$

If we have a distⁿ D over 2 bits, then the distⁿ after applying AND is

$$|D'\rangle = M_{AND} \cdot |D\rangle$$

$(\mathbb{R}^+)^2$ $\qquad$ $(\mathbb{R}^+)^4$

Randomized operations

eg 1: Operation that produces n uniformly random bits

$$M = \frac{1}{2^n}\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ \vdots & \vdots \\ 1 & 1 \end{bmatrix}$$

eg 2: AND w/p $1/3$ OR w/p $2/3$

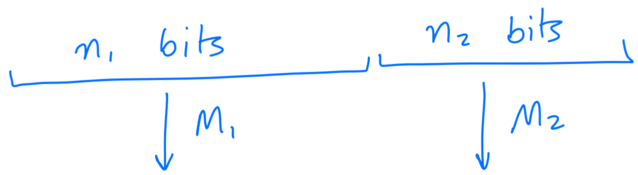
$$M_{AND} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad M_{OR} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

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

Thm: Any randomized process mapping n_1 bits to n_2 bits can be described by a STOCHASTIC MATRIX $M \in (\mathbb{R}^+)^{2^{n_2} \times 2^{n_1}}$

non neg. entries
every col. sums up to 1

→ Independent operations



Suppose state of the system before op. is $|\alpha_1\rangle \otimes |\alpha_2\rangle$

Then state after op. is

$$(M_1 |\alpha_1\rangle) \otimes (M_2 |\alpha_2\rangle)$$

$$= (\underline{M_1 \otimes M_2})(|\alpha_1\rangle \otimes |\alpha_2\rangle)$$

Tensor Product Rule:

$$(M_1 \otimes M_2) \cdot (A_1 \otimes A_2) = (M_1 A_1 \otimes M_2 A_2)$$

Q2: Prove that $\nexists$ stochastic matrix $M \in \mathbb{R}^{2^{2n} \times 2^{2n}}$ s.t. $\forall\ |\mathcal{D}\rangle \in \mathbb{R}^{2^n}$,

$$M \cdot \left(|\mathcal{D}\rangle \right) = |\mathcal{D}\rangle \otimes |\mathcal{D}\rangle$$

$$\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} \otimes \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} \neq \begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}$$

→ **Measurement**

Extracting information from a dist.^{n}

$|\mathcal{D}\rangle \xrightarrow[\nearrow]{\text{measure}}$ string x w.p. $\mathcal{D}_x$.

state is destroyed, and we "observe" x as the outcome.

We can also make partial measurements

eg. $\begin{bmatrix} 1/2 \\ 0 \\ 1/3 \\ 1/6 \end{bmatrix} \xrightarrow[\text{1st bit}]{\text{measure}}$

0 w.p. $1/2$
residual state $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

1 w.p. $1/2$
residual state $\begin{bmatrix} 2/3 \\ 1/3 \end{bmatrix}$

→ Summary of classical discrete prob.

- n bit system described using non-neg. vector of dim.^{n} 2^n, ℓ_1 norm 1.
- Independent systems → tensor product of state vectors
- Operations → stochastic matrices
- (Partial) Measurement : means to extract classical bits / info from state vector.

CRAZY DISCRETE PROB.

Imagine a world governed by the following rules of probability:

→ state of n bit system:

$$|v\rangle \in \mathbb{R}^{2^n}, \quad \| \, |v\rangle \|_1 = 1.$$

$$\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}, \quad \begin{bmatrix} 1/3 \\ -2/3 \end{bmatrix}$$

→ valid operations:

stochastic matrix, followed by rescaling of resulting vector (to make ℓ_1 norm $= 1$)

parity operation $\quad M = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

$$|v\rangle = \begin{bmatrix} 2/3 \\ 0 \\ 0 \\ -1/3 \end{bmatrix} \qquad M|v\rangle = \begin{bmatrix} 1/3 \\ 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

→ Measurement of $|v\rangle$ produces x with prob. $|v_x|$.

$$
|v\rangle \;
\begin{cases}
|v_{0\cdots 0}| \\
|v_{0\cdots 01}| \\
\;\vdots \\
|v_{1\cdots 1}|
\end{cases}
$$

$|\cdots|$

$$|v\rangle \xrightarrow{\text{measure}} \;\; \xrightarrow{\text{parity}} \;\; \xrightarrow{\text{measure}}$$

$$|v\rangle \xrightarrow{\text{parity}} \;\; \xrightarrow{\text{measure}}$$

$$
\begin{bmatrix} 1/4 \\ 1/4 \\ -1/4 \\ 1/4 \end{bmatrix}
\xrightarrow{\text{measure}}
\begin{bmatrix} 1/4 \\ 1/4 \\ 1/4 \\ 1/4 \end{bmatrix}
\xrightarrow{\text{parity}}
\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}
\xrightarrow{\text{measure}}
\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}
$$

$\times$

$$
\begin{bmatrix} 1/4 \\ 1/4 \\ -1/4 \\ 1/4 \end{bmatrix}
\xrightarrow{\text{parity}}
\begin{bmatrix} 1 \\ 0 \end{bmatrix}
\xrightarrow{\text{measure}}
\begin{bmatrix} 1 \\ 0 \end{bmatrix}
$$

Prob. dist

→ $|v\rangle \in (\mathbb{R}^+)^{2^n}$

$\|v\|_1 = 1$

→ All operations are stochastic matrices

→ measurement

"No interference"

Quantum

→ $|v\rangle \in \mathbb{C}^{2^n}$

$\|v\|_2 = 1$

→ unitary matrices

→ measurement

"Interference"

- AXIOMS OF QUANTUM COMPUTING

A1 $\rightarrow$ Quantum state over n qubits described by vector $v \in \mathbb{C}^{2^n}$

$$\|v\|_2 = 1$$

$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} -1 \\ 0 \end{bmatrix}$, $|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$, $|-\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$

A2 $\rightarrow$ $\underline{|v_1\rangle}$: state over n_1 qubits

$\underline{|v_2\rangle}$: state over n_2 qubits

combined state : $\underline{|v_1\rangle \otimes |v_2\rangle}$

A3 $\longrightarrow$ Quantum operations :

only two kinds of operations available:

1. Unitary operation :

multiply a unitary matrix

$$\begin{tikzcd} |v\rangle \arrow[r, "U"] & |v'\rangle \arrow[l, bend left, "U^{\dagger}"] \end{tikzcd}$$

UNITARY MATRIX :

U is unitary if $U \cdot U^{\dagger} = I$

conj. transpose

- unitary matrices are invertible
- unitary matrices preserve l_2 norm.
- unitary matrices preserve inner product

$$\langle |v\rangle, |w\rangle \rangle = \langle U|v\rangle, U|w\rangle \rangle$$

$$\langle v|w\rangle \qquad \langle v| \underbrace{U^{\dagger} U}_{I} |w\rangle$$

$$= \langle v|w\rangle$$

2. Measurement

$$|v\rangle \xrightarrow{\text{measure}} x \quad \text{w.p. } |v_x|^2$$

$$\begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \xrightarrow{\text{measure}} \begin{matrix} 0 \text{ w.p. } 1/2 \\ 1 \text{ w.p. } 1/2 \end{matrix}$$

$$|-\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} \xrightarrow{\text{measure}} \begin{matrix} 0 \text{ w.p. } 1/2 \\ 1 \text{ w.p. } 1/2. \end{matrix}$$

Partial measurement :

similar to classical measurement, however we get a 'mixture' of quantum states.

changed $1/\sqrt{2}$ to $1/2$

eg. $$\begin{bmatrix} 1/2 \\ -1/2 \\ 1/\sqrt{3} \\ 1/\sqrt{6} \end{bmatrix} = \frac{1}{2}|0\rangle|0\rangle - \frac{1}{2}|0\rangle|1\rangle + \frac{1}{\sqrt{3}}|1\rangle|0\rangle + \frac{1}{\sqrt{6}}|1\rangle|1\rangle$$

measure first qubit

0 w.p. $1/2$

res. state $$\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$$

1 w.p. $1/2$

res. state $$\frac{\frac{1}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle}{\left\| \frac{1}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle \right\|_2}$$

$$\begin{bmatrix} 1/2 \\ -1/2 \\ 1/\sqrt{3} \\ 1/\sqrt{6} \end{bmatrix} = 1/2\, |0\rangle|0\rangle - \frac{1}{2}|0\rangle|1\rangle + \frac{1}{\sqrt{3}}|1\rangle|0\rangle + \frac{1}{\sqrt{6}}|1\rangle|1\rangle$$

$$\Big\downarrow \text{ measure second qubit}$$

0 w.p. $\frac{1}{4} + \frac{1}{3}$ 1 w.p. $\frac{1}{4} + \frac{1}{6}$

$$\frac{1/2\,|0\rangle + \frac{1}{\sqrt{3}}|1\rangle}{\sqrt{1/4 + 1/3}} \quad \text{res. state} \quad \frac{-\frac{1}{2}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle}{\sqrt{\frac{1}{4} + \frac{1}{6}}}$$

$$|\psi\rangle = \alpha_0 |0\rangle \otimes |\psi_0\rangle + \alpha_1 |1\rangle \otimes |\psi_1\rangle \xrightarrow[\text{1st qubit}]{\text{measure}}$$

0 w.p. $|\alpha_0|^2$

$|\psi_0\rangle$

1 w.p. $|\alpha_1|^2$

$|\psi_1\rangle$

Suppose a quantum state is

$|\psi_i\rangle$ w.p. p_i , $\sum p_i = 1$

This is not the same as

$\sum p_i |\psi_i\rangle$.

mixture of quantum states

$$\{(p_i, |\psi_i\rangle)\}$$

$\sum p_i = 1$

each $|\psi_i\rangle$ is a quantum state.

- Unitary operation on pure state produces pure state.

- Measurement / partial measurement may produce mixed state.

Qn: You are given either

$$|\psi_0\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \quad \text{or} \quad |\psi_1\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}.$$

How do you distinguish?

You are allowed to perform any unitary op. or measurement.

Qn: Show that $\nexists$ unitary U s.t.

$\forall\ |\psi\rangle \in \mathbb{C}^2$,

$$U\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

'Encrypting' a quantum state using classical bits:

Let $|\psi\rangle$ be a quantum state in $\mathbb{C}^2$.
We will discuss how to 'encrypt' any quantum state using a classical key.

formally,

$\text{Enc}(\underline{\text{key } k}, \underline{|\psi\rangle}) \longrightarrow \underline{|ct\rangle}$

$\text{Dec}(\underline{\text{key } k}, \underline{|ct\rangle}) \longrightarrow \underline{|\psi\rangle}$

In fact, our key k will be just 2 bits!

$\text{Enc}((a,b), |\psi\rangle)$:

→ $a = b = 0$, output $|\psi\rangle$

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$

→ $a = 1$, $b = 0$, output $X|\psi\rangle$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

→ $a = 0$, $b = 1$, output $Z|\psi\rangle$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$Z|0\rangle = |0\rangle$

$Z|1\rangle = -|1\rangle$

→ $a = 1$ $b = 1$ output $XZ|\psi\rangle$

Dec. is just inverse operation.

Chall. Adv.

$\xleftarrow{|\psi_0\rangle,\ |\psi_1\rangle}$

(a, b)

$\beta \leftarrow \{0,1\}$

$\xrightarrow{\mathcal{E}nc((a,b),\ |\psi_\beta\rangle) = |\psi'\rangle}$

$U|\psi'\rangle$

measures

$$\Pr_{a,b,\beta}[\text{outcome} = 0]$$

Qn: Pick any ψ_0, ψ_1, U, compute

$\Pr[\text{outcome} = 0]$.

QUANTUM CIRCUITS :

Some popular quantum gates –

For each of these, check that they're unitary

1. X gate : $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $X^2 = I$

$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$|0\rangle \rightarrow |1\rangle$

$|1\rangle \rightarrow |0\rangle$

2. Z gate : $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$Z^2 = I$

$|0\rangle \rightarrow |0\rangle$

$|1\rangle \rightarrow -|1\rangle$

It suffices to define gate's behaviour on some basis

Note that $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is not the only basis

For eg. consider the following basis

$\begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}, \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$

$|+\rangle$ $|-\rangle$

Check : $Z|+\rangle = |-\rangle$

$Z|-\rangle = |+\rangle$

3. Hadamard Gate H

$$|0\rangle \rightarrow |+\rangle$$

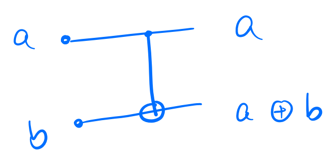
$$|1\rangle \rightarrow |-\rangle$$

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

$$|+\rangle \rightarrow |0\rangle$$

$$|-\rangle \rightarrow |1\rangle$$

4. Controlled NOT gate :



$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$