TODAY

Announcement: HW1 due this Friday, midnight

OUTLINE:
* Mixed states, continued
* Quantum key distribution (QKD).

MIXED STATE

Probability distribution over pure states $\{(p_i, |\psi_i\rangle)\}_{i \in [k]}$

What happens when we measure a mixed state in computational basis.

Measuring a pure state $|\psi\rangle$.
(in any orthonormal basis)

Measure $|\psi\rangle = \sum_{i \in [N]} \alpha_i |i\rangle$ in basis $\{|1\rangle \ldots |N\rangle\}$
"computational basis"

$\Pr["i"] = |\alpha_i|^2$

Measure $|\psi\rangle$ in ⟶ basis $\{|v_1\rangle, |v_2\rangle \ldots |v_N\rangle\}$
(any orthonormal basis).

$\Pr["v_i"] = |\langle v_i | \psi \rangle|^2$

Measure mixed state $\{p_j, |\psi_j\rangle\}$ in orthonormal basis

$\{|1\rangle, |2\rangle \ldots |N\rangle\}$.

$$\Pr[\text{"}i\text{"}] = \sum_j p_j |\langle v_i | \psi_j \rangle|^2$$

$$= \sum_j p_j \langle v_i | \psi_j \rangle (\langle v_i | \psi_j \rangle)^\dagger$$

$$= \sum_j p_j \langle v_i | \psi_j \rangle \langle \psi_j | v_i \rangle$$

$$= \sum_j p_j \langle v_i | \psi_j \times \psi_j | v_i \rangle$$

$$= \langle v_i | \left(\sum_j p_j |\psi_j \times \psi_j| \right) | v_i \rangle .$$

$\left(\sum_j p_j |\psi_j \times \psi_j| \right)$ ↑ Density matrix ρ

ANY measurement outcome is ONLY a function of ρ.

Density matrix of $S = \{(p_j, |\psi_j\rangle)\}_{j \in [k]}$

$$= \sum_j p_j |\psi_j \times \psi_j|$$

Measure S in computational basis.

$$Pr[\text{"1"}] = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} \rho_{11} & \rho_{12} & & \\ \rho_{21} & & \ddots & \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \rho_{11}$$

$$Pr[\text{"2"}] = \rho_{22} \qquad \cdots \qquad Pr[\text{"i"}] = \rho_{ii}$$

$$\begin{aligned} Tr[\rho] &= \rho_{11} + \rho_{22} + \rho_{33} \cdots \rho_{NN} \\ &= Pr[\text{"1"}] + Pr[\text{"2"}] + \cdots + Pr[\text{"N"}]. \\ &= 1. \end{aligned}$$

PROPERTY 1 : $Tr[\rho] = 1$

$$\rho = \sum_i p_i |\psi_i \times \psi_i|$$

$$= \sum_i p_i \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \begin{bmatrix} \alpha_0^* & \cdots & \alpha_{N-1}^* \end{bmatrix}$$

$$= \sum_i p_i \begin{bmatrix} \alpha_0\alpha_0^* & M_{12} \\ M_{21} & \alpha_1\alpha_0^* \end{bmatrix}$$

$$\rho = \rho^\dagger \quad \text{(Hermitian Matrix)}.$$

PROPERTY 2: ρ is Hermitian

Positive Semi-Definite

$\forall\, v \in \mathbb{C}^N, \quad \langle v|\rho|v\rangle \geq 0$

Let's assume that v is unit vector. (w.l.o.g.)

orthonormal basis : $B = \{v, v_2, v_3 \ldots\ldots v_N\}$.

$\langle v|\rho|v\rangle$ = Pr["v"] when measuring in basis B.

PROPERTY 3 : POSITIVE SEMI-DEFINITE

UNITARY OPERATIONS ON MIXED STATES.

$S_1 = \{(p_i, |\psi_i\rangle)\} \qquad U(S_1) \rightarrow S_2.$

$$\rho_{S_1} = \sum_i p_i \, |\psi_i\rangle\langle\psi_i|$$

$$\rho_{S_2} = \sum_i p_i \, |U(\psi_i)\rangle \left(|U(\psi_i)\rangle\right)^\dagger \qquad = \langle\psi_i|U^\dagger$$

$$= \sum_i p_i \, U|\psi_i\rangle\langle\psi_i|U^\dagger$$

$$= U\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right)U^\dagger$$

$$= U \rho_{S_1} U^\dagger$$

Hermitian Matrices satisfy : for every Hermitian M,

There is an orthonormal basis $|v_1\rangle \dots |v_N\rangle$ of $\mathbb{C}^N$ and real ~~eigenvalues~~ "scaling factors".

$\lambda_1, \dots \lambda_N$ such that

M's action is to scale by λ_i in direction $|v_i\rangle$.

i.e. $$M = \sum_{j=1}^{N} \lambda_j |v_j\rangle\langle v_j|$$

and "scaling" $|v_j\rangle$ by λ_j

$$\langle v_j | M | v_j \rangle = \lambda_j$$

A density matrix ρ is Hermitian, $\mathrm{Tr}(\rho) = 1$, $\rho \geq 0$ (p.s.d.)

$\rho \geq 0 \Rightarrow \langle v_i | \rho | v_i \rangle \geq 0 \Rightarrow \lambda_i \geq 0 \quad (\forall i)$

(linear algebra fact).

For any orthonormal $|v_1\rangle \ldots |v_N\rangle$, there is a unitary $U_{v_1 \ldots v_N}$ s.t. $\forall\, i$ $U|v_i\rangle \to |i\rangle$, $U^\dagger |i\rangle \to |v_i\rangle$.

Given density matrix ρ with associated $\lambda_1 \ldots \lambda_N$ and basis $|v_1\rangle \ldots |v_N\rangle$.

Apply $U_{v_1 \ldots v_N}$ to ρ, resulting in $\rho' = U \rho U^\dagger$

① [ρ' has the same λ_i's as ρ.]

② [ρ' has basis $|1\rangle \ldots |N\rangle$]

ρ' action is to scale each $|i\rangle$ by λ_i

$$\langle v | \rho' | v \rangle$$

$$= \langle v | U \rho U^\dagger | v \rangle .$$

Simplify so that $|v\rangle = |i\rangle$.

$$\underbrace{\langle i | U \rho U^\dagger | i \rangle}_{\langle v_i | \rho = |v_i\rangle} = \lambda_i$$

$$\rho' = \sum \lambda_i \, |i\rangle\langle i|$$

$$= \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ 0 & & \ddots & \\ & & & \lambda_N \end{bmatrix}$$

$Tr[\rho'] = 1$ because ρ' is a density matrix.

$\Rightarrow \lambda_1 + \lambda_2 \ldots + \lambda_N = 1.$

In conclusion, Hermitian matrix ρ that is a density matrix has each $\lambda_i \geq 0$, $\sum_i \lambda_i = 1$.

So, any Density Matrix ρ with distinct* eigenvalues $\lambda_1 \ldots \lambda_N$ has a canonical mixed state associated with it $\{\lambda_i, |v_i\rangle\}_{i \in [N]}$

MAXIMALLY MIXED STATE

This is a mixed state for which all of its eigenvalues (scaling factors $\lambda_1 \ldots \lambda_N$ are identical

$$\sum_i \lambda_i = 1 \qquad \rho = \begin{bmatrix} \frac{1}{N} & & 0 \\ & \frac{1}{N} & \\ 0 & & \ddots & \\ & & & \frac{1}{N} \end{bmatrix} = \sum_i \underbrace{\lambda_i}_{=\frac{1}{N}} |i\rangle\langle i|$$

Game 1.

$$\left\{\frac{1}{2}|0\rangle, \frac{1}{2}|1\rangle\right\}$$

$$\rho = \frac{1}{2}\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$$

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

Maximally mixed state on 1 qubit ($N=2$)

Game 2.

$$\left\{\frac{1}{2}|+\rangle, \frac{1}{2}|-\rangle\right\}$$

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

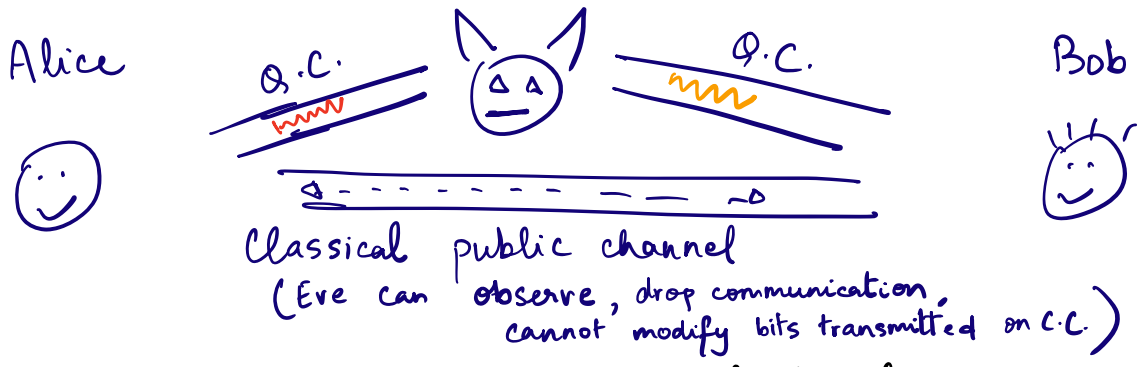
$$= \frac{1}{2}\begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\\frac{1}{2} & \frac{1}{2}\end{bmatrix} + \frac{1}{2}\begin{bmatrix}\frac{1}{2} & -\frac{1}{2}\\-\frac{1}{2} & \frac{1}{2}\end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix}\frac{1}{2}+\frac{1}{2} & \cancel{\frac{1}{2}-\frac{1}{2}}\\\cancel{\frac{1}{2}-\frac{1}{2}} & \frac{1}{2}+\frac{1}{2}\end{bmatrix}$$

$$= \begin{bmatrix}\frac{1}{2} & 0\\0 & \frac{1}{2}\end{bmatrix}.$$

Wiesner, Bennett - Brassard 84

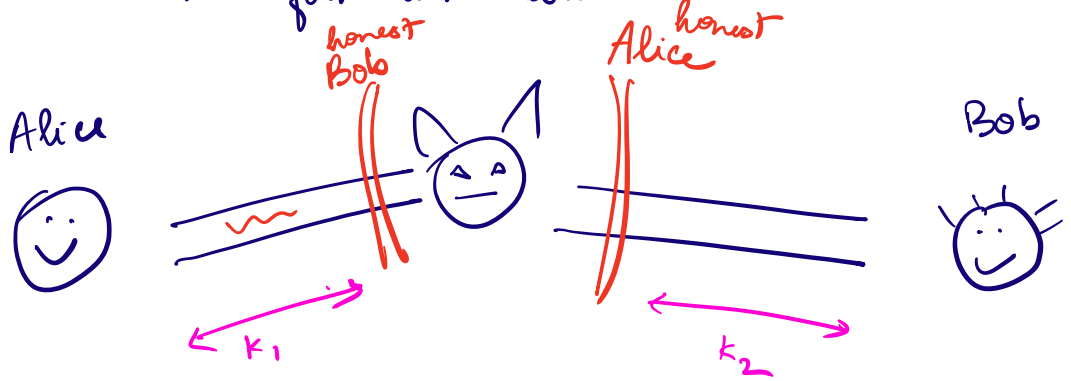
Quantum Key Distribution (QKD)



Classical public channel
(Eve can observe, drop communication, cannot modify bits transmitted on C.C.)

Authenticated classical channel.

Goal: Alice, Bob agree on key k that Eve has no information about



"k" does not have information about k. "k"

$\{|0\rangle |1\rangle |+\rangle |-\rangle\}$ Q.C. N states