CS6846 – Quantum Algorithms and Cryptography

Quantum Cryptography

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Road Ahead:

- QKD.
- Q one time Pads.
- Q SKE
- Q PKE.
- Try: Q FHE / q Money

Mixed States.

Let's say a device outputs

$|\psi_1\rangle$ w.p. p_1

$|\psi_2\rangle$ w.p. p_2

$\vdots$

$|\psi_n\rangle$ w.p. p_n

Can represent such a state by $\{p_i, |\psi_i\rangle\}$

Let us say that we measure the above device in basis $|v_1\rangle, \ldots, |v_d\rangle$.

$$\Pr\left(|v_i\rangle \text{ is observed}\right) = \sum_j p_j \left|\langle v_i | \psi_j\rangle\right|^2$$

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

$$= \langle v_i | \underbrace{\left(\sum_j p_j |\psi_j\rangle\langle\psi_j| \right)}_{\rho} |v_i\rangle$$

$$= \langle v_i | \rho | v_i\rangle$$

Definition: The mixed state $\{p_i, |\psi_i\rangle\}$ is represented by matrix $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$.

Example :

$$S_1 = |0\rangle \quad \text{w.p } 1$$
$$= |1\rangle \quad \text{w.p } 0$$

$$\rho = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$S_2 = -|0\rangle \quad \text{w.p. } 1$$
$$= |1\rangle \quad \text{w.p } 0$$

$$\rho = (-|0\rangle)(-\langle 0|) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$S_3 = |0\rangle \quad \text{w.p. } \tfrac{1}{2}$$
$$= |1\rangle \quad \text{w.p. } \tfrac{1}{2}$$

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

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

Evolution: suppose a mixed state S_1 $\{p_i, |\psi_i\rangle\}$ goes through unitary U, transforms to $S_2 = \{p_i, U|\psi_i\rangle\}$.

Let ρ_{S_b} be matrix corres. to S_b
$b \in \{1, 2\}$

$$\rho_{S_2} = ?\ \rho_{S_1}\ ? = U \rho_{S_1} U^\dagger$$

Proposition: If ρ represents a mixed state then $tr(\rho) = 1$, ρ is positive semidefinite & Hermitian.

PSD: $\forall\ x \in \mathbb{C}^N$, $\langle x|\rho|x\rangle \geq 0$.

Hermitian: $\rho = \rho^{\dagger}$

Proof: Let's consider $|\psi\rangle = \sum_{i=1}^{d} a_i |i\rangle$

$$tr\left(|\psi\rangle\langle\psi|\right) = \sum |a_i|^2 = 1.$$

Now consider mixed state:

$$tr\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) = \sum_i p_i \underbrace{tr\left(|\psi_i\rangle\langle\psi_i|\right)}_{1}$$

$$= \sum p_i = 1.$$

Hermitian: Exercise

PSD: Note for any $|v\rangle$,

$$\langle v|\rho|v\rangle = \Pr(\text{observe } |v\rangle) \geq 0.$$

$\Rightarrow \rho$ is PSD.

Definition: We say that a matrix ρ is a density matrix iff $tr(\rho) = 1$, ρ is PSD & Hermitian.

Proposition: If ρ is a density matrix, it corresponds to a mixed state

$$\rho = \sum_{i=1}^{d} \lambda_i \, |v_i\rangle\langle v_i|$$ by spectral theorem.

λ_i: real eigenvalues.

$|v_i\rangle$: Form orthonormal basis

$$tr(\rho) = 1, \quad \sum \lambda_i = 1$$

Want $\{ \underline{\underline{p_i}}, |\psi_i\rangle \} = \{ \underline{\underline{\lambda_i}}, |v_i\rangle \}$ for $i \in [d]$

Maximally mixed state:

All eigenvalues λ_i are identical

for $i \in [N]$, $\lambda_i = \frac{1}{N}$.

Quantum Algos & Density Matrix:

In the HSP for group G, if "f" hides subgroup H, then our algorithm outputs a uniformly random coset

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

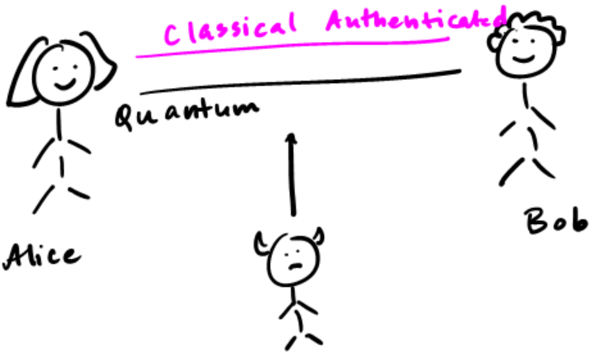
Each coset $|gH\rangle$ is output w.p. $\frac{1}{|G|}$.

So the density matrix representing the mixed state is $\rho_H = \sum_{g \in G} \frac{1}{|G|} |gH\rangle\langle gH|$

Quantum Key Distribution

Bennett & Brassard 1984.

Information Theoretic Security.



Protocol:

Main Property: If bit b is encoded in an unknown basis, Eve cannot get info abt b w/o disturbing the state.

1). Alice chooses n random bits $a_1 \dots a_n$,
& n random bases, $b_1 \dots b_n$

$b_i \in \{$ Comp, Had $\}$

$\{|0\rangle, |1\rangle\}$ $b=0$
$\{|+\rangle, |-\rangle\}$ $b=1$

Sends a_i in basis b_i.

$a_i = 0$, $b_i = 1$ $\Rightarrow |+\rangle$

2). Bob chooses random bases $b_1' \dots b_n'$
& measures received qubits in these.
Gets $a_1' \dots a_n'$.

3) Bob sends $\{b_i'\}$ to Alice, Alice sends $\{b_i\}$ to Bob.

For "matching" positions $a_i' = a_i$

IF Eve did not tamper.

4) Alice selects $n/4$ locations in shared string & sends Bob a_i & locations.

If fraction of errors is "high", they abort.

5) If not, they get $n/4$ shared bits.