25.01.23

Ch1.

1.1 Mixed state. (probabilistic state).

ex. $\frac{1}{\sqrt{2}}\left(|00\rangle_{A,B} + |11\rangle_{AB}\right) \Rightarrow$ Alice has mixed state.

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|+\rangle$ are different if you measure them in $(|+\rangle, |-\rangle)$.

- A mixed quantum state is a clean way of describing the state.

$$\rho \begin{cases} |e_1\rangle & \text{w.p } p_1 . \\ \vdots & \\ |e_t\rangle & \text{w.p. } p_t . \end{cases}$$

- We will write this

$$\rho = \sum_i p_i |e_i\rangle\langle e_i|$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}.$$

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

$$|+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \qquad |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}.$$

Definition : A mixed state on qubits is a matrix $\rho = \sum_i p_i |e_i\rangle\langle e_i|$ where each $|e_i\rangle$ is a n-qubit pure state, each $p_i \geq 0$ and $\sum_i p_i = 1$.

- Properties of quantum states
  - ρ is Hermision $\rho = \rho^* = \rho^{-T}$
  - $Tr(\rho) = 1$
  - Because ρ is Hermition, it is diagonalizable with real - valued eigenvalues.

This means we can write $\rho = \sum_i \lambda_i |f_i\rangle\langle f_i|$ with $\{|f_i\rangle\}$ orthonormal basis and $\lambda_i \geq 0$.

$$\rho_1 = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix} \Rightarrow \begin{cases} |0\rangle \text{ w.p } 3/4 \\ |1\rangle \text{ w.p } 1/4. \end{cases}$$

$$\Rightarrow \begin{cases} 1/2 \text{ to get } |+\rangle \\ 1/2 \text{ to get } |-\rangle \end{cases}$$

$$\rho_2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -| = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix} \Rightarrow \begin{cases} |0\rangle \text{ w.p. } 1/2 \\ |+\rangle \text{ wp } 1/4 \\ |-\rangle \text{ wp } 1/4. \end{cases}$$

$$\Rightarrow \begin{cases} 1/2 \text{ to get } |+\rangle \\ 1/2 \text{ to get } |-\rangle \end{cases}$$

1.2 Applying quantum operations on mixed state.

If we start from $|e_i\rangle$ and apply U, we obtain $|f_i\rangle = U|e_i\rangle$.

$$|f_i\rangle\langle f_i| = U|e_i\rangle\langle e_i|U^\dagger = U(|e_i\rangle\langle e_i|)U^\dagger.$$

$$\rho = \sum_i p_i |e_i\rangle\langle e_i|.$$

$$\rho \xrightarrow{U} \sum_i p_i |f_i\rangle\langle f_i| = \sum_i p_i U|e_i\rangle\langle e_i|U^\dagger$$

$$= U\left(\sum_i p_i |e_i\rangle\langle e_i|\right)U^\dagger = U\rho U^\dagger.$$

Projective measurements

$B = \{|b_1\rangle, \ldots, |b_n\rangle\}$.

we start from

$$Pr[\text{output } k \mid |e_i\rangle] = |\langle e_1|b_1\rangle|^2.$$

$$\rho \xrightarrow[\text{basis } B]{\text{measurement}} \text{output "}k\text{" w.p } \sum_i p_i |\langle e_i|b_k\rangle|^2$$

$$= \sum_i p_i \langle b_k|e_i\rangle\langle e_i|k\rangle$$

$$= \langle b_k|\left(\sum_i p_i |e_i\rangle\langle e_i|\right)|b_k\rangle$$

$$= \langle b_k|\rho|b_k\rangle.$$

ex.

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |1+\rangle\right)_{AB} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

$$= \sqrt{\frac{3}{4}}\overbrace{\left(\sqrt{\frac{3}{2}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle\right)}^{|\phi\rangle}|0\rangle + \frac{1}{2}|11\rangle$$

$$\rho_A = \frac{3}{4}|\phi\rangle\langle\phi| + \frac{1}{4}|1\rangle\langle 1| = \begin{pmatrix} 1/2 & \sqrt{2}/4 \\ \sqrt{2}/4 & 1/2 \end{pmatrix}.$$

Definition: For a (possibly mixed) state

ρ_{AB} we define.

$$\mathrm{Tr}_B(\rho_{AB}) = \sum_j (I_A \otimes \langle j|)\,\rho_{AB}\,(I_A \otimes |j\rangle).$$

Special cases.

$|\psi\rangle = \sum_i \alpha_i |e_i\rangle|f_i\rangle$ where $\{|e_i\rangle\}$ forms an orthonormal basis.

$$\rho_B = \mathrm{Tr}_A(|\psi\rangle\langle\psi|) = \sum_i |\alpha_i|^2 |f_i\rangle\langle f_i|$$

but, $\rho_A \neq \sum_i |\alpha_i|^2 |e_i\rangle\langle e_i|.$

$|\psi\rangle_{AB} = \sum_i \alpha_i |e_i\rangle\langle f_i|$ where the $\{|f_i\rangle\}$ form a orthonormal basis.

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \sum_i |\alpha_i|^2 |e_i\rangle\langle e_i|.$$

1.3 Generalized measurements

Definition : A POVM is an measurement of matricies $\{M_i\}$, s.t. $\sum_i M_i M_i^\dagger = I$

Measuring a state ρ with this POVM gives outcome i w.p. $P_i = \mathrm{tr}(\rho M_i M_i^\dagger)$.

and the resulting state is

$$\boxed{\rho_i = \frac{M_i \rho M_i^\dagger}{\mathrm{tr}(M_i \rho M_i^\dagger)}}$$

Measurement in an orthonormal basis, $\{|b_1\rangle, \dots, |b_n\rangle\}$.

Take $M_i = |b_i\rangle \rightarrow M_i M_i^\dagger = |b_i\rangle\langle b_i|$

- $P_i = \mathrm{tr}(\rho |b_i\rangle\langle b_i|) = \mathrm{tr}(\langle b_i|\rho|b_i\rangle)$

$$= \langle b_i|\rho|b_i\rangle.$$

- Resulting state is $\dfrac{|b_i\rangle \rho \langle b_i|}{tr(|b_i\rangle \rho \langle b_i|)} = |b_i\rangle\langle b_i|$

- Sometimes, the POVM is charactrized by.

$$F_i = M_i M_i^\dagger \qquad \sum_i F_i = Id.$$

$$tr(\rho M_i M_i^\dagger) = tr(\rho F_i).$$

Feb.03.23

Purification

Def: A purification $|\psi_{AB}\rangle$ of a state ρ_B is a quantum pure state that satisfies

$$\mathrm{Tr}_A |\psi\rangle\langle\psi|_{AB} = \rho_B$$

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

$$\rho_B' = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$$

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|+0\rangle + |-0\rangle).$$

there can be several purificate

$\rho_B = \rho_B'$ because they have the same density matrix.

(It becomes clear if you write it on matrix form)

$$\boxed{\frac{1}{2}\sum_i |P_1 - P_0|}$$

$$\rho_B = \sum_{i=1}^{0} p_i |\psi_i\rangle\langle\psi_i|$$

$\{|e_i\rangle\}$ is orthonormal basis.

Schmits Decomposition

Proposition: Let $|\psi_{AB}\rangle$ be a state of $2n$ qubits.
where each register contains n qubits.

- There exists two orthonormal basis $\{|e_1\rangle \to |e_{2^n}\rangle\}$,

$\{|f_1\rangle, \longrightarrow \{|f_1\rangle, —, |f_{2^n}\rangle\}$ s.t.

$$|\psi_{AB}\rangle = \sum^{2^n} \alpha_i |e_i\rangle_A |f_i\rangle_B$$

Propositio

Assume we have two quantum pure states. $|\psi_{AB}\rangle$, $|\psi_{AB}\rangle$

s.t. $Tr_A(|\phi\rangle\langle\phi|_{AB}) = R$ is

Then exist a unitary U_A

Ch. 3 : Distance measures for quantum states.

Definition: For any 2 quantum states ρ, σ, the trace distance between ρ and σ is defined as.

$$D(\rho,\sigma) = \frac{1}{2} \operatorname{Tr} \sqrt{(\rho-\sigma)(\rho-\sigma)^\dagger}$$

$$(\rho-\sigma) = \sum_i \lambda_i |e_i\rangle\langle e_i|$$

$$(\rho-\sigma)(\rho-\sigma)^\dagger = \sum_i \lambda^2 |e_i\rangle\langle e_i|$$

$$\sqrt{(\rho-\sigma)(\rho-\sigma)^\dagger} = \sum_i |\lambda_i| \, |e_i\rangle\langle e_i|$$

$$\Rightarrow \boxed{D(\rho,\sigma) = \frac{1}{2}\sum_i |\lambda_i|.}$$

- $D(\rho,\sigma) = 0 \iff \rho = \sigma$
- $0 \leq D(\rho,\sigma) \leq 1$.
- $D(\rho,\delta) = D(\delta,\rho)$
- $D(\rho,\sigma) + D(\sigma,\tau) \geq D(\rho,\tau)$.
- ρ, σ are pure states. then.

$$\rho = |\psi\rangle\langle\psi| \quad , \quad \sigma = |\phi\rangle\langle\phi| .$$

$$D(\rho,\sigma) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$$

- Property. D is invariant by unitary operation.

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho,\sigma).$$

· ρ, σ are diagonalizable in the same basis

$$\rho = \sum_i p_i |e_i\rangle\langle e_i|$$

$\{|e_i\rangle\}$

$$\sigma = \sum_i q_i |e_i\rangle\langle e_i|.$$

$$D(\rho, \sigma) = \frac{1}{2} \sum_i |p_i - q_i|.$$

Interpretetion

let Alice and Bob. Alice has a random bit b. unknown to Bob. Suppose Alice sends a state ρ_b (that depends on b). What is the probability that Bob guesses b.?! (ρ_0, ρ_1 known description)

$$\max \Pr(\text{Bob guess } b) = \frac{1}{2} + \frac{D(\rho_0, \rho_1)}{2}.$$

If we write $(\rho_0 - \rho_1) = \sum_i \lambda_i |e_i\rangle$

$\{|e_i\rangle\}$ orthonormal basis.

then the maximum is achieved measuring in this basis.

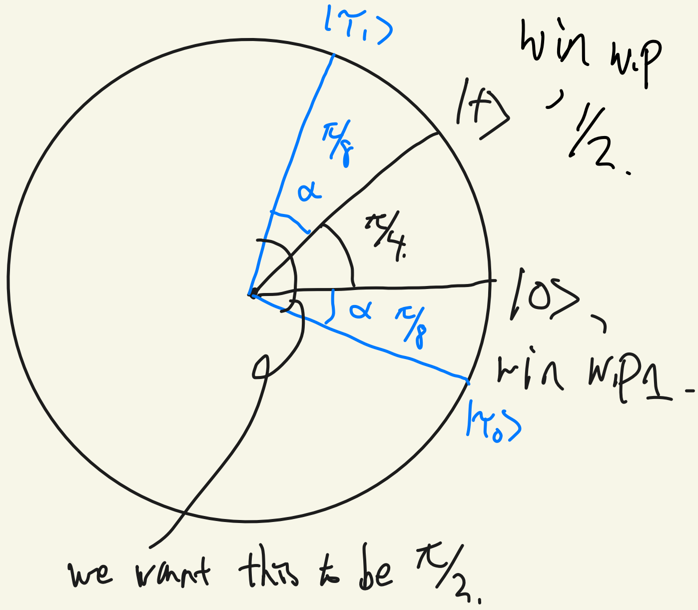
example

$$P_0 = |0\rangle\langle 0| \qquad P_1 = |+\rangle\langle +|.$$

· Measure in the computational basis.

Outcome '0' $\to 0$

Outcome '1' $\to 1$.



$$P = 3/4$$

$$|\langle 0|\tau_0\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right) \simeq 0.85$$

$$|\langle +|\tau_1\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right) \simeq 0.85$$

$$\cos(2x) = 2\cos^2(x) - 1$$

$$2\cos^2(\pi/8) = \cos(\pi/4) + 1$$

$$= \frac{1}{\sqrt{2}} + 1$$

$$\to \cos^2(\pi/8) = 1/2 + \frac{1}{2}\cdot\frac{1}{\sqrt{2}} = \frac{1}{2} + \frac{\sqrt{2}}{4}.$$

17. Feb. 23

Proposition:

$$\max\{\Pr(\text{Bob guess } b)\} = \frac{1}{2} + \frac{D(\rho_0, \rho_1)}{2}.$$

$\rho_0 - \rho_1 = \sum_i \lambda_i |e_i\rangle\langle e_i|$: spectral decomposition

$\sum_i \lambda_i = 0$ $\lambda_i \in \mathbb{R}$.

$\{|e_i\rangle\}$ form an ortho. basis

- Bob's strategy: measure in the $\{|e_i\rangle\}$.

Let "$|e_i\rangle$" be the outcome.

- If $\lambda_i \geq 0$ guess $b=0$

If $\lambda_i < 0$ guess $b=1$.

ρ_0 contribute to positive λ value and ρ_1 contribute to negative λ value let :

$p_i = \langle e_i | \rho_0 | e_i \rangle$. $\Pr[\text{Bob output } "|e_i\rangle" \mid \rho_0]$

$q_i = \langle e_i | \rho_1 | e_i \rangle$ $\Pr[$ " $| \rho_1]$

$\langle e_i | \rho_0 - \rho_1 | e_i \rangle = d_i = p_i - q_i$

$$\Pr[\text{Bob guesses correctly} \mid b=0] = \sum_{i,\, d_i \geq 0} p_i$$

$$\Pr[\quad \text{''} \quad \mid b=1] = \sum_{i,\, d_i < 0} q_i$$

$\downarrow$

$$\Pr[\text{Bob guesses correctly}] = \frac{1}{2}\sum_{i,\, d_i \geq 0} p_i + \frac{1}{2}\sum_{i,\, d_i < 0} q_i$$

$$2\Delta(\rho_0, \rho_1) = \sum_i |d_i| = \sum_{i:\, d_i \geq 0} d_i - \sum_{i:\, d_i < 0} d_i$$

$$= \sum_{i,\, d_i \geq 0} (p_i - q_i) - \sum_{i,\, d_i < 0} (p_i - q_i)$$

$$= \sum_{i, d_i \geq 0} p_i - \left(1 - \sum_{i: d_i < 0} q_i\right) - \left(1 - \sum_{i, d_i \geq 0} p_i\right) + \sum_{i, d_i < 0} q_i$$

$$= 2\left(\sum_{i, d_i \geq 0} p_i + \sum_{i, d_i < 0} q_i\right) - 2$$

$$\Pr[\text{Bob guesses correctly}] = \frac{1}{2}\left(\sum_{i, d_i \geq 0} p_i + \sum_{i, d_i < 0} q_i\right)$$

$$\Rightarrow \frac{1}{2} + \frac{D(\rho_0, \rho_1)}{2}.$$

Fidelity of quantum state

If we have $|\psi\rangle$ and $|\phi\rangle$, we define.

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|$$

Closeness of two quantum state

Definition: For any 2 quantum state ρ, σ

we define.

$$\boxed{F(\rho, \sigma) = \mathrm{Tr}\left(\sqrt{\sqrt{\rho}\,\sigma\,\sqrt{\rho}}\right)}$$

you don't use this buddy.

Properties.

- $0 \leq F(\rho, \sigma) \leq 1$.
- $F(\rho, \sigma) = 1 \iff \rho = \sigma$.
- $F(\rho, \sigma) = F(\sigma, \rho)$

if, ρ, σ are pure state.

$\rho = |\psi\rangle\langle\psi| = \sqrt{\rho}$

$\sigma = |\phi\rangle\langle\phi| = \sqrt{\sigma}$

$\sqrt{\sigma}\sqrt{\rho} = |\phi\rangle\langle\phi|\psi\rangle\langle\psi|$

$\sqrt{\rho}\sqrt{\sigma} = |\psi\rangle\langle\psi|\phi\rangle\langle\phi|$

$\sqrt{\rho}\sigma\sqrt{\rho} = |\psi\rangle |\langle\psi|\phi\rangle|^2 \langle\psi|$

$= |\langle\psi|\phi\rangle|^2 |\psi\rangle\langle\psi|$

For pure state.

$$\boxed{F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|}$$

If ρ and σ are <u>diagonalizable in the same basis</u>.

$\rho = \sum_i p_i |e_i\rangle\langle e_i|$

$\sigma = \sum_i q_i |e_i\rangle\langle e_i|$

$\sqrt{\rho}\sigma\sqrt{\rho} = \sum_i p_i q_i |e_i\rangle\langle e_i|$

$$\boxed{F(\rho, \sigma) = \sum_i \sqrt{p_i q_i}}$$

Invariance property

For any unitary U

$$F(U\rho U^{\dagger}, U\sigma U^{\dagger}) = F(\rho, \sigma).$$

---

recall.

For any state ρ_B we say that $|\psi\rangle_{AB}$ is a purification of ρ_B iff $Tr(|\psi\rangle\langle\psi|_{AB}) = \rho_B$.

Uhlmann's theorem

$$\boxed{\text{For any } \rho, \sigma, \ F(\rho,\sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle\psi|\phi\rangle|. \quad \text{where } |\psi\rangle \text{ (resp. } |\phi\rangle) \text{ is a purification of } \rho \text{ (resp. } \sigma).}$$

$$F(\rho,\sigma) = \max_{|\psi\rangle} |\langle\psi|\phi\rangle| ,$$

$|\phi\rangle$ is any purification of σ,

where max over all purification of ρ.

Fuchs Van de Graaf inequality

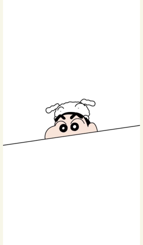
For any states ρ, σ

$$1 - F(\rho,\sigma) \leq \Delta(\rho,\sigma) \leq \sqrt{1 - F^2(\rho,\sigma)}$$

or inequality.

$$1 - \Delta(\rho,\sigma) \leq F(\rho,\sigma) \leq \sqrt{1 - \Delta^2(\rho,\sigma)}$$

Chapter 3



3.1 Bit commitment

- classical way is by using Hash function

- A bit commitment scheme is a protocol between 2 parties. Alice and Bob which consits of 2 phases:

1) Commit Phase :

Alice commits to his $b \in \{$

Bob should not be able to guess the b.

Security requirements.

└ Completeness: If both parties are honest, the protocol always succeeds.

Hiding. If Alice is honest and Bob cheats,

$$\Pr(\text{Bob guesses } b) = p_B^*.$$

Binding: