25.01.23

Ch1.

1.1 Mixed state, (probabilistic state).

Ex $\frac{1}{\sqrt{2}}(|00\rangle_{A,B} + |11\rangle_{AB})$ $\Rightarrow$ 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.

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

- We will write this

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

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

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

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

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

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 $\lambda_i \geq 0$.

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

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

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

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

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

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

measurement basis B

$$\rho \longrightarrow \text{output } "k" \text{ w.p } \sum_i p_i |\langle e_i|b_k\rangle|^2$$

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

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

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

ex.

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

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

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

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

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

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

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

and the resulting state is

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

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

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

- $p_i = tr(\rho |b_i\rangle\langle b_i|) = tr(\langle b_i|\rho|b_i\rangle)$

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

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

- 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

$$Tr_A |\psi\rangle\langle\psi|_{AB} = \rho_B$$

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

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

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

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

Then can be several purificate

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

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

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

$$\frac{1}{2}\sum_i |p_1 - p_0|$$

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

$\{|e_i\rangle\}$ is orthogonal 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 $\{|e_1\rangle \rightarrow |e_{2^n}\rangle\}$, $\{|f\rangle_1 \longrightarrow \{|f_1\rangle_1 \text{ —}, |f_{2^n}\rangle\}$ s.t.

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

Propositio

Assume we hve tw quante pure State. $|\psi_{AB}\rangle$, $|\psi_{43}$ S.t. $Tr_A(|\phi\rangle\langle\phi|_{AB}) = R$ i)

Tlere exis a unitary U_A

Ch. 2 : Distance measures for quantum states.

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

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

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

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

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

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

- $D(\rho,\sigma) = 0 \iff \rho = \sigma$
- $0 \le D(\rho,\sigma) \le 1$.
- $D(\rho,\delta) = D(\delta,\rho)$
- $D(\rho,\sigma) + D(\sigma,\tau) \ge D(\rho,\tau)$

- ρ, σ are pure states. then.

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

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

- 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

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

$\{|e_i\rangle\}$

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

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

Interpretation

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.

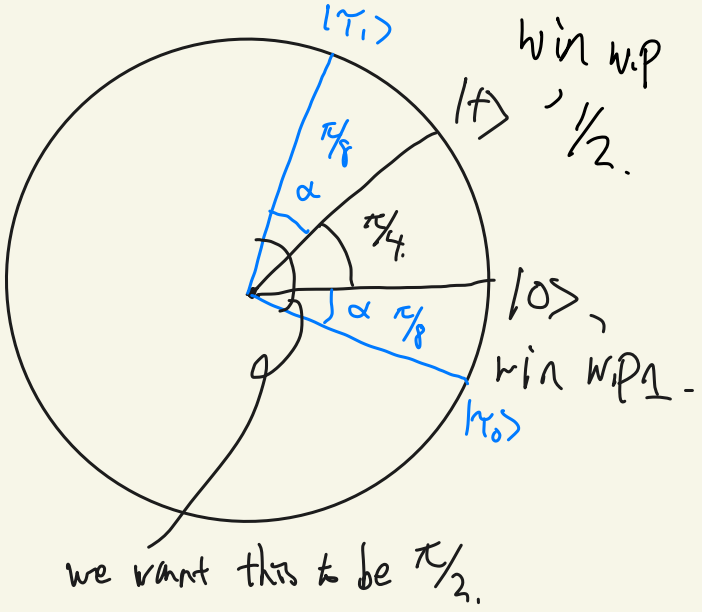
Exemplo

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

- Measure in the computational basis.

Outcome '0' $\rightarrow 0$

Outcome '1' $\rightarrow 1$.



$$P = 3/4$$

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

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

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

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

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

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

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

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

$\{|e_i\rangle\}$ 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:

$$p_i = \langle e_i | \rho_0 | e_i \rangle \cdot \Pr[\text{Bob output } |e_1\rangle \mid \rho_0]$$

$$q_i = \langle e_i | \rho_1 | e_i \rangle \qquad \Pr[\quad \text{“} \quad | \rho_1]$$

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

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

$$\Pr[\quad \text{“} \quad | b=1] = \sum_{i,\, \delta_i < 0} q_i$$

↓

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

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

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

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

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

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

$$\Rightarrow \frac{1}{2} + \frac{D(P_0, P_1)}{2}.$$

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.

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

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

For pure state.

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

If ρ and σ are diagonalizable in the same basis.

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

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

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 $\mathrm{Tr}(|\psi\rangle\langle\psi|_{AB}) = \rho_B$.

Uhlmann's theorem

For any ρ, σ, $F(\rho,\sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle\psi|\phi\rangle|$.

where $|\psi\rangle$ (resp. $|\phi\rangle$) is a purification of ρ (resp. σ).

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

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

where max over all purification of ρ.

Fochs Van de Groof inequality

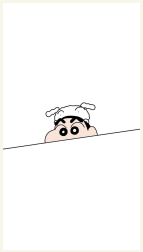
For any states ρ, σ

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

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 functions

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

1) Commit Phase :

Alice commits to $b \in \{0,1\}$

Bob should not be cable to guess b.

Security requirements.

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

Hiding. If Alice is honest and Bob cheats,

$$\Pr(B \text{ ab guesses } b) = p^*_B.$$

Binding:

24. Feb. 23.

example.

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

attemp: 1.

commit phase
- Alice and Bob share $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- if $b=0$, Alice measure in the computational basis
- if $b=1$, ——— Hadamard basis.

- reveal: reveal b.

~~~

$\rho_0 = |0\rangle\langle 0|$

ρ_b: $\rho_1 = |+\rangle\langle +|$.

not orgonal: or not equal. state can represent partial information about b.
~~~

BC - proof.

Commit

if $b=0$: Alice sends $|0\rangle$

if $b=1$: ——— $|+\rangle$

Reveal

Alice reveal b.

if $b=0$: Bob measure in comp. basis

if $b=1$: ———→

Genetic Bit Commitment protocol.

Let $|\psi^0_{AB}\rangle, |\psi^1_{AB}\rangle$ be two quantum bipartite states.

Consider the following protocol:

Commit: Alice wants to commit to b.

She constructs $|\psi^b_{AB}\rangle$ and sends the B register to Bob.

Bob has $\rho_b = Tr_A(|\psi^b_A\rangle\langle\psi^b_{AB}|)$ after commit.

Reveal: Alice reveals b and sends the A register to Bob.

He measure using measurement

$$\{|\psi^b_{AB}\rangle\langle\psi^b_{AB}|, I - |\psi^b_{AB}\rangle\langle\psi^b_{AB}|\}$$

Accept reject.

Cheating Alice sends a states a state σ to Bob,

(and potentially keeps a

equivelancy, Alice construct.

$$|\Omega_{AB}\rangle \quad \text{s.t.} \quad Tr_A(|\Omega_{AB}\rangle\langle\Omega_{AB}|) = \sigma$$

At the reveal phase ; Alice wants to reveal σ.

She can apply a local unitary.

U_σ on the A register before sends it to Bob.

$|\Omega^\sigma_{AB}\rangle$ is the state that Bob has, after the reveal.

Goal for Alice : $|\Omega^0_{AB}\rangle = |\psi^0_{AB}\rangle$.

$|\Omega'_{AB}\rangle = |\psi'_{AB}\rangle$.

But : $Tr_A\left(|\Omega^0_{AB}\rangle\langle\Omega^0_{AB}|\right) = Tr_A\left(|\Omega'_{AB}\rangle\langle\Omega'_{AB}|\right) = \sigma$

$$|\Omega^\sigma_{AB}\rangle = \left(U^\sigma_B \otimes I_A\right)|\Omega_{AB}\rangle$$

$Tr_B\left(|\Omega^0_{AB}\rangle\langle\Omega^0_{AB}|\right) = P_0$

$Tr_B\left(|\Omega'_{AB}\rangle\langle\Omega'_{AB}|\right) = P_1$.

$$P^{\text{Alice}}_A = \frac{1}{2}\left|\langle\Omega^0_{AB}|\psi^0_{AB}\rangle\right|^2 + \frac{1}{2}\left|\langle\Omega'_{AB}|\psi'_{AB}\rangle\right|^2$$

//.

$$|\langle \Omega^0_{AB} | \psi^0_{AB} \rangle|^2 \leq F^2(\sigma, \rho_0)$$

$$|\langle \Omega^1_{AB} | \psi^1_{AB} \rangle|^2 \leq F^2(\sigma, \rho_1)$$

$$p_A^* \leq \frac{1}{2}\left(F^2(\rho_0, \sigma) + F^2(\rho_1, \sigma)\right)$$

$$p_B^* = \frac{1}{2} + \frac{1}{2} A(\rho_0, \rho_1)$$

$$p_{A\,(opt)}^* \leq \max_\sigma \left\{ \frac{1}{2}\left(F^2(\rho_0, \sigma) + F^2(\rho_1, \sigma)\right) \right\}$$

$$p_{B\,(opt)}^* = \frac{1}{2} + \frac{1}{2} \Delta(\rho_0, \rho_1)$$

Lemma: $\forall \sigma$: $\frac{1}{2}\left(F^2(\sigma, \rho_0) + F^2(\sigma, \rho_1)\right)$

$$\leq \frac{1}{2}\left(1 + F(\rho_0, \rho_1)\right)$$

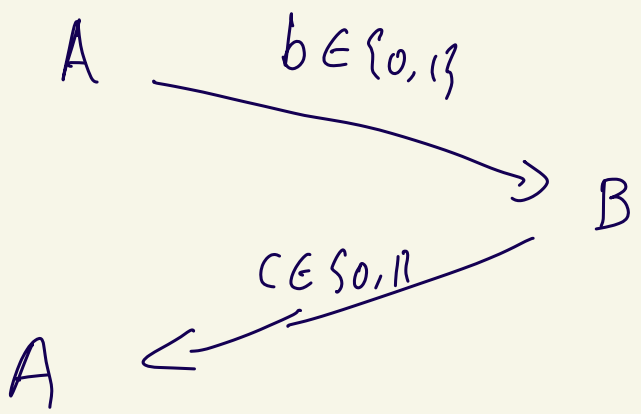
$$\Rightarrow \quad p_A^* \leq \frac{1}{2} + \frac{1}{2} F(\rho_0, \rho_1)$$

$$p_B^* \leq \frac{1}{2} + \frac{1}{2} \Delta(\rho_0, \rho_1)$$

$$p_A^* + p_B^* = 1 + \frac{1}{2}\left(F(\rho_0, \rho_1) + \Delta(\rho_0, \rho_1)\right)$$

- there exists a quantum bit commitment protocol s.t. $P_A^*, P_B^* \simeq 0.739$

Bit commitment based coin flipping



Bob can cheat by saying he get the same bit.

output is $\boxed{c \oplus b}$.

08.03.23.

Quantum key Distribution

key distribution.

- Alice and Bob communicated over a public and authenticated channel.
- At the end of the protocol, they should agree on a key $\in \{0,1\}^k$.
- An eavesdropper Eve shouldn't have any information (or really small information) about K.

means that both side knows that there're nobody in between.

Diffie-Hellman protocol.

p: prime number,

g: generator of $(\mathbb{Z}/p\mathbb{Z})^* = \{1, \dots, p-1\}$.

$(g^0 = 1, g, g^2, \dots, g^{p-1})$

$[p]$ $[p]$.

Discrete log: given $g^k [p]$, Find k.

- g, p are public.
- Alice picks a random $a \in \{2, \ldots, p-1\}$.

  Computes $A = g^a$ and sends A to Bob.
- Bob picks a random $b \in \{1, -, p-1\}$

  compute $B = g^b$. and send B to Alice.

The secret key is $K = g^{ab} = (A^b) = (B^a)$

g^b: Bob can compute

g^a: Alice can compute

1. Classical KD -
2. Quantum KD -

Alice has a string $k_{init} = (k_1, \_, k_n) \in \{0,1\}^n$.

Her goal is to transmit k_{init} (or part of k_{init}) to Bob s.t. Eve has no information about these bits.

BB84 Encoding of k_i

- Pick a random $b_i \in \{0,1\}$
- If $b_i = 0$, construct $|\psi_i\rangle = |k_i\rangle$
  If $b_i = 1$, construct $|\psi_i\rangle = H|k_i\rangle$.
- Output $|\psi_i\rangle$

k_i	b_i	$\|\psi_i\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

with known k_i

$P_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$, $P_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|-\rangle\langle -|$.

$\sigma_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, $\sigma_1 = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \sigma_0$.

with known b_i

The protocol starts like ...

① Alice picks a random $k_{init} = k_1, \_, k_n$.

② For each i, Alice picks random ~~$b_i \in \{0,1\}$~~ and sends $|\psi_i\rangle$ constructed by ~~the~~ BB84 protocols.

③ Bob picks a ~~basis~~ $b'_1, \_, b'_n$ at random. measures each $|\psi_i\rangle$ ~~in the basis~~ b'_i, let C be the outcome of this measurement.

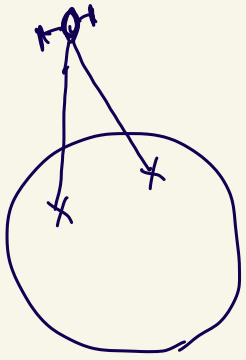
The BB84 protocol

everything sent is sent to public

- Alice picks a random initial raw key $K = k_1, \ldots, k_n$ uniformly at random.
- For each $i \in \{1, \ldots, n\}$, Alice picks a random $b_i \in \{+, \times\}$, constructs $|\psi_i\rangle = |k_i\rangle^{b_i}$ and sends $|\psi_i\rangle$ to Bob.
- Bob picks some random basis $b'_1, \ldots, b'_n \in \{+, \times\}$ and measures each qubit $|\psi_i\rangle$ in the b'_i basis. Let c_i be the outcome of this measurement.
- Bob sends to Alice the basis $\mathbf{b}' = b'_1, \ldots, b'_n$ he used for his measurements using a public channel. Alice sends back the subset $I = \{i \in [n] : b_i = b'_i\}$ to Bob.
- Alice then picks a random subset $J \subseteq I$ of size $\frac{|I|}{2}$ which is the subset of indices for which Alice and Bob check that there wasn't any interception and sends J to Bob. For $j \in J$, Alice also sends k_j to Bob. — with noise, it can be $\neq$.
- For each $j \in J$, Bob checks that $k_j = c_j$. If one of these checks fail, he aborts.
- Let $L = I \backslash J = l_1, \ldots, l_{|L|}$ be the subset of indices used for the final raw key. We write $K_A = \{k_l\}_{l \in L}$ and $K_B = \{c_l\}_{l \in L}$.
- Alice and Bob perform key reconciliation to agree on a key K_{raw}.
- They perform privacy amplification to ensure that Alice has no information about the key.

- Alice and Bob perform key reconciliation. to agree on a common knew $\in \{0,1\}^A$
- they perform privacy amplification to agree on $k \in \{0,1\}^k$ unknown to Eve.

noise and loss.

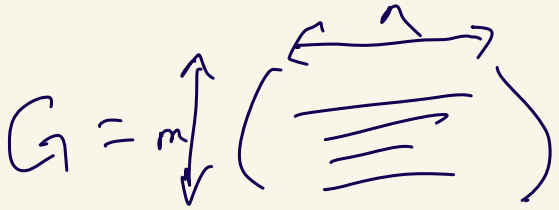


Classical error correction

repetition code.

Parity check:

→ can be generalized to linear codes.

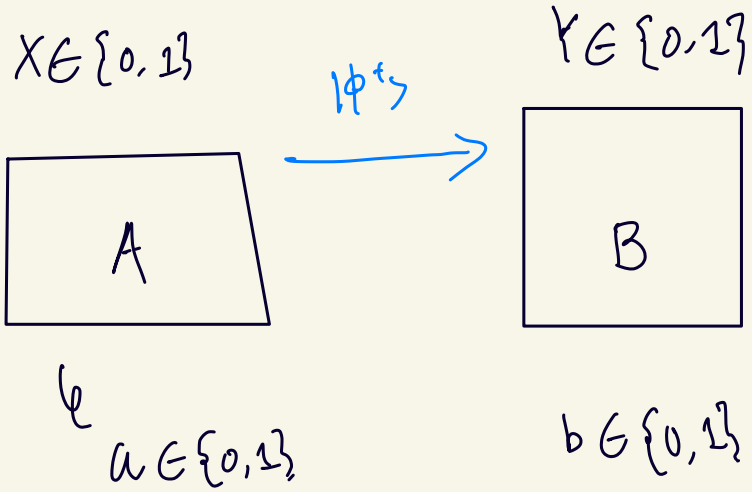


Entangled games & Bell's inequalities.

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$$

Recap of CHSH

win : $a \oplus b = x \wedge y$.



Proposition :

classical.

Sum the condition and then ie leads to contradiction

$$f_A(0) \oplus f_B(0) = 0 \wedge 0 = 0$$
$$f_A(0) \oplus f_B(1) = 0 \wedge 1 = 0$$
$$f_A(1) \oplus f_B(0) = 1 \wedge 0 = 0$$
$$f_A(1) \oplus f_B(1) = 1 \wedge 1 = 1$$

$\hookrightarrow$ $0 = 1$. contradiction

Quantum entropy

Classical entropy

Def. : let $p = (p_1, \dots p_n)$ be a discrete probability function $p_i \geq 0$, $\sum_i p_i = 1$.

the entropy is of defined as:

$$H(p) = \sum_i -p_i \log_2(p_i).$$

degree of randomness

amount

Ex

- $p_1 = 1$, $p_2 = 0$. $(n=2)$ $H(p) = 0$
- $p_1 = p_2 = 1/2$.

$$H(p) = -\tfrac{1}{2}\overbrace{\log_2(1/2)}^{-1} - \tfrac{1}{2}\overbrace{\log_2(1/2)}^{-1} = 1.$$

- $p_1 = 3/4$ $p_2 = 1/4$

$$H(p) = -\tfrac{3}{4}\log_2(3/4) - \tfrac{1}{4}\log_2(1/4) = -\tfrac{3}{4}\left(\log_2(3) - 2\right) + \tfrac{1}{4}\cdot 2$$

$$= 2 - \frac{3\log_2(3)}{4} \simeq 0.8$$

Take $P_0 = 3/4$, $P_1 = 1/4$

take the 2-fold repetition.

$P_{00} = \frac{9}{16}$: $P_{01} = P_{10} = \frac{3}{16}$, $P_{11} = \frac{1}{16}$.

strategy for submitting her two bits.

If (0,0) -> send 0

If (0,1) -> send 01.

If (1,0) -> 011

If (1,1) -> 111

average amount of bits send.

$$\frac{9}{16} \cdot 1 + \frac{3}{16} \cdot 2 + \frac{3}{16} \cdot 3 + \frac{1}{16} \cdot 3 = \frac{27}{16}$$

$$= 1.6875 < 2.$$

- you can use entropy to compress information.

Quantum entropy

Def: Let $\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$ in spectral decomposition

we define $S(\rho)$ as

$$S(\rho) = \sum_i -\lambda_i \log_2(\lambda_i)$$
$$= H(\lambda_1, \dots, \lambda_n).$$

Properties

U: unitary operation

- $S(U\rho U^\dagger) = S(\rho)$

$U: |e_i\rangle \to |f_i\rangle$

$$U\rho U^\dagger = \sum_i \lambda_i |f_i\rangle\langle f_i|$$

$$S(U\rho U^\dagger) = H(\lambda_1, \dots, \lambda_n) = S(\rho)$$

- $S(\rho) \geq 0$
- $S(\rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B)$

Proposition Let ρ be a quantum state.

Let $\Pi = \{\Pi_1, \cdots, \Pi_n\}$ be a projective measurement.

Let $p_i = \mathrm{tr}(\rho \Pi_i)$

We have $S(\rho) \geq H(p)$

Quantum Error Correction

I. Classical error correction.

Alice has $b_1, \dots, b_n \in \{0,1\}^n$ ⟶ Bob has $b_1', \dots, b_n' \in \{0,1\}^n$.

sometimes : $b_i' \neq b_i$.

$\Pr(b_i' \neq b_i) = p \quad (\forall i)$

How to ensure that Bob knows b_i?

1) Repetition code

- repeat twice

$b_i = 0$: I send 00

if $b_i = 1$: I send 11.

Bob sees.

00 : Bob thinks $b_i = 0$

01 : no idea.

10 : guess b_i random

11 : Bob thinks $b_i = 1$

If $b_i = 0$.

guess w.p

- Bob gets 00 w.p $(1-p)^2$ → 1.
- — 01 w $p(1-p)$ → 1/2
- — 10 — → 1/2
- — 11 — p^2 → 0.

Total probability.

$$(1-p)^2 + p(1-p)\cdot\frac{1}{2} + p(1-p)\cdot\frac{1}{2}$$

$$= 1-p.$$

repeat 3 times.

To send 0, Alice sends 000.

To send 1, Alice sends 111.

resending into increase noise.

Bob sees

000, 001, 010, 100 } bob thinks $b_i = 0$

101, 110, 011, 111 } bob thinks $b_i = 1$.

Probability Bob correctly guesses b_i (when $b_i = 0$)

$$= (1-p)^3 + 3 \cdot (1-p)^2 \cdot p \cdot 1 + \cancel{3p^2(1-p) \cdot 0 + p^2 \cdot 0}$$

$$= -p^3 + 3p^2 - 3p + 1 + 3(p^3 - 2p^2 + p)$$

$$= 2p^3 - 3p^2 + 1 \quad \text{v.s.} \quad (1-p)$$

$$= (p-1)(2p^2 - p - 1) \quad = (1-p)(1+p-2p^2) \overset{?}{\geq} (1-p)$$

$$\overset{?}{1} + p - 2p^2 \geq 1$$

$$\iff 2p^2 - p \leq 0$$

$$\iff p(2p-1) \leq 0$$

$$\iff (2p-1) \leq 0$$

$$\iff p \leq 1/2.$$

II) Quantum error correction.

1. Noise model.

$X \rightarrow |\psi\rangle' = \alpha|1\rangle + \beta|0\rangle$

We have a qubit $|\psi\rangle \longrightarrow |\psi'\rangle$.

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

with some probability

$|\psi'\rangle = \alpha|0\rangle - \beta|1\rangle$.

$= \alpha|0\rangle + i\beta|1\rangle$.

$\vdots$

$|\psi\rangle\langle\psi| \rightarrow (1-p)|\psi\rangle\langle\psi| + pI$.

- an infinite amount of possible noises.

Proposition: If we can correct bit flips X and phase flip Z.

then we can correct all types of errors.

2) the quantum repitition code

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

wants to send $|\psi\rangle$ to Bob using

Alice doesn't know α, β.

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \rightarrow (\alpha|000\rangle + \beta|111\rangle)$$

Bob gets — only taken account bit flips.

w.p $(1-p)^3$: $\alpha|000\rangle + \beta|111\rangle$ S_1

w.p $(1-p)^2 p$: $\alpha|100\rangle + \beta|011\rangle$ S_2

— : $\alpha|010\rangle + \beta|101\rangle$ S_3

— : $\alpha|001\rangle + \beta|110\rangle$:

w.p. $p^2(1-p)$: $\alpha|011\rangle + \beta|100\rangle$.

— $\alpha|101\rangle + \beta|010\rangle$.

— $\alpha|110\rangle + \beta|001\rangle$.

w.p. p^3 : $\alpha|111\rangle + \beta|000\rangle$ S_8

Bob's recovery strategy

$|000\rangle \rightarrow |000\rangle$

$|111\rangle \rightarrow |111\rangle$

ideally $|001\rangle \rightarrow |000\rangle$ ✗ we cannot do because

$|110\rangle \rightarrow |111\rangle$ ✗ two different states.

→ We add an extra register

$|000\rangle|0\rangle \longrightarrow |000\rangle|0\rangle$

$|111\rangle|0\rangle \longrightarrow |111\rangle|0\rangle$

$|001\rangle|0\rangle \longrightarrow |000\rangle|3\rangle$

$|110\rangle|0\rangle \longrightarrow |111\rangle|3\rangle$

$|010\rangle|0\rangle \longrightarrow |000\rangle|2\rangle$

$|101\rangle|0\rangle \longrightarrow |111\rangle|2\rangle$

$|100\rangle|0\rangle \longrightarrow |000\rangle|1\rangle$

$|011\rangle|0\rangle \longrightarrow |111\rangle|1\rangle$

After some strategy., Bob gets.

$|S_1\rangle = (\alpha|000\rangle + \beta|111\rangle) \otimes |0\rangle$

$|S_2\rangle = (\alpha|000\rangle + \beta|111\rangle) \otimes |1\rangle$

$|S_3\rangle = (\quad\quad\quad) \otimes |2\rangle$

$|S_4\rangle = (\quad\quad\quad) \otimes |3\rangle$

$|S_5\rangle = (\beta|000\rangle + \alpha|111\rangle) \otimes |1\rangle$ $\Rightarrow$ Bad recovery.

$\vdots$

$|S_8\rangle$

From $\alpha|000\rangle + \beta|111\rangle$, we can easily recover

$\alpha|0\rangle + \beta|1\rangle$.

$\rightarrow$ this is bad for phase flip.

$$\alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|000\rangle - \beta|111\rangle$$

$$\Downarrow$$

recovery.

$$(\alpha|000\rangle - \beta|111\rangle) \otimes |0\rangle$$

$$\Downarrow$$

$$\alpha|0\rangle - \beta|1\rangle.$$

Idea of Correcting phase flips.

A phase flip in the computational basis.

$\Leftrightarrow$ A bit flip in the Hadamard basis.

Bit flip : $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$

$|+\rangle \to |+\rangle$, $|-\rangle \to -|-\rangle$

phase flip : $|0\rangle \to |0\rangle$ $\quad |1\rangle \to -|1\rangle$

$|+\rangle \to |-\rangle$ $\quad |-\rangle \to |+\rangle$

In order to correct phase flips.

Alice has $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$= \alpha'|+\rangle + \beta''|-\rangle$

Alices sends $\alpha|+++\rangle + \beta'|---\rangle$.

Model : Apply a phase flip on each wire

w.p. $(1-p)^3$: Bob has $\alpha'|+++\rangle + \beta'|---\rangle$.

w.p $p(1-p)^2$ ——— $\alpha'|++-\rangle + \beta'|--+\rangle$

w.p $p^2(1-p)$ ——— $\alpha'|+--\rangle + \beta'|-++\rangle$

w.p p^3 ——— $\alpha'|---\rangle + \beta'|+++\rangle$

Recap.

III). Shor's 9 qubit code.

we use 2 levels of encoding to protect from both bit flip and phase flip.

- We start from $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha'|+\rangle + \beta'|-\rangle$

Outer encoding : protect against phase flip.

$$|\psi\rangle \longrightarrow \alpha'|+++\rangle + \beta'|---\rangle = |\psi_1\rangle$$

$$|\psi_1\rangle = \alpha'\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes 3} + \beta'\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes 3}$$

Inner encoding : protect each qubit from bit flip

$$|\psi_1\rangle \rightarrow |\psi_2\rangle = \alpha'\left(\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle\right)^{\otimes 3}$$

$$+ \beta'\left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle\right)^{\otimes 3}$$

N. ≠.

I encode my qubits $|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle$.

$$\Rightarrow |\psi_2\rangle = \alpha' \Big[\Big(\tfrac{1}{\sqrt{2}}|000\rangle + \tfrac{1}{\sqrt{2}}|111\rangle\Big)_{123} \otimes \Big(\tfrac{1}{\sqrt{2}}|000\rangle + \tfrac{1}{\sqrt{2}}|111\rangle\Big)_{456} \otimes \Big(\tfrac{1}{\sqrt{2}}|000\rangle + \tfrac{1}{\sqrt{2}}|111\rangle\Big)_{789} \Big]$$

$$+ \beta' \Big[\Big(\tfrac{1}{\sqrt{2}}|000\rangle - \tfrac{1}{\sqrt{2}}|111\rangle\Big)_{123} \otimes \Big(\tfrac{1}{\sqrt{2}}|000\rangle - \tfrac{1}{\sqrt{2}}|111\rangle\Big)_{456} \otimes \Big(\tfrac{1}{\sqrt{2}}|000\rangle - \tfrac{1}{\sqrt{2}}|111\rangle\Big)_{789} \Big].$$

This protect from any 2 bit flip error as

1 phase flip error