

חשבון ממוצע - קוונטום HSP - I

הצורה ρ היא ממוצע (density matrix) של σ_1, σ_2 .
 נניח σ_1, σ_2 הם 2×2 matrices. $\rho = \frac{1}{2}(\sigma_1 + \sigma_2)$.
 האם ρ הוא density matrix? $\rho \geq 0$?

יש לנו $\rho = \frac{1}{2}(\sigma_1 + \sigma_2)$. σ_1, σ_2 הם density matrices.
 כלומר $\sigma_1 \geq 0, \sigma_2 \geq 0$.
 האם $\rho \geq 0$?
 נניח $\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
 אז $\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} I$.
 זהו density matrix.

$$Pr[i] = \frac{1}{2} \text{Tr}(\sigma_1 E) + \frac{1}{2} \text{Tr}(\sigma_2 (I - E))$$

נניח $\rho = \frac{1}{2}(\sigma_1 + \sigma_2)$

$$= \frac{1}{2} \text{Tr}(\sigma_2) + \frac{1}{2} \text{Tr}(E(\sigma_1 - \sigma_2))$$

אם $E \geq 0$ אז $\text{Tr}(EX) \geq 0$ עבור $X \geq 0$.

$$\text{Tr}(EX), \quad X = \sigma_1 - \sigma_2$$

אם $E \geq 0$ אז $\text{Tr}(EX) \geq 0$ עבור $X \geq 0$.
 אבל $\sigma_1 - \sigma_2$ אינו ≥ 0 .
 לכן $\text{Tr}(E(\sigma_1 - \sigma_2))$ יכול להיות שלילי.

X הוא matrix הריינג' $\sigma_1 - \sigma_2$.
 האם ρ הוא density matrix?

$$X = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$$

$$X_+ \triangleq \sum_{i|\lambda_i \geq 0} \lambda_i |\psi_i\rangle \langle \psi_i|$$

100

$$X_- \triangleq \sum_{i|\lambda_i < 0} \lambda_i |\psi_i\rangle \langle \psi_i|$$

כל $0 \leq \lambda_i$ של $\lambda_1, \dots, \lambda_n$ יוצרים E כך ש

$$E = \sum_{i|\lambda_i \geq 0} |\psi_i\rangle \langle \psi_i|$$

$E \in \mathbb{R}^{n \times n}$ ו- λ_i הם הערכים העigen של E ו- $\lambda_i \geq 0$

$$P_r[\psi] = \frac{1}{2} \left(1 + \underbrace{\text{Tr}(E(\sigma_1 + \sigma_2))}_{\text{Tr}(X_+)} \right)$$

$$\sigma_1 - \sigma_2 = X = X_+ + X_-$$

100

$$0 = \text{Tr}(X) = \text{Tr}(X_+) + \text{Tr}(X_-)$$

$\Leftarrow$

$$(8) \quad \text{Tr}(X_+) = -\text{Tr}(X_-)$$

$\Leftarrow$

כל $X \in \mathbb{R}^{n \times n}$ יש $\lambda_1, \dots, \lambda_n$ ו- $\lambda_i \geq 0$ ו- $\lambda_i \leq 0$ ו- $\lambda_i = 0$

$$\text{Tr}(X) =$$

הערה

$$\text{Tr}(X_+ - X_-) = \sum_i |\lambda_i|$$

$$\textcircled{C} \text{Tr}(X_+) - \text{Tr}(X_-) \stackrel{\text{מכאן}}{=} 2 \text{Tr}(X_+)$$

הערה

→ מכאן נובע כי המרחק בין X_+ ל- X_- הוא $2\|X_+\|_{\text{Tr}}$

$$P_r[\ddot{U}] = \frac{1}{2} + \frac{1}{4} \sum_i |\lambda_i|$$

הערה: $\lambda_1, \dots, \lambda_n$ הם הערכים העigen של X (המרחק בין X_+ ל- X_-) → מכאן נובע כי המרחק בין X_+ ל- X_- הוא $2\|X_+\|_{\text{Tr}}$

$$\|X\|_{\text{Tr}} \triangleq \sum_{i=1}^n |\lambda_i|$$

הערה: $\|X\|_{\text{Tr}}$ הוא המרחק בין X_+ ל- X_-

→ $\|X\|_1$ הוא סכום הערכים העigen של X

לכן $\|X\|_{\text{Tr}}$ הוא המרחק בין X_+ ל- X_-

$$\|X\|_{\text{Tr}} = \text{Tr} \sqrt{X^+ X} = \text{Tr} \sqrt{X^2}$$

הערה: $\|X\|_{\text{Tr}}$ הוא המרחק בין X_+ ל- X_-

לכן $\|X\|_{\text{Tr}}$ הוא המרחק בין X_+ ל- X_-

לכן $\|X\|_{\text{Tr}}$ הוא המרחק בין X_+ ל- X_-

$$P_r[\ddot{U}] = \frac{1}{2} + \frac{1}{4} \|\sigma_1 - \sigma_2\|_{\text{Tr}}$$

מאמק, כחץ יש רון וליטה איתן אלוטוטי — מקלים מסיקה
(מרה). ואמ, צי מוקר יי הלוטו א בסיס

$$\text{Dist}(\sigma_1, \sigma_2) \stackrel{\Delta}{=} \frac{1}{2} \|\sigma_1 - \sigma_2\|_1$$

↑
ניטח מקול

לקרי → Trace Distance

באמק — היגד כי נוס אהסן שהסמכה — העס' מקמין יין יס
! יס נוס יי

$$P_1[\cdot] = \frac{1}{2} + \frac{1}{2} \text{Dist}(\sigma_1, \sigma_2)$$

יסנה הקרה חסרה נוסס — מליז — מונק (ווא, רויט ויק, קירי)
דין מקים קונו"ר:

הקרה (מאנו) Fidelity
ה fidelity א יי מקרה (מ.ל. — לביט) ρ יי
מאנו יי

$$F(\rho, \sigma) \stackrel{\Delta}{=} \|\sqrt{\rho} \sqrt{\sigma}\|_{\text{Tr}} \\ = \text{Tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}}$$

אין א ניסח מוסמך מלתי מהקרה בי — מליז — מליז
קרים הקו. ריכין מונק א fidelity ρ Trace
distance הא הימקו — מליז

(12-2) → JOC

$$F(\rho^{\otimes n}, \sigma^{\otimes n}) = F(\rho, \sigma)^n$$

Trace Norm & Fidelity - נקרא גם
Fuchs - van de Graaf

Def (האנרגיה הקטנה ביותר של ρ)

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

אם ρ ו- σ הם מדידות ב- $\mathcal{H}$ אז
ההסתברות של ρ להיות
ב- $\mathcal{H}_1$ היא $\text{Tr}(\rho P_{\mathcal{H}_1})$ וכן
ההסתברות של σ להיות
ב- $\mathcal{H}_1$ היא $\text{Tr}(\sigma P_{\mathcal{H}_1})$.

Def נקרא ρ ו- σ orthogonal אם
ההסתברות של ρ להיות
ב- $\mathcal{H}_1$ היא 0 או 1.

$$1 - m \cdot \max_{i \neq j} F(\rho_i, \rho_j)$$

HSP - נקרא

הבעיה של ρ ו- σ להיות
orthogonal היא NP-Complete.
כלומר, אין אלגוריתם פולינומי
לפתור אותה.

$$\rho_H = \frac{1}{|G|} \sum_{g \in G} |g_H\rangle\langle g_H|$$

כלומר, ρ_H הוא הממוצע
של כל המדידות ρ_g עבור
כל $g \in G$.

הם גם רגילים של G וכן H' וכן H' וכן H'

$$\{ \rho_{H'} \mid H' < G \}$$

וזהו תוצאה

הוא $q = \text{poly} \log |G|$ וזהו תוצאה של HSP_G וכן HSP_G

הוא G וכן G וכן G וכן G

$$m \leq 2^{\log^2 |G|}$$

$k \rightarrow \text{poly} |G|$ וכן G וכן G וכן G וכן G

$$H = \langle h_1, h_2, \dots, h_k \rangle$$

$H_{l+1} = \langle h_1, \dots, h_{l+1} \rangle$ וכן H_l וכן H_l וכן H_l

$$|H_{l+1}| \geq 2 |H_l|$$

$$|G| \geq |H| \geq 2^h$$

$\Leftarrow$

$$h \leq \log_2 |G| \Leftarrow$$

הוא $\log_2 |G| \geq \gamma \rightarrow \exists G \in \mathcal{G}$ וכן G וכן G וכן G

$$\binom{|G|}{\log_2 |G|} \leq 2^{\log^2 |G|}$$

לפי

המשפט של גולדשטיין, יש קבוצה של q מספרים שבהם

$$1 - m \cdot \max_{\substack{H \neq H' \\ |G| \leq G}} F(p_H, p_{H'})$$

$\nearrow$

$m \leq 2^{\log^2 |G|}$

יש קבוצה של m מספרים p_H ו- $p_{H'}$ כך שלכל $H \neq H'$ מתקיים $F(p_H, p_{H'}) \leq \frac{1}{m}$.
 נניח שיש קבוצה של m מספרים p_H ו- $p_{H'}$ כך שלכל $H \neq H'$ מתקיים $F(p_H, p_{H'}) \leq \frac{1}{m}$.
 נניח שיש קבוצה של m מספרים p_H ו- $p_{H'}$ כך שלכל $H \neq H'$ מתקיים $F(p_H, p_{H'}) \leq \frac{1}{m}$.
 נניח שיש קבוצה של m מספרים p_H ו- $p_{H'}$ כך שלכל $H \neq H'$ מתקיים $F(p_H, p_{H'}) \leq \frac{1}{m}$.

$$1 - 2^{\log^2 |G|} \cdot \max_{H \neq H'} F(p_H^{\otimes t}, p_{H'}^{\otimes t})$$

$$= 1 - 2^{\log^2 |G|} \cdot \left(\max_{H \neq H'} F(p_H, p_{H'}) \right)^t$$

הקבוצה של m מספרים p_H ו- $p_{H'}$ היא

$$\max_{H \neq H'} F(p_H, p_{H'}) < 0.9$$

אם $t = O(\log^2 |G|)$ אז $1 - 2^{\log^2 |G|} \cdot (0.9)^t > 0$.
 כלומר, יש קבוצה של m מספרים p_H ו- $p_{H'}$ כך שלכל $H \neq H'$ מתקיים $F(p_H, p_{H'}) < 0.9$.

$$D(p_H, p_{H'}) \geq \frac{1}{2} \quad \forall H \neq H'$$

$\forall H \neq H'$

$\frac{1}{2}$

for arbitrary $p_H, p_{H'}$, just

$$\sqrt{1 - F(p_H, p_{H'})^2} \geq D_{\frac{1}{2}}(p_H, p_{H'}) \geq \frac{1}{2}$$

$$F(p_H, p_{H'}) \leq \frac{\sqrt{3}}{2} \quad (< 1)$$

$\Leftarrow$

for arbitrary $p_H, p_{H'}$ — $D(p_H, p_{H'})$ is the distance between p_H and $p_{H'}$ in the simplex

$$Pr[\tilde{c}] = \frac{1}{2} + \frac{1}{2} D_{\text{dist}}(p_H, p_{H'})$$

given a code $\tilde{c}$, $\frac{1}{2} \rightarrow$ the probability of success if $p_H = p_{H'}$.
 $\frac{3}{4} \leq Pr[\tilde{c}] \leq \frac{1}{2} + \frac{1}{2} D_{\text{dist}}(p_H, p_{H'}) \Rightarrow D_{\text{dist}} \geq \frac{1}{2}$

$$\frac{3}{4} \leq Pr[\tilde{c}] \leq \frac{1}{2} + \frac{1}{2} D_{\text{dist}}(p_H, p_{H'}) \Rightarrow D_{\text{dist}} \geq \frac{1}{2}$$

$|H| \geq |H'| \Rightarrow$: p_H is a PPM $\Rightarrow$ the message p is in H

$$E = \frac{|G|}{|H|} p_H$$

$(E, I-E)$ is a code

: p_H is a PPM $\Rightarrow$ the message p is in H

$$E = \frac{|G|}{|H|} p_H = \frac{|G|}{|H|} \cdot \frac{1}{|G|} \sum_{g \in G} |g_H \times g_H|$$

$$= \frac{1}{|H|} \sum_{g \in G} |gH X gH|$$

← $\begin{matrix} \text{הסדרות } \rightarrow \text{הן } gH \\ \text{בסדר } G \text{ . כל } gH \\ \text{הן } H \text{ . כל } gH \end{matrix}$

$$= \sum |C \times C|$$

C is an H -coset
of G

המחלקות הן $\{C \mid C \cap H = \emptyset\}$ ו- H בלבד

$$Pr[\bar{0}] = \frac{1}{2} \text{Tr}(E \rho_H) + \frac{1}{2} \text{Tr}((I - E) \rho_{H'})$$

$\begin{matrix} \text{ה } E \\ \text{ה } \rho_H \\ \text{ה } \rho_{H'} \end{matrix} \rightarrow$
$$= \frac{1}{2} \text{Tr}(\rho_H) + \frac{1}{2} \text{Tr}(\rho_{H'}) - \frac{1}{2} \text{Tr}(E \rho_{H'})$$

$$= 1 - \frac{1}{2} \text{Tr}(E \rho_{H'})$$

$$= 1 - \frac{|G|}{2|H|} \text{Tr}(\rho_H \rho_{H'})$$

$$\text{Tr}(\rho_H \rho_{H'}) = \text{Tr} \left[\left(\frac{1}{|G|} \sum_{g \in G} |gH X gH| \right) \left(\sum_{g' \in G} |g'H' X g'H'| \right) \right] \quad \text{כך}$$

$$= \frac{1}{|G|^2} \sum_{g, g'} \text{Tr}(|gH X gH| \overbrace{|g'H' X g'H'|}^{\text{כך}})$$

$$\begin{aligned} &= \langle gH | g'H' \rangle \cdot \text{Tr}(|gH X g'H'|) \\ &= |\langle gH | g'H' \rangle|^2 \end{aligned}$$

1a)

$$\langle gH | g'H' \rangle = \left\langle \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle, \frac{1}{\sqrt{|H'|}} \sum_{h' \in H'} |g'h'\rangle \right\rangle \quad \text{GK}$$

$$= \frac{1}{\sqrt{|H| \cdot |H'|}} \sum_{\substack{h \in H \\ h' \in H'}} \langle gh | g'h' \rangle$$

$$= \frac{|gH \cap g'H'|}{\sqrt{|H| \cdot |H'|}}$$

$$P_r[\cdot] = 1 - \underbrace{\frac{|G|}{2|H|} \cdot \frac{1}{|G|^2} \left(\frac{1}{\sqrt{|H| \cdot |H'|}} \right)^2}_{\frac{1}{2|G||H|} \cdot \frac{1}{|H| \cdot |H'|}} \sum_{g, g' \in G} |gH \cap g'H'|^2 \quad \text{pr}$$

$$= 1 - \frac{1}{2|G| \cdot |H|} \sum_{\substack{H \cap C \neq \emptyset \\ H' \cap C \neq \emptyset}} |C \cap C'|^2$$

$$= 1 - \frac{1}{2|G||H|} \cdot \sum_{g, g' \in G} 1$$

$$= 1 - \frac{1}{2|G||H|} \cdot \sum_{\substack{H \cap C \neq \emptyset \\ H' \cap C \neq \emptyset}} \sum_{\substack{g \in C \cap C' \\ g' \in C \cap C'}} 1$$

$$= 1 - \frac{1}{2|G||H|} \sum_{g, g' \in G} \mathbb{1} \left[g, g' \in C \cap C' \right] \quad \text{where } H \text{ is a subgroup of } G \text{ and } C, C' \text{ are cosets of } H$$

$$= 1 - \frac{1}{2|G||H|} \sum_{g, g' \in G} \mathbb{1} [g'g^{-1} \in H \cap H']$$

$$= 1 - \frac{1}{2|G||H|} \sum_{g \in G} |H \cap H'|$$

$$= 1 - \frac{|H \cap H'|}{2|H|}$$

$$\text{Since } H \cap H' \neq \emptyset, |H| \geq |H'|$$

$$|H| \geq 2|H \cap H'|$$

Since $H' \neq H$, $H \cap H' \neq H$.
Therefore, $|H \cap H'| < |H|$.

$$\Pr[\bar{c}] \geq 1 - \frac{|H|/2}{2|H|} = \frac{3}{4}$$