שעור 2

נזכור שקבענו כבר יותר בקופסה ורציף לחישוב הענין
יותר אינטואיטיבי
נסמן observables של

$$A^0 = A^0_0 - A^0_1$$

בהינתן כזה, אם יש POVM $\{E_i\}$
ולתוצאה i יש ערך λ_i

נגדיר

$$H = \sum \lambda_i E_i$$

נשים לב, שבכל מצב ρ

$$Tr(H\rho) = \sum \lambda_i \, Tr(E_i\rho) = \sum \lambda_i \, Pr(\text{תוצאה } i) =$$ תוחלת ערך המשחק בהנחה.

הסבר: אם נסמן ערך המשחק לתשובה $(-1)^a$
(במקרה הכללי) אם נסמן 1, -1

$$\begin{pmatrix} (-1)^0 = 1 & 0 & \text{תשובה} \\ (-1)^1 = -1 & 1 & \text{''} \end{pmatrix}$$

$$A^0 = A^0_0 - A^0_1$$

תוחלת ערך המשחק בהינתן ש A נשאל 0.
(0 נכון ערך 1, 1 תשובה ערך -1)

כנ"ל

$$A^1 = A^1_0 - A^1_1$$

$$B^0 = B^0_0 - B^0_1$$

$$B^1 = B^1_0 - B^1_1$$

אם עכשיו נחשב את $A^0 \otimes B^0$,

אז הע"ע המתאים למספר המבוקש ב- $s=0$, $t=0$

וערך המשחק, כמו הוע"ע, הוא את הו"ע $v \otimes w$,

ע"ע של $\lambda_v \cdot \lambda_w$, כי $(A \otimes B)(v \otimes w) = (Av) \otimes (Bw) = \lambda_v \cdot \lambda_w (v \otimes w)$.

כלומר $(-1)^{x_1} \cdot (-1)^{x_2} = (-1)^{x_1 \oplus x_2}$

ובפרט: אנו מקבלים $1 = (-1)^0$ אם $x_1 \oplus x_2 = 0$

ומקבלים $-1 = (-1)^1$ אם $x_1 \oplus x_2 = 1$,

מכאן ש- $A^0 \otimes B^0$ מייצג את תוחלת הניצחון/הפסד

בניסוי שקורה כש- $s=0$, $t=0$. הניצחון נקרא $a \oplus b = 0$

כנ"ל $A^0 \otimes B^1$ עבור הניסוי $s=0$, $t=1$

$A^1 \otimes B^0$ " " $s=1$, $t=0$

עבור $A^1 \otimes B^1$ – ניצחון – $\oplus = 0$; הפסד – $\oplus = 1$ — הפוך מהניצחון במשחק $a \oplus b = s \cdot t$

ולכן תוחלת הניצחון במשחק $a \oplus b = s \cdot t$

$$H = \frac{1}{4}\Big[\underbrace{A^0 \otimes B^0}_{\text{קורה } s=t=0} + \underbrace{A^0 \otimes B^1}_{\text{קורה } s=0,\ t=1} + \underbrace{A^1 \otimes B^0}_{\text{קורה } s=1,\ t=0} \overset{\text{הפוך}}{-} \underbrace{A^1 \otimes B^1}_{\text{קורה } s=1,\ t=1} \Big]$$

– כי מנצחים כש $a \oplus b = 1$

כלומר הפוך בין נצחון והפסד.

[illegible]

[illegible] $A \otimes A$ [illegible]

[illegible]

[illegible] $(A \otimes B)(C \otimes D) = AC \otimes BD$ [illegible]

[illegible]

[illegible]

[illegible]

[illegible] $\|v\| = \sqrt{\sum |v_i|^2}$

[illegible] $\|A\| = \max_v \frac{\|Av\|}{\|v\|}$

[illegible] $\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$ [illegible]

[illegible] $\|A\| = \max |\lambda_i(A)|$ [illegible]

[illegible]

$\|AB\| \le \|A\| \cdot \|B\|$

$\|A+B\| \le \|A\| + \|B\|$

$\|A \otimes B\| = \|A\| \cdot \|B\|$

[illegible]

[illegible]

[illegible]

$|\langle v|w\rangle| \le \|v\| \cdot \|w\|$

[illegible]

$\langle\psi| A_0\otimes B_0 + A_0\otimes B_1 + A_1\otimes B_0 - A_1\otimes B_1 |\psi\rangle$

$\leq \| (A_0\otimes B_0 + A_0\otimes B_1 + A_1\otimes B_0 - A_1\otimes B_1)|\psi\rangle \|$

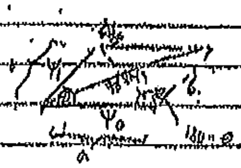
$\leq \| (A_0\otimes (B_0+B_1))\psi \| + \| (A_1\otimes (B_0-B_1))\psi \|$

$\leq \| (I\otimes (B_0+B_1))\psi \| + \| (I\otimes (B_0-B_1))\psi \|$

$= \| \psi_0+\psi_1 \| + \| \psi_0-\psi_1 \|$

$\psi_1 = (I\otimes B_1)\psi, \quad \psi_0 = (I\otimes B_0)\psi$

$\|\psi_0\| \leq 1 \quad \|\psi_0\| = \| I\otimes B_0 \, \psi \| \leq \| I\otimes B_0 \| \cdot \|\psi\| \leq \|B_0\| \leq 1$



$\underbrace{\|\psi_0+\psi_1\|} + \underbrace{\|\psi_0-\psi_1\|} =$

$\sqrt{a^2+b^2-2ab\cos(180-\theta)} + \sqrt{a^2+b^2-2ab\cos\theta}$

$= \sqrt{a^2+b^2+2ab\cos\theta} + \sqrt{a^2+b^2-2ab\cos\theta}$

$\leq \sqrt{2+2\cos\theta} + \sqrt{2-2\cos\theta}$

$|a|\,|b| \leq 1 \qquad \langle\psi_0|\psi_1\rangle = \cos\theta \; |\psi_0|\,|\psi_1|$

$\leq 2\sqrt{2}$

[illegible]

$$\|A\otimes B\psi\| = \sqrt{\psi^\dagger (A\otimes B)^\dagger A\otimes B\psi}$$

$$= \sqrt{\psi^\dagger A^\dagger A\otimes B^\dagger B\,\psi}$$

[illegible]

$A^\dagger A = I$

$$= \sqrt{\psi^\dagger I\otimes B^\dagger B\,\psi}$$

([illegible])

$$= \|I\otimes B\psi\|$$

The trace norm (הכללה לנורמה 1).

יהי A אופרטור לינארי

אז $|A| = \sqrt{A^{\dagger}A}$

הסבר: $AA^{\dagger} \geq 0$, לכן יש בסיס בו הוא אלכסוני $AA^{\dagger} = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$

ובבסיס זה $|A| = \sqrt{A^{\dagger}A} = \begin{pmatrix} \sqrt{\lambda_1} & & \\ & \ddots & \\ & & \sqrt{\lambda_n} \end{pmatrix}$

תכונה: $|A| \geq 0$

[יהי A ~~[illegible]~~ הרמיטי אם v ו"ע ו"ע λ

אז v הוא ו"ע של $|A|$ עם ע"ע $|\lambda|$: $v^{*}A^{\dagger}A v = \lambda^2 v$, $|A|v = |\lambda| \cdot v$]

הגדרה: $\|A\|_{tr} = Tr(|A|)$

תכונות: $\| \, \|_{tr}$ נורמה

$\|A+B\|_{tr} \leq \|A\|_{tr} + \|B\|_{tr}$

$\|A \cdot B\|_{tr} \leq \|A\| \cdot \|B\|_{tr}$

$\|A \cdot B\|_{tr} \leq \|A\|_{tr} \cdot \|B\|$

$\|A \otimes B\|_{tr} = \|A\|_{tr} \cdot \|B\|_{tr}$

$\forall_{U}$ $\|AU\|_{tr} = \|A\|_{tr}$

טענה: [illegible] [illegible] [illegible]

[illegible] [illegible] [illegible] [illegible] [illegible]

טענה לכל X: $\|X\|_{tr} = \max_{U} Tr(UX)$

מסקנה לכל X: $\|X\|_{tr} \geq Tr(X)$

6

מה טוב עבור להבחין בין 2 תערובות

נניח ש-ρ היא בהסתברות שווה או תערובת ρ_0
בהסתברות שווה, או תערובת ρ_1. נרצה לדעת.

אנו רוצים לבנות טסט הכי טוב שאפשר שיבחין בין
2 המקרים.

(אם $\rho_0=\rho_1$ אז נשאר רק לנחש קודם).

משפט 1: יש טסט T שמבחין

$$\Pr[T \text{ צודק}] \le \frac{1}{2} + \frac{\|\rho_0-\rho_1\|_{tr}}{4}$$

בחירת ρ_0, ρ_1 באקראי למקרים

הוכחה: נניח שיש לנו מדידה עם 2 תוצאות אפשריות

$$Q_0 + Q_1 = I \quad , \quad Q_0, Q_1 \ge 0$$

כש-Q_0 יוצא אומרים שזה "ρ_0"
וכש-Q_1 " " " "ρ_1"

$$\Pr[\text{נכון}] = \underbrace{\frac{1}{2}}_{\text{ההסתברות לבחור } \rho_0} Tr(Q_0 \rho_0) + \underbrace{\frac{1}{2}}_{\text{במקרה } \rho_1} Tr(Q_1 \rho_1)$$

$$\Pr[\text{טעות}] = \frac{1}{2} Tr(Q_0 \rho_1) + \frac{1}{2} Tr(Q_1 \rho_0)$$

$$\Pr[\text{נכון}] - \Pr[\text{טעות}] = \frac{1}{2} Tr(Q_0(\rho_0-\rho_1)) + \frac{1}{2} Tr(Q_1(\rho_1-\rho_0))$$
$$= \frac{1}{2} Tr((Q_0-Q_1)(\rho_0-\rho_1))$$

$$\le \frac{1}{2} \| (Q_0 - Q_1) \cdot (\rho_0 - \rho_1) \|_{tr}$$

$$\le \frac{1}{2} \underbrace{\| Q_0 - Q_1 \|}_{\overset{\wedge}{1}\ 1} \cdot \| \rho_0 - \rho_1 \|_{tr}$$

$$* v^\dagger (Q_0 - Q_1) v = v^\dagger Q_0 v - \underbrace{v^\dagger Q_1 v}_{\overset{\vee}{0}} \implies$$

$$\le v^\dagger Q_0 v \le \lambda_i(Q_0) \le 1$$

וכן עבור $v^\dagger (Q_1 - Q_0) v$.

מסקנה: לכל T עבור $pr[\text{ינצח } T] \le \frac{1}{2} + \frac{\| \rho_0 - \rho_1 \|_{tr}}{4}$

הוכחה: נסתכל על $\rho_0 - \rho_1$ (הרמיטי).

יהי $\{v_i\}$ בסיס של ו"ע של $\rho_0 - \rho_1$ v_i עם ע"ע μ_i

ונגדיר את המדידה: $\Pi_0 = \sum_{i:\mu_i \ge 0} |v_i\rangle\langle v_i|$

$\Pi_1 = \sum_{i:\mu_i < 0} |v_i\rangle\langle v_i|$

$$\Pi_0 + \Pi_1 = I, \quad \Pi_0, \Pi_1 \ge 0$$

$$pr(\text{מצליח } T) - pr(\text{טועה } T) = \frac{1}{2} \underbrace{Tr((\Pi_0 - \Pi_1)(\rho_0 - \rho_1))} = \frac{1}{2} \sum_{i=1} |\mu_i| = \frac{1}{2} Tr|\rho_0 - \rho_1| = \frac{1}{2} \|\rho_0 - \rho_1\|_{tr}$$

בבסיס v_i שלו

$$\begin{array}{l} \mu_i \ge 0 \\ \mu_i < 0 \end{array} \underbrace{\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & -1 \\ & & & & \ddots \\ & & & & & -1 \end{pmatrix}}_{\Pi_0 - \Pi_1} \underbrace{\begin{pmatrix} \mu_1 & & & \\ & \ddots & & \\ & & \mu_k & \\ & & & \mu_{k+1} \\ & & & & \ddots \end{pmatrix}}_{\rho_0 - \rho_1}$$

אפסים

The reduced dm operator

נגדיר עבור $v_1, v_2 \in \mathcal{H}_A$
$w_1, w_2 \in \mathcal{H}_B$

$$Tr_B\left(|v_1\rangle\langle v_2| \otimes |w_1\rangle\langle w_2|\right) = \underbrace{\langle w_1 | w_2\rangle}_{Tr(|w_2\rangle\langle w_1|)} \, |v_1\rangle\langle v_2|$$

ונרחיב לינארית

(10) מעבר הגבלה

מסקנה: נניח ρ מ"מ מצב על $\mathcal{H}_A \otimes \mathcal{H}_B$
(אפשר גם לא מכפלה entangled)

$$Tr_B (U\otimes I)^{*} \rho (U\otimes I)^{t} = U \, Tr_B \rho \, U^{t}$$

זה מבטא מדידה על A,

- מדידה $M\otimes I$ על $A\otimes B$
אז Tr_B

שקול ל Tr_B ואז מדידה M.

- B טרנספורמציה לוקלית על B
או מדידה " " "
לא משנה את מצב המערכת Tr_B

מסקנה: אם אליס B רק מבצעת רק פעולות לוקליות
מצב קוונטי של הסטטיסטיקה על A

מסקנה: B לא יכול להעביר מידע ל A
ע"י פעולות לוקליות בלבד. Non-Signaling

מצב שבו התוצאות יהיו תמיד Correlated

לדוגמא $EPR = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$

אם A,B מודדים בבסיס הסטנדרטי:

A: תוצאה 0 בהסת' $\frac{1}{2}$, 1 בהסת' $\frac{1}{2}$
ושום דבר לוקלי ש-B יעשה לא ישנה זאת.

מצב שבו התוצאות קשורות:
אם A קיבל 0 גם B קיבל 0
1 " " " 1.

הסבר: B ~~...~~ כדי ש-B ידע על התוצאה של A
הוא צריך לשלוח לו תוצאה-מצב
אי אפשר להעביר אינפורמציה יותר מהר ממהירות האור.

ולכן המערכת היא non-signalling את זה מאפשר.

רק לוקליות מפריעה!

non Signaling	✓	
local	?	לא שניהם ביחד
realism	?	

Safe storage principle – במקום למצב מסוכן, אפשר להוציא אותה למחוץ אותה מהמצב מהמערכת, וזה שקר חשוב.

שאלה מהסמינר: באיזה בסיס יש יתרונות, ואז כן רק גישה שקילה
ב עם ניתן יתרונות לשמור את מצבים היום "הכל"
כאשר יש מצב משהו המערכת.

תשובה מקומית non-signalling

פעולה מקומית של A : עושה, לא משפיעה על סטטיסטיקה של B

[אין מידע המועבר של A ל-B, ידוע הקורלציה. B התוצאות של B]

עבור -
- תשובה לכן הוא מקומית
- תשובה קוונטית " "

כאשר שניהם A, B קיוביטים

$\frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$

התפלגות של תשובות ... הקורלציה.

		שאלה B: 0		שאלה B: 1	
שאלה A	תשובה A \ תשובה B	0	1	0	1
0	0	1/2	0	1/2	0
0	1	0	1/2	0	1/2
1	0	1/2	0	0	1/2
1	1	0	1/2	1/2	0

PR Box

non signalling — תנאי n.s., A של ... לא משפיעה על ההתפלגות של B ולהפך.

שאלה 5

(classical) realism

השאלה היא מה בדיוק EPR מראים? או האם יש קו של התכונות האלו.
אולם המציאות לא מתנהגת — מקומית המציאות לא מתנהגת.
אלא יש קור' התנהגות מקומית קורלציה קוונטית.

דוגמה

דוגמה $\frac{1}{2}$ AB מציגים 0,0
" $\frac{1}{2}$ " " 1,1

אלא תלוי תוצאת A ב תוצאת B.

האם אפשר להסביר את התוצאה ע"י Hidden classical RV?

משל: יכול להתנהג מקומית כמו ... לכל ערך
ש A ו B מציגים

אלא יש רנדומיות a_0 - התוצאה ש A מציג כשהוא מקבל 0
a_1 " " " " 1
b_0 " " B " 0
b_1 " " " " 1

$$\Pr(S \wedge T = a_S \oplus b_T) \le \frac{3}{4}$$ אבל

עם משאב קוונטי $\Pr(S \wedge T = a_S \oplus b_T) \approx 0.86$
אפשר לעבור את 3/4, ומשמעותו רבה!

ובקופסה PR $\Pr(S \wedge T = a_S \oplus b_T) = 1$

א"ש Bell נותן שלא יכול להיות יחד:

- non-signaling
- Classical realisim
- ולאפשר להגדיר מצבים לכולם בעולם קלסי:

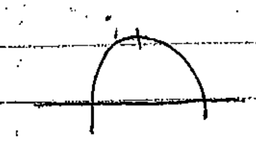
יש לנו מידה [illegible]^2 ....

קמירות ואנטרופיה

עבור $1 \geq p \geq 0$ נגדיר $H(p) = p \cdot \lg\frac{1}{p} + (1-p)\lg\frac{1}{1-p}$

<u>תכונות:</u> – $H(p) \geq 0$ (מיידי)

– פונק' קמורה (גזירה שנייה)



– מקסימום ב $\frac{1}{2}$, $H(\frac{1}{2})=1$

<u>באופן כללי:</u> אם A משתנה על $\{1,\dots,k\}$

$$H(A) = \sum_{x=1}^{k} Pr(A=x)\ \lg\frac{1}{Pr(A=x)}$$

סימן האנטרופיה הבינארית הוא עבור המקרה הפרטי של התפלגות על 2 ערכים.

<u>תכונות:</u> – לכל התפלגות p $H(p) \geq 0$ (מיידי)

– אם p מוגדרת על k ערכים $H(p) \leq \lg_2 k$

והמקסימום מתקבל כש p אחידה על k הערכים.

<u>קמירות:</u>

<u>משפט:</u> אם p,q התפלגויות $1 \geq \lambda \geq 0$

אז $H(\lambda p + (1-\lambda) q) \geq \lambda H(p) + (1-\lambda) H(q)$

<u>הוכחה:</u> נגדיר $f(\lambda) = H(\lambda p + (1-\lambda) q)$

צריך להראות $f(\lambda) = \lambda f(1) + (1-\lambda) f(0)$

לכן מספיק להראות ש f קמורה כלומר מספיק $f'' \leq 0$

f קמורה ממש

14

שלב:

$$f(\lambda) = \sum_x (\lambda p_x + (1-\lambda) q_x) \lg \frac{1}{\lambda p_x + (1-\lambda) q_x}$$

$$f'(\lambda) = \sum_x \Big[(p_x - q_x) \cdot \lg \frac{1}{\lambda p_x + (1-\lambda) q_x} + \underbrace{\cancel{(\lambda p_x + (1-\lambda) q_x)} \cdot \frac{(-1)}{c} \cdot \frac{1}{\cancel{\lambda p_x + (1-\lambda) q_x}} (p_x - q_x)}_{\text{לא תלוי ב-} \lambda .}$$

כי $c > 0$ קבוע

$$f''(\lambda) = \sum_x (p_x - q_x) \cdot (-1) \cdot \underset{\geq 0}{\frac{1}{c}} \cdot \underset{\geq 0}{\frac{1}{\lambda p_x + (1-\lambda) q_x}} (p_x - q_x)$$

$(p_x - q_x)^2 \geq 0$, $-1 < 0$, ולכן ≤ 0

טענה: אם A,B ב"ת אז: $H(A,B) = H(A) + H(B)$

$$\sum_{a,b} \Pr((A,B)=(a,b)) \cdot \lg \frac{1}{\Pr((A,B)=(a,b))}$$

$$= \sum_{a,b} p_a \cdot p_b \cdot \lg \frac{1}{p_a \cdot p_b}$$

$$= \underbrace{\sum_{a,b} p_a\, p_b \lg \frac{1}{p_a}}_{\underbrace{\sum_a \left(\sum_b p_b\right) \cdot p_a \cdot \lg \frac{1}{p_a}}_{H(A)}} + \underbrace{\sum_{a,b} p_a p_b \lg \frac{1}{p_b}}_{H(B)}$$

חוק כללי:

טענה:

$$H(A,B) = H(A) + \underbrace{H(B|A)}_{= \mathbb{E}_a\, H(B|A=a)}$$

הוכחה

$$H(A,B) = \sum_{a,b} p_{a,b} \lg \frac{1}{p_{a,b}}$$

$$= \sum_{a,b} p_a \cdot p_{b|a} \cdot \lg \left(\frac{1}{p_a} \cdot \frac{1}{p_{b|a}} \right)$$

$$= \underbrace{\sum_a \left(\sum_b p_{b|a} \right) \cdot p_a \cdot \lg \frac{1}{p_a}}_{H(A)} + \underbrace{\sum_a p_a \cdot \underbrace{\sum_b p_{b|a} \lg \frac{1}{p_{b|a}}}_{H(B|A=a)}}_{H(B|A)}$$

מסקנות: 1. $H(B|A) \geq 0$ (כלומר, צריך להוכיח)

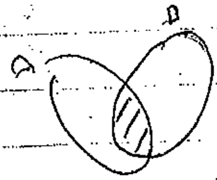
2. $H(A) \leq H(A,B) \quad \forall B$

כי: $H(B) = H\left(\sum_a p_a \cdot (B|A=a)\right)$

$$\underset{\text{ג'נסן}}{\geq} \sum_a p_a \, H(B|A=a) = H(B|A)$$

4. $H(A,B) = H(A) + H(B|A) \leq H(A) + H(B)$

מידע הדדי: $I(A:B) = H(A) + H(B) - H(A,B)$



האינפורמציה ההדדית של A, B.

טענה: $\forall_{A,B} \quad I(A;B) \geq 0$

דוגמאות: 1. אם A, B ב"ת: $I(A:B) = H(A) + H(B) - (H(A)+H(B)) = 0$

2. אם $(A:B)$ מוגדרים ע"י (a,a)

אז $I(A:B) = H(A) + H(A) - \underset{H(A)}{H(A,B)} = H(A)$

כי B לא מוסיף מידע על A.

$$H(p) = \underbrace{\sum_x p_x \lg \frac{1}{p_x}}_{\text{כמות "ההפתעה" מ-}x\text{ כש-}X\text{ הצפויה}}$$

$$\underbrace{\sum_x p_x \lg \frac{1}{q_x}}_{\text{כמות ההפתעה כשחושבים (בטעות) שזה } q \text{ ולא } p}$$

[illegible] חושבים [illegible] q.

ההפרש: $D(P\|Q) = \sum_x p_x \left(\lg \frac{1}{q_x} - \lg \frac{1}{p_x}\right) = \sum_x p_x \cdot \lg \frac{p_x}{q_x}$

משפט: לכל P, Q $\quad D(P\|Q) \geq 0$

הוכחה: $D(P\|Q) = \sum_x p_x \cdot -\lg\left(\frac{q_x}{p_x}\right) \leq -\log\left(\sum_x p_x \cdot \frac{q_x}{p_x}\right) = \lg\left(\sum_x q_x\right) = \lg(1) = 0$

טענה: Alice ו Bob מחזיקים [illegible] מהמצב
המשותף (A,B). Alice מקבלת a מ' B
מקבל b

Alice ו Bob צריכים פרוטוקול תקשורת (קלאסי)
כך שבסוף התהליך שבסופו גם Alice
וגם Bob יחזיקו את a.

כמה ביטים של תקשורת עוברים בפרוטוקול?

פתרון: לפחות $H(A|B)$

~~[illegible]~~

המידע המשותף הדרוש להבנה של Alice ו Bob הוא $I(A:B)$
בסוף " " " " " הוא $H(A)$

אם מוסרים C שביטים, יכול להגדיל את המידע המשותף
לכל היותר ב $H(C)$, כי:

$$I(XC:Y) = H(XC) + H(Y) - H(XCY)$$
$$= H(X) + H(C|X) + H(Y) - (H(XY) + H(C|XY))$$
$$= I(X:Y) + H(C|X) - H(C|XY)$$
$$\le I(X:Y) + H(C|X)$$
$$\le I(X:Y) + H(C)$$

לכן, אם עבור המסרים $C_1 \dots C_m$, $l(c_i) = l_i$

$$H(A) \le I(A:B) + H(C_1) + H(C_2) \dots + H(C_m)$$
$$\le I(A:B) + l_1 + \dots + l_m$$

לכן $l = l_1 + \dots + l_m \ge H(A) - I(A:B)$
$$= H(AB) - H(B)$$
$$= H(A|B)$$

Quantum information theory

עבור מצב קוונטי ρ_A

$\rho \geq 0$, $Tr(\rho)=1$

ידוע $\rho = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$ עבור בסיס הנ"ל

לכן $\rho = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$ בבסיס הזה

נגדיר $H(\rho) = H(\lambda_1,...,\lambda_N)$ (הגדרה שקולה: $V(\rho)$ Von Neumann entropy)

תכונות:

1. לכל ρ $H(\rho) \geq 0$ ברור.

2. אם ρ מוגדרת על מרחב הילברט ממימד N
אז $H(\rho) \leq \log_2(N)$ ברור.
מקסימום ב completely mixed state $\frac{1}{N} I$.

3. עבור pure state $\rho = |\psi\rangle\langle\psi|$ $\Leftrightarrow$ $H(\rho)=0$

נראה גם הקשר ש H נכונה, אבל צריך לעבוד יותר קשה.

ישנו $H(A,B) \leq H(A) + H(B)$

כלומר אם $\rho_{A,B}$ נתון $\rho_A = Tr_B(\rho_{AB})$, $\rho_B = Tr_A(\rho_{AB})$

אז $H(\rho_{AB}) \leq H(\rho_A) + H(\rho_B)$

ראינו: $S(\rho) = -Tr(\rho \lg \rho)$

נגדיר $D(\rho \| \sigma) = Tr(\rho(\lg \rho - \lg \sigma))$

משפט (Klein): לכל ρ, σ, $D(\rho \| \sigma) \geq 0$

הוכחה:

$\sigma = \sum q_i w_i w_i^*$

$\rho = \sum p_i v_i v_i^*$

נניח v_i הם ו"ע של ρ

w_i ... של σ

$$D(\rho \| \sigma) = Tr\Big(\sum_i p_i \lg p_i \, v_i v_i^* - \sum_{i,j} p_i \log q_j \, v_i v_i^* w_j w_j^* \Big)$$

$$= \sum_i p_i \log p_i - \sum_{i,j} p_i \log q_j |v_i^* w_j|^2$$

$$= \sum_i p_i \Big[\log p_i - \sum_j P_{ij} \log q_j \Big]$$

נסמן $P_{ij} = |v_i^* w_j|^2$, ו- $P = (P_{ij})$ doubly stochastic

$$\sum_i P_{ij} = \sum_i |v_i^* w_j|^2 = \|w_j\| = 1$$
$$\sum_j P_{ij} = \sum_j |v_i^* w_j|^2 = \|v_i\| = 1$$

$$\geq \sum_i p_i \Big[\log p_i - \log\Big(\sum_j P_{ij} q_j \Big) \Big]$$

$-\log$ קמורה

נסמן $r_i = \sum_j P_{ij} q_j$ אז $r_i \geq 0$

$$\sum_i r_i = \sum_{i,j} P_{ij} q_j = \sum_j q_j \underbrace{\sum_i P_{ij}}_{1} = \sum_j q_j = 1$$

ולכן r פונק' הסתברות

$= D(p \| r) \geq 0$ ∎

(הסתברותי הקודם)

משפט: לכל ρ_{AB} : $H(\rho_{AB}) \le H(\rho_A) + H(\rho_B)$

הוכחה: נגדיר $\sigma_{AB} = \rho_A \otimes \rho_B$

אז

$$H(\rho_{AB}) = -Tr(\rho \lg \rho) \underset{\text{שוויון Klein}}{\le} -Tr(\rho \lg \sigma)$$

$$= Tr\left(\rho_{AB} \left(\log \underbrace{(\rho_A \otimes I)(I \otimes \rho_B)}_{\text{מתחלפים}}\right)\right)$$

$$= -Tr_{A,B}\left(\rho_{AB} \underset{(\log(\rho_A) \otimes I)}{\log(\rho_A \otimes I)}\right) - Tr\left(\rho_{AB} \log(I \otimes \rho_B)\right)$$

$$= -Tr_A(\rho_A \log \rho_A) - Tr(\rho_B \log \rho_B)$$

$$= H(A) + H(B)$$

מסקנה $I(A:B) = H(\rho_{AB}) - H(\rho_A) - H(\rho_B)$, $I(A:B) \ge 0$

משפט: H קעורה

$$H\left(\sum \lambda_i \rho_i\right) \ge \sum \lambda_i H(\rho_i)$$

הוכחה: נניח $\rho_A = \sum \lambda_i \rho_i$

נבנה $\rho_{AB} = \sum_i \lambda_i \underbrace{\rho_i}_{A} \otimes \underbrace{|i\rangle\langle i|}_{B}$

$$S(A) = S(\rho)$$

$$S(B) = S\left(\sum \lambda_i |i\rangle\langle i| \underbrace{Tr(\rho_i)}_{1}\right) = H(\lambda_1 \ldots \lambda_N) = H(\lambda)$$

$$S(A,B) = H(\lambda) + \sum_i \lambda_i S(\rho_i)$$

$\Leftarrow$ $S(A,B) \le S(A) + S(B)$

(הסבר בשאלה קודמת)

$$\boxed{\sum \lambda_i S(\rho_i) \le S(\rho)}$$

$\square$

$$S\left(\sum_{i=1}^{k} \lambda_i \rho_i \otimes |i\rangle\langle i|\right) = \begin{array}{c} \\ |1\rangle \\ \\ \vdots \\ |k\rangle \end{array} \begin{pmatrix} \rho_1 & & & \\ & \rho_2 & & \\ & & \ddots & \\ & & & \rho_k \end{pmatrix}$$

[illegible]

$$= \sum_{i=1}^{k} \sum_{j=1}^{N} \lambda_i p_{ij} \lg \frac{1}{\lambda_i p_{ij}}$$

$$= \sum_{i=1}^{k} \sum_{j=1}^{N} \lambda_i p_{ij} \lg \frac{1}{\lambda_i} + \underbrace{\sum_i \lambda_i \sum_j p_{ij} \lg \frac{1}{p_{ij}}}$$

$$H(\lambda) \qquad + \quad \sum_i \lambda_i S_i(\rho_i)$$

משפט Holevo :

נניח A מוציא $x \in X$, X מספר לו p_x.

נניח B מקבל קבוצה קוונטית ב-x, $\rho(x) \in H$,

אז לכל מדידה ש B יבצע, והמידע הקלאסי שיקבל

$$I(A:B) \le \underbrace{S\left(\sum_x p_x \rho_x\right)}_{\text{Shannon} \ \ldots \ \text{קידוד מיטבי}} - \sum_x p_x S(\rho_x)$$

מסקנה: אם ρ_x הוא pure state

אז:

$$I(A:B) \le S\left(\sum_x p_x \rho_x\right)$$

מסקנה: אם $\rho \in H_K$, מרחב הילברט ממימד $K = 2^k$

$$I(A:B) \le k \le \lg(K).$$

במילים: אי אפשר להעביר יותר מ k ביטים של אינפורמציה ע"י k ביטים קוונטים.

בקוונטים זה שקר לא נכון ש $H(A) \le H(A,B)$

דוגמא: $\rho_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}|$ כאשר $\Psi_{AB} = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$

אז: $H(\rho_{AB}) = 0$

אבל: $\rho_B = \rho_A = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ ולכן $H(A) = H(B) = 1$

RAC

A מקבל $x \in_R \{0,1\}^m$

מחפשים קוד $p(x) \in H_k$ עבור k כמה שיותר קטן.

לכל שלב חד צדדי

יש הגבלה: Θ_i, שמתפקדת $\leq p$ מתקבל על X_i

עכשיו נראה שאי אפשר לקבל יותר מזה של ... על $X_1, \dots, X_n$
כי $I(A:B) \leq \lg(k) = k$

אבל ניתן לקבל ... קידוד ... רק ...
... ...
... ... של ההגבלה.

נראה שגם זה מחוכם!

באופן כללי קוד כזה, $k \geq (1-H(p))\cdot m$

הוכחה נסמן $X_1 \dots X_n$ ... ...
C ... ...

טענה $I(X_1 X_2 : C) = I(X_1 : C) + I(X_2 : X_1 C)$
כאשר X_1, X_2 ב"ת

הוכחה $H(X_1X_2) + \cancel{H(C)} - H(X_1 \cancel{X_2 X_1}) \overset{?}{=} H(X_1) + \cancel{H(C)} - H(\cancel{X_1}C) + H(X_2) + H(\cancel{X_1}C) - H(X_1X_2C)$
$H(X_1X_2) = H(X_1) + H(X_2)$

תזכורת: כאשר $X_1 \dots X_n$ ב"ת:

$$I(X_1 \dots X_n ; C) = I(X_1;C) + I(X_2 ; X_1 C) + \dots + I(X_n ; X_1 \dots X_{n-1} C)$$

הוכחה: אם C נתון ההסתברות ש- X_1 שונה מ- C היא p

אז $I(X_1 ; C) \ge (1-H(p))C$

ולכן:

$$I(X_1 \dots X_n C) = \sum_{i=1}^{n} I(X_i ; C X_1 \dots X_{i-1})$$

$$\ge \sum_{i=1}^{n} I(X_i ; C)$$

$$\boxed{\ge n(1-H(p))}$$

תרגילי חזרה

① יהיו משתנים ב"מ X,Y כך ש- $pr(X=Y)=p$, X,Y מפולגים אחיד, X בינאריים

אז $I(X;Y) \ge 1-H(p)$

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

② יהיו X,Y קבועים,

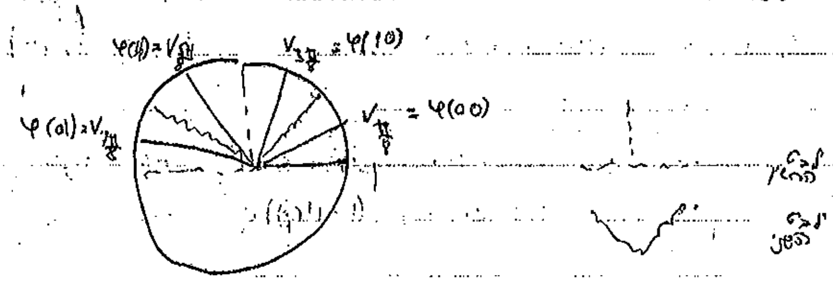
Y' קבוע, תלוי רק ב- Y

אז $I(X;Y') \le I(X;Y)$,

$\rho = \cos^2\frac{\pi}{8} \approx 0.86$

$2 \longrightarrow 1$

כלומר יש RAC



מסקנה: יש RAC ל $2 \xrightarrow{0.86} 1$

2. לסיכום $R''(EQ)$ [illegible] $R''(EQ) = \Theta(\sqrt{n})$

$Q''(EQ)$

להראות $Q''(EQ) = O(\log n)$

3. הוכחה של טענה (10) מקודם.