תרגיל 7 — coin flipping

1. A בוחר $a \in_R \{0,1\}$
מכינה $\Psi_a = \frac{1}{\sqrt{2}}\left[|aa\rangle + |22\rangle\right]$
שולחת qubit הראשון ל B.

2. B בוחר $b \in_R \{0,1\}$ שולח ל A

3. A שולחת a ל B
ואת ה qubit השני.
התוצאה היא: $a \oplus b$.

4. B מודד את Ψ_{aa} ו $\Psi_a^{\perp}$ ובודק אם קיבל Ψ_a
התוצאה היא $a \oplus b$.

1. אם שניהם הוגנים $Pr[\text{זוכה } A] = \frac{1}{2}$.

2. אם A הוגנת ו B רמאי.

$$\rho_0 = \begin{bmatrix} \frac{1}{2} & & \\ & 0 & \\ & & \frac{1}{2} \end{bmatrix}, \quad \rho_1 = \begin{bmatrix} 0 & & \\ & \frac{1}{2} & \\ & & \frac{1}{2} \end{bmatrix}$$

$$\rho_0 - \rho_1 = \begin{bmatrix} \frac{1}{2} & & \\ & -\frac{1}{2} & \\ & & 0 \end{bmatrix} \qquad \|\rho_0 - \rho_1\|_{tr} = 1$$

$$Pr[\text{זוכה } B] \le \frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_{tr}}{4} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$$

המסקנה: רמאי B ממדד לפי הבסיס ו"ע של $\rho_0 - \rho_1$
כלומר הבסיס $|0\rangle, |1\rangle, |2\rangle$.

10 (1) נ"ל

ה. אם B מגן, A מנצח ...

פרוטוקול מס' 1:

- A בוחרת a שולחת Ψ_a

- אם קיבלה b ורוצה תוצאה ~~...~~ – מודדת a, מחזירה qutrit 0

אם רוצה תוצאה הפוכה – שולחת 1-a, ו-1 מחזירה qutrit ב.

$$Pr[\text{A מנצח}] = \underset{\substack{\downarrow\\ \text{כי b שווה לרצוי}}}{\frac{1}{2}} + \underset{\substack{\downarrow\\ \text{אם b שונה מהרצוי}}}{\frac{1}{2}} \cdot \underbrace{|<\Psi_a, \Psi_{1-a}>|^2}_{(\frac{1}{2})^2 = \frac{1}{4}} = \frac{5}{8}$$

פרוטוקול מס' 2:

- A מכינה $\Psi = \frac{\Psi_0+\Psi_1}{\|\Psi_0+\Psi_1\|}$ $\qquad \Psi = \frac{\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle + \frac{2}{\sqrt{2}}|22\rangle}{\sqrt{3}}$

שולחת a ו-B, qutrit ראשון $= \frac{|00\rangle}{\sqrt{6}} + \frac{|11\rangle}{\sqrt{6}} + \frac{2}{\sqrt{6}}|22\rangle$

- אם רוצה לשנות את a שולחת 1-a qutrit שני

$$Pr[\text{A מנצח}] = \frac{1}{2}|<\Psi|\Psi_0>|^2 + \frac{1}{2}|<\Psi|\Psi_1>|^2 = \cancel{2}\cdot\frac{1}{\cancel{2}}\left[\frac{9}{12}\right] = \frac{3}{4}$$

$$<\ > = \frac{2}{\sqrt{6}}\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{6}}\frac{1}{\sqrt{2}} = \frac{3}{\sqrt{12}}$$

□.

טענה: לכל A רמאי, $pr(\text{זוכה } A) \le \frac{3}{4}$

הוכחה: נסמן רמאי כללי ל A:

- לפני ה 3>, $\Psi \in H \otimes \mathbb{C}^3 \otimes \mathbb{C}^3 = H \otimes H_A \otimes H_B$.

ושולחת את ה qutrit ב H_B ל Bob

- בשלב ב, שולחת a כמו שהיא רוצה

(a=b אם היא רוצה לזכות 0

a≠b .. .. 1)

- מפעילה U_a על $H \otimes H_A$ $\quad \tilde{\Psi}_a = (U_a \otimes I)|\Psi\rangle$

ושולחת את ה qutrit ב H_A ל B

נניח b=0, ו A רוצה לקבל תוצאה 0 (המקרים האחרים דומים)

$$pr\left[\begin{matrix} B \text{ תוצאה} \\ 0 \text{ היא} \\ b=0 \text{ אם} \end{matrix}\right] = \langle \Psi_0 | Tr_H \left(|\tilde{\Psi}_0\rangle\langle\tilde{\Psi}_0|\right) | \Psi_0 \rangle$$

$$pr\left[\begin{matrix} B \text{ תוצאה} \\ 0 \text{ היא} \end{matrix}\right] = \underset{\downarrow\, b=0}{\frac{1}{2}} \langle \Psi_0 | \underbrace{Tr_H |\tilde{\Psi}_0\rangle\langle\tilde{\Psi}_0|}_{\sigma_0 \text{ נסמן}} |\Psi_0\rangle + \underset{\downarrow\, b=1}{\frac{1}{2}} \langle \Psi_1 | \underbrace{Tr_H |\tilde{\Psi}_1\rangle\langle\tilde{\Psi}_1|}_{\sigma_1 \text{ נסמן}} |\Psi_1\rangle$$

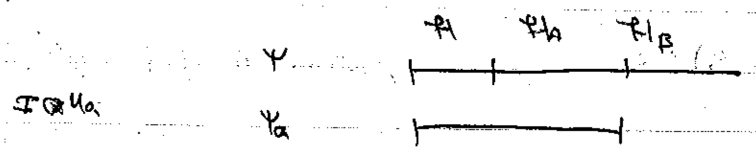
$$= \frac{1}{2} F(\underbrace{|\Psi_0\rangle\langle\Psi_0|}_{\rho_0 \text{ נסמן}}, \sigma_0) + \frac{1}{2} F(\underbrace{|\Psi_1\rangle\langle\Psi_1|}_{\rho_1 \text{ נסמן}}, \sigma_1)$$

$$\le \frac{1}{2} F(Tr_{H_A} |\Psi_0\rangle\langle\Psi_0|, Tr_{H_A} \sigma_0) + \frac{1}{2} F(Tr_{H_A} \rho_1, Tr_{H_A} \sigma_1)$$

(15)

המשך 14 1

[illegible]



לא משנה על החלק A B

לכן $\quad \mathrm{Tr}_{\mathcal{H}_A}\,\sigma_0 = \mathrm{Tr}_{\mathcal{H}_A}\,\sigma_1$

נסמן $\quad \sigma =$

$$= \frac{1}{2}\left[F(\rho_0, \sigma) + F(\rho_1, \sigma)\right]$$

$$\le \frac{1}{2}\left[1 + \sqrt{F(\rho_0, \rho_1)}\right]$$

$$\sqrt{F(\rho_0,\rho_1)} = \|\sqrt{\rho_0}\sqrt{\rho_1}\|_{tr} = \left\|\frac{1}{2}\begin{pmatrix}1 & \\ & 0\end{pmatrix}\begin{pmatrix}0 & \\ & 1\end{pmatrix}\right\|_{tr} = \frac{1}{2}\left\|\underbrace{\begin{pmatrix}0 & \\ & 0\end{pmatrix}}\right\|_{tr} = \frac{1}{2}$$

לכן $\quad \Pr[O \text{ עונה } B] \le \frac{1}{2}\left[1 + \frac{1}{2}\right] = \frac{3}{4} \quad \nabla$

Q4 [illegible] 2 [illegible]

Cleve, van Dam, Nielsen, Tapp
Quantum ent. & the comm. comp. of the IP function.

תשובה לגבי QCC

משפט: $Q_0(IP) \geq \frac{n}{2}$

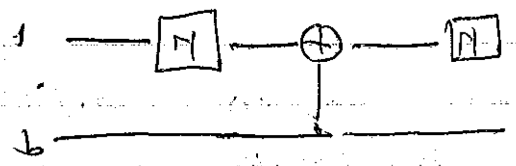
הוכחה: נניח שיש פרוטוקול קוונטי חסר שגיאה שמחשב IP ב-k קיו' תקשורת.

נראה איך A יכולה לתקשר $x \in \{0,1\}^n$ ל-B ב-2k ביטים

ולפי חסם הולבו נדרש $2k \geq n$, $k \geq \frac{n}{2}$

הערה: למעשה החסם יכול להשתפר
$Q_0(IP) \geq n$
ולא נוכיח זה כאן.

ש"א – דיון: הפאזה חוזרת לפונק'



$b=0$ $\quad HH|1\rangle \otimes |0\rangle = |1,0\rangle$

$b=1$

$$H\left(\tfrac{1}{\sqrt2}(|1\rangle - |0\rangle)\right)\otimes|1\rangle = HH(-|1\rangle)\otimes|1\rangle = -|1,1\rangle$$

ולכן $\quad |1,b\rangle \to (-1)^b\,|1,b\rangle$

שאלה מס' 2 : ניקוי זבל

נניח A מחזיקה $x\in\{0,1\}^n$

$\qquad\quad B \quad y\in\{0,1\}^n$

ורוצים לחשב $IP(x,y)$

$$|x,\bar 0\rangle\otimes|y,\bar 0\rangle\otimes\underbrace{|0\rangle}_{\text{תוצאה}} \to |x,\underbrace{g_A(x,y)}_{\text{זבל}}\rangle\otimes|y,g_B(x,y)\rangle\otimes|IP(x,y)\rangle$$

אם נעניין את IP הבינה (או נעבור לספר)

~~?~~ ונרצה את התוצאה רק

נקבל את הבעיה של זבל ונוסר די' התקשורת הנכונו.

הערכה: נניח A שולחת k_A ביט

ו B " k_B ביט

ואז הפכנו: A שולחת k_B, ו B שולחת k_A ביטים.

<u>הכיוון</u>: (נראה איך A יכולה להעביר את $x\in\{0,1\}^n$ ל-B):

A מחזיקה $x\in\{0,1\}^n$

B מכין $\bar{0}$, ψ

- B יוצר מצב $\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}|z\rangle$

- הם יוצרים על אותו ה-EPR, תוך הבנת השיטה למעבר ונקודה ויקטור

$$|x\rangle\otimes\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle$$

- B יפעיל $H^{\otimes n}$ על החלק שלו

$$\sum(-1)^{x\cdot z}|z\rangle\to|x\rangle$$

והנה B מקבל את $|x\rangle$.

<u>מס' ביטי התקשורת</u>: $2k$ (k לכל הכיוון הראשון, ו-k לשני).

לפי Holevo: $2k\ge n$, ולכן $k\ge n$.

מסקנה: אפשר לקבל מ-Holevo המקורי when A משדרת את x ל-B

אין מספר ביטי התקשורת שמעבירים בין A ל-B הוא לפחות $|x|$.

ולכן יוצא $\boxed{k\ge n}$ $\boxed{Q_0(IP)\ge n}$

עוד הערה: אפשר להוכיח רק עם Holevo

אם A, B משתמשים ב-pre-shared entangl.

אז A ישלח $x \in \{0,1\}^n$ ל-B

אז צריך רק (מ-A ל-B) קיוביטים $\le \frac{n}{2}$

[זכר חלק, ל-super dense coding]

ולכן $\boxed{Q^*[IP] \ge \frac{n}{2}}$

סיבוכיות תקשורת כש-A ו-B חולקים pre-shared ent.

הכללה (ללא הוכחה): ניתן להראות:

$$Q_\varepsilon(IP) \ge (1-O(\varepsilon))\,n$$

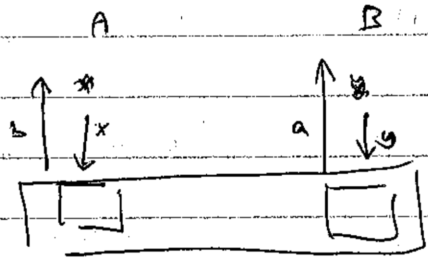
$$Q^*_\varepsilon(IP) \ge \frac{1}{2}(1-O(\varepsilon))\,n \qquad \text{(ע"י שימוש ב-Holevo)}$$

Wim van dam

הראנו שאם PR boxes (יותר חזק מ pre-shared ent.
אבל עדיין non-signalling
((אבל nonlocal)

אפשר לחשב $IP(\bar{x},\bar{y})$ עם ביט אחד תקשורת.

תזכורת: PR box



ומקיים $x\cdot y = a\oplus b$

הוכחה: A מקבלת $x_1 \dots x_n \in \{0,1\}$
B " $y_1 \dots y_n \in \{0,1\}$

רוצים לחשב $(x_1\cdot y_1)\oplus \dots \oplus (x_n \cdot y_n)$

לכל i, משתמשים ב-PR-box ה-i
A נותנת x_i מקבלת a_i
B נותן y_i " b_i

$$x_i \cdot y_i = a_i \oplus b_i$$

$$IP(\bar{x},\bar{y}) = (a_1\oplus b_1)\oplus \dots \oplus (a_n \oplus b_n)$$
$$= \underbrace{(a_1\oplus \dots \oplus a_n)}_{\text{ביט אחד תקשורת}} \oplus (b_1 \oplus \dots \oplus b_n)$$

מ A ל B

טענה: לכל $f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

אפשר לחשב ע"י $IP: \{0,1\}^N \times \{0,1\}^N \to \{0,1\}$, $N=2^n$

כלומר יש
$$\Phi_A : \{0,1\}^n \to \{0,1\}^N$$
$$\Phi_B : \{0,1\}^n \to \{0,1\}^N$$

כך ש:
$$f(\bar{x},\bar{y}) = IP(\Phi_A(\bar{x}), \Phi_B(\bar{y}))$$

הוכחה: נכתוב את f כסכום של מונומים (פולינום) מעל $\mathbb{F}_2$

$$\prod_{i\in S} \prod_{j\in T} x_i y_j$$

$$f(x_1 \dots x_n; y_1 \dots y_n) = \sum_{S\subseteq[n]} \underbrace{\prod_{i\in S} x_i}_{(\Phi_A)_S} \cdot \underbrace{(\Phi_B)_S}_{\text{תלוי רק ב-}y} \pmod 2$$

תלוי רק ב-x

פונק' מסובכת של $y_1 \dots y_n$

□.

מסקנה: עם 2^n PR-boxes
אפשר לחשב כל $f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$
אם כי לא ברור שזה מעשי!

□.