RAC

A מקבל $x \in_R \{0,1\}^m$

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

רק שלכל $1 \le i \le n$

יש מדידה Θ_i, שבהסתברות $\geq p$ מחזירה את x_i.

קודם אמרנו שאי אפשר לזהות שמתאים ניחוש את כל $x_1, \dots, x_n$

כי $I(A:B) \le \lg(k) = k$.

אבל יתכן שנוכל לעשות קידוד שבו אפשר לחלץ רק ביט אחד, אבל כל ביט לחוד, כי אחרי שמודדים לא נשאר בגלל מדידה יתכן שהרסנו את המצב.

נראה שזה לא מתקיים!

טענה: לכל קוד כזה, $k \geq (1-H(p)) \cdot m$

הוכחה: נסמן $X_1 \dots X_n$ מידע קלט

C המצב הקוונטי של הקידוד

למה: $I(X_1X_2:C) = I(X_1:C) + I(X_2:X_1C)$

כאשר X_1, X_2 ב"ת

הוכחה: $H(X_1X_2) + \cancel{H(C)} - H(X_1X_2C) \overset{?}{=} H(X_1) + \cancel{H(C)} - \cancel{H(X_1C)} + H(X_2) + \cancel{H(X_1C)} - H(X_1X_2C)$

$H(X_1X_2) = H(X_1) + H(X_2)$

עבור לעמ' 12 (1)

מסקנה כאשר $X_1 \ldots X_n$ ק"מ:

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

טענה אם לכל i ניתן לשחזר את X_i בהסתברות $\geq p$

אז $I(X_i : C) \geq (1-H(p))$.

הוכחה

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

$$\geq \sum_{i=1}^{n} I(X_i : C)$$

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

הוכחת הטענה

① לכל משתנים מקריים X,Y אם $\Pr(X=Y)=p$, X,Y בוליאניים, X אחיד,

אז $I(X:Y) \geq 1-H(p)$.

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] I

② אם X,Y מקריים,

Y' מקרי, תלוי רק ב-Y

אז $I(X:Y') \leq I(X:Y)$.

- ECC קודים:

- תרגיל $R_{\frac13}(EQ) = O(\log n)$

A: $x \in \{0,1\}^n$, $\bar{x} = ECC(x)$, $i \in_R [\bar{n}]$ $\xrightarrow{i,\ \bar{x}_i}$ B: $y \in \{0,1\}^n$, $\bar{y} = ECC(y)$, $\bar{x}_i = \bar{y}_i \Leftrightarrow 1$

$[\bar{n}, n, \underbrace{\tfrac12 - \varepsilon}_{\frac{1}{k}}]$

- δ $\varepsilon\bar{n}$ k-local decoding עבור

יש אלגו' פותר D

קריאות לאורך המילה המורחבת

כך ש $\forall_{x \in \{0,1\}^n,\ \bar{x} = ECC(x)}\ \forall_{1 \le i \le n}\ \forall_{w \in \{0,1\}^{\bar{n}},\ d(\bar{x}, w) \le \varepsilon\bar{n}}\ \Pr_{D}\left[D^{w}(i) = x_i\right] \ge \frac{2}{3}$

1. D שואל לכל היותר k שאילתות לביטים של $ECC(x)$.

- תרגיל $HAD: \{0,1\}^n \to \{0,1\}^{(2^n)}$

$(HAD(x))_y = x \cdot y = \sum x_i y_i \pmod 2$, $y \in \{0,1\}^n$

אלגו' פתרון: $D(i) = w_y \oplus w_{y \oplus e_i}$

בחר $y \in_R \{0,1\}^n$, $e_i = (0 \ldots 1 \ldots 0)$ (מקום i)

אם שני ערכי w נכונים (שווים לערכי $\bar{x}$)

אז $D(i) = y \cdot x \oplus x \cdot (y \oplus e_i) = x \cdot e_i = x_i$

וגם $\Pr[\text{לא נכונים}] \le 2\varepsilon$

שאלה 12 (3) 2-local, ערוץ קידוד $n \ge 2^n$

קודים לינאריים : כל קוד לינארי שהוא 2-local
דורש אורך קוד $2^{\Omega(n)}$.

הוכחה קודם לקודים לינאריים, והוכחה מסובכת יותר (וגם יותר קוונטי) לקודים כלליים.

<u>רעיון ההוכחה</u> : נהפוך 2 שאילתות קלאסיות
לשאילתה קוונטית אחת
ואז קוד 2-local הופך להיות RAC !
משחזרים ב i לרצוננו !
ונשתמש בחסם של RAC.

<u>Trevisan Katz</u> : אם יש 2-local decoding עם הצלחה $\Omega(1)$
אז יש אלג׳-ם decoding בצורה הבאה

לכל $i \in [n]$
יש זיווג חוקי $M_i \subseteq [n] \times [n]$, $|M_i| = \Omega(n)$
והאלג׳ פועל:
- בוחר $(k_1, k_2) = c \in_R M_i$
- שואל $(\bar{x})_{k_1}$ $(\bar{x})_{k_2}$
- מחזיר ערך $f((\bar{x})_{k_1}, (\bar{x})_{k_2})$

f קבועה (תלויה רק ב i, k_1, k_2).

<u>ה RAC</u>
<u>הק׳ 3/3</u>

$$\psi_x = \sum_{j \in [\bar{n}]} (-1)^{(\bar{x})_j} |j\rangle$$

שלם רוצים לבדוק ערך X_i [כלשהו]

לכל j כשמצאנו את שני הביטים האלה j שנמצאים ב- M_i
אז * אם גילינו שגיאה ומצבנו

אם קיבלנו * – הפסקנו (כמו, קבוצה)
אחרת קיבלנו

$$\frac{1}{\sqrt{2}}\left[(-1)^{(\bar{x})_{k_1}}|k_1\rangle + (-1)^{(\bar{x})_{k_2}}|k_2\rangle\right]$$

עבור $(k_1,k_2)\in M_i$, ואחרי זה מ- M_i

אם הוספנו את $|0\rangle$ קיבלנו, נניח

$$\frac{1}{\sqrt{3}}\left[|0\rangle + (-1)^{(\bar{x})_{k_1}}|k_1\rangle + (-1)^{(\bar{x})_{k_2}}|k_2\rangle\right]$$

נמדוד לפי 4 המצבים הבאים ל- $a,b\in\{0,1\}$

$$\frac{1}{2}\left[\underset{00}{|0\rangle} + (-1)^{a}\underset{01}{|1\rangle} + (-1)^{b}\underset{10}{|2\rangle} + (-1)^{a+b}\underset{11}{|3\rangle}\right]$$

x_{aba}

ההסתברות שנקבל $\Psi_{a,b}$ כאשר $a=(\bar{x})_{k_1}$, $b=(\bar{x})_{k_2}$
היא

$$\left(\frac{1}{\sqrt{3}}\cdot\frac{1}{2}\cdot 3\right)^2 = \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4}$$

וההסתברות לקבל $\Psi_{a',b'}$ אחר הוא

$$\left(\frac{1}{\sqrt{3}}\cdot\frac{1}{2}\cdot(\pm 1)\right)^2 = \frac{1}{12}$$

לכן ההסתברות של (1) לקבל תשובה, ואחרת quit

ובהסתברות תשובה – תקינה $\ge \frac{3}{4}$ נכונה $\ge \frac{1}{4}$ שגויה. 18.

שאלה 2: משמעות הוכחה במקום בהסתברות לפחות קבועה.

פרוטוקול ל coin flipping

משתתפים הוגנים

- A בוחרת $|0\rangle$ או $|+\rangle$ באקראי ושולחת ל B.
- B בוחר basis באקראי ושולח ל A.
- A מגלה איזה וקטור היא שלחה $|0\rangle$ - נאמר 0, $|+\rangle$ - נאמר 1

תוצאת המשחק: אם 0, A מנצחת באופן, B ב 1.

דרוש: כשהם הוגנים תוצאת המשחק מאוזנת.

אם A הוגנת ו B רמאי

$$pr(B \text{ מנצח}) = pr(\text{מנחש נכון } B) \le \frac{1}{2} + \frac{\| |0\rangle\langle 0| - |+\rangle\langle +| \|_{tr}}{4}$$

$$\| |0\rangle\langle 0| - |+\rangle\langle +| \|_{tr} = \| |v_{\frac{\pi}{8}}\rangle\langle v_{\frac{\pi}{8}}| - |v_{-\frac{\pi}{8}}\rangle\langle v_{-\frac{\pi}{8}}| \|_{tr} = \left\| \begin{pmatrix} \cos^2\frac{\pi}{8} & c(\frac{\pi}{8})s(\frac{\pi}{8}) \\ c(\frac{\pi}{8})s(\frac{\pi}{8}) & \sin^2\frac{\pi}{8} \end{pmatrix} - \begin{pmatrix} c^2 & -cs \\ -cs & s^2 \end{pmatrix} \right\|_{tr}$$

$$= \left\| \begin{pmatrix} 0 & \sin(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) & 0 \end{pmatrix} \right\|_{tr} = 2\sin(\frac{\pi}{4}) = 2\frac{\sqrt{2}}{2} = \sqrt{2}$$

$\lambda_1 = -\lambda_2$ $\quad$ $\lambda_1 = \sin(\frac{\pi}{4})$

$\lambda_1 \cdot \lambda_2 = -\sin^2(\frac{\pi}{4})$ $\quad$ $\lambda_2 = -\sin(\frac{\pi}{4})$

$$pr(B \text{ מנצח}) \le \frac{1}{2} + \frac{\sqrt{2}}{4} \sim 0.85..$$

אם B הוגן ו A רמאית

① אם A הכינה לא pure state,

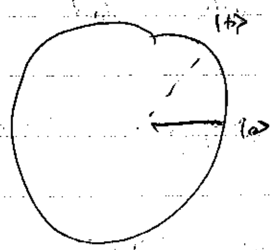
אז היא מקסימום רק הכינה pure state

לכן נניח כי A ב pure state,

הוכחה: נניח כי שאר הוכחה רק עם pure states

שאלה חלק ב – Bob!

① אם A מודד $\psi \in H_2$ ושולח ל Bob
רק לשלוח את A של יכולה לזהות אבל.



למשל או המצב $|0\rangle$
או המצב $|+\rangle$

ולכן אחד המקרים יגרום לזה
בסבירות גבוהה.

② נניח קורה עם A יוצרת pure state
אבל שולחת רק את החלק ל Bob?

$\rho = Tr_B |\psi\rangle\langle\psi|$

ואז או $|\langle 0|\rho|0\rangle| < 1$
או $|\langle +|\rho|+\rangle| < 1$

ולכן בהסתברות קטנה Bob יגלה ש A רמאי.