תזכורת: Johnson's bound

משפט: אם C קוד $[\bar{n}, t, (\frac{1}{2}-\varepsilon')\bar{n}]_2$

אז קוד $(\frac{1}{2}-\sqrt{\frac{\varepsilon'}{2}}, \frac{1}{4\varepsilon'}+1)$ l.d.

כלומר: לכל $y \in \{0,1\}^{\bar{n}}$

$$\left|\{c \in C \mid Ag(c,y) \geq (\tfrac{1}{2}-\sqrt{\tfrac{\varepsilon'}{2}})\bar{n}\}\right| \leq L = \frac{1}{4\varepsilon'}+1$$

בניה של strong-ext $E: \mathbb{F}_2^n \times [\bar{n}] \to \mathbb{F}_2$ (תר' 99)

נקח C אשר קוד E.C.C $[\bar{n}, n, (\frac{1}{2}-\varepsilon)\bar{n}]_2$ $\varepsilon' = \frac{\varepsilon^2}{2}$

ונגדיר $E: \mathbb{F}_2^n \times [\bar{n}] \to \mathbb{F}_2$

ע"י $E(x,y) = \underbrace{(C(x))_y}_{\text{הביט ה-}y\text{ של }C(x)}$

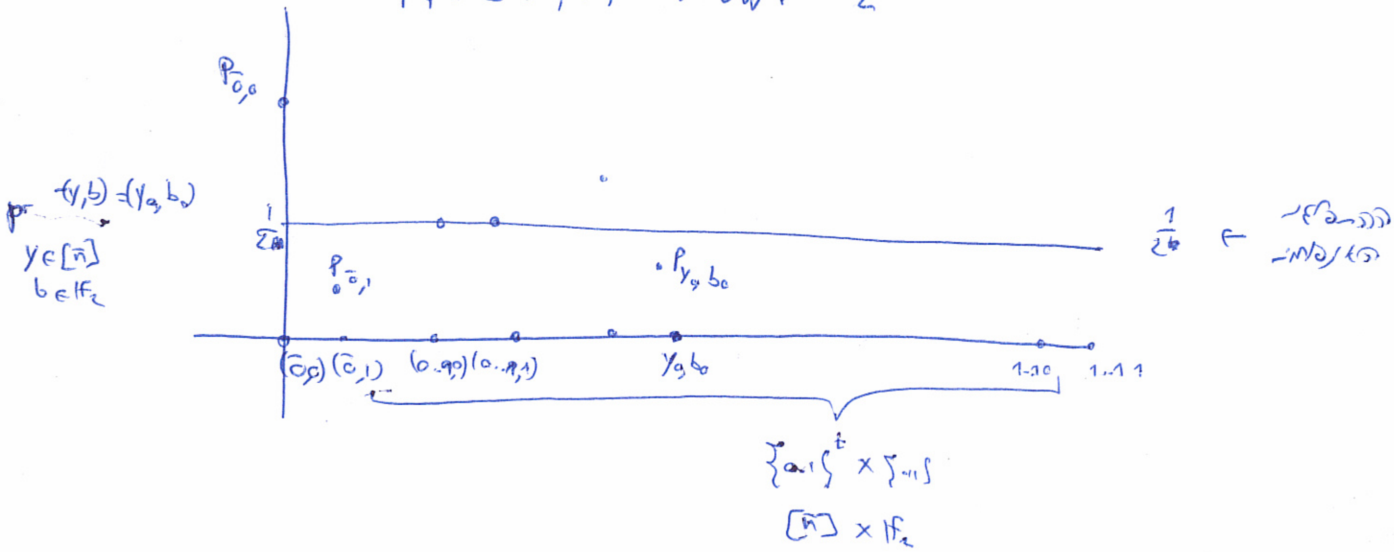
משפט: E הוא strong-ext $(k^* = 2\lg\frac{1}{\varepsilon}, \varepsilon^* = \sqrt{2\varepsilon'})$

הוכחה

הוכחה   נניח שלא.

נניח יש X הקבוצה שגודלה לפ 2^{k^*} איברים

כך ש $|Y_0 \circ E(X,Y) - U \times U|_1 \geq \epsilon^*$



לכל b $y \in [n]$ נסמן $P_{y,b} = \Pr_{x \in X}[E(x,y) = b]$

לכל $y \in [n]$ $P_{y,0} + P_{y,1} = 1$

אנחנו יודעים ש $\frac{1}{2n} \sum_{\substack{y \in [n] \\ b \in \{0,1\}}} \left| P_{y,b} - \frac{1}{2} \right| \geq \epsilon^*$

$$D : [\tilde{n}] \to \{0,1\}$$

נסמן

$$D(y) = \begin{cases} 0 & P_{y,0} \geq P_{y,1} \quad \text{אם} \\ 1 & \text{אחרת} \end{cases}$$

D מגדיר התפלגות X אבל לא ב $x \in X$ ספציפי.

D מגדירה מילה $D \in \{0,1\}^n$ כי $D_x = D(x)$.

$$\Pr_{\substack{x\in X \\ y\in[\tilde{n}]}} \left(D(y) = E(x,y)\right) = \frac{1}{n} \sum_{y\in[\tilde{n}]} \underbrace{\max\{P_{y,0}, P_{y,1}\}}_{\text{נסמן } P_y}$$

$$\left(P_y - \tfrac{1}{2}\right) + \left(\tfrac{1}{2} - (1-P_y)\right) = 2P_y - 1$$

$$2P_y = 1 + \left|P_{y,\max} - \tfrac{1}{2}\right| + \Big|\underbrace{P_{y,1\max}}_{1-P_{y,\max}} - \tfrac{1}{2}\Big|$$

$$\frac{1}{n}\sum_{y\in[\tilde{n}]} P_y = \frac{1}{2} + \frac{1}{n}\sum_{y,b} \left|P_{y,b} - \frac{1}{2}\right| \geq \frac{1}{2} + \varepsilon' \quad \text{הנ"ל}$$

$$\Pr_{\substack{x\in X \\ y\in[\tilde{n}]}} \left(D(y) = E(x,y)\right) = \frac{1}{n}\sum_{y\in[\tilde{n}]} P_y \geq \frac{1}{2} + \varepsilon',$$

נניח ש $x_0 \in G$ אז

x_0 "טוב"

$$\Pr_y \left[D(y) = E(x_0, y) \right] \ge \frac{1}{2} + \frac{\epsilon^*}{2}$$

וכן

$$\Pr_x \left[x_0 \in G \right] \ge \frac{\epsilon^*}{2}$$

אם $x_0 \in G$!

המפה D מקיימת $Ag(D, e(x_0)) \ge \frac{1}{2} + \frac{\epsilon^*}{2}$

$\frac{\epsilon^*}{2} \ge \sqrt{\frac{\epsilon'}{2}}$

~~מאחר~~ מכיון שיש לכל היותר $O(\frac{1}{\epsilon})$

$\epsilon' \ge O(\sqrt{\epsilon})$

מילים כאלו

נקבל

$$\frac{\epsilon^*}{2} |X| \le |G| \le O\left(\frac{1}{\epsilon'}\right)$$

$$2^{t^*} = |X| \le O\left(\frac{1}{\epsilon \epsilon'}\right) = O\left(\left(\frac{1}{\epsilon'}\right)^{1.5}\right)$$

$k' \le O(\log \frac{1}{\epsilon})$ כנדרש.

$\square$

בניה 2 של str. ext — לא הראנו בכלל — Trevisan's al

הגדרה: $S_1,\dots,S_m \subseteq [t]$ נקרא (l,a)-design אם

$$\forall i \quad |S_i| = l$$

$$\forall i \neq j \quad |S_i \cap S_j| \le a$$

משפט: קיים כזה עם $t = O\left(\frac{l^2}{a}\right)$

וגם ניתן לבנות בזמן פולינומי.

הבנייה: $T: \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ משתמש ב-ECC $C[\bar{n}, n, \tfrac{1}{2}-\epsilon']_2$

$\epsilon' = \frac{\epsilon^2}{2m^2}$

וכן $S_1 \dots S_m \subseteq [t]$ (l,a)-design. $l = \lg \bar{n}$,

$a = O(\lg n)$ או $a = O(1)$

אז:

$$T(\underset{\{0,1\}^n}{\underset{\uparrow}{x}}, \underset{\{0,1\}^t}{\underset{\uparrow}{y}}) = z_1 \dots z_m$$

$$z_i = (\underbrace{C(x)}_{\substack{\text{הקידוד של } x \\ C(x)\in\{0,1\}^{\bar{n}}}})_{\underbrace{y|_{S_i}}_{\text{אינדקס}}}$$

$$\underbrace{\overset{S_i}{y}}_{\in \{0,1\}^l}$$

כמו ext. זה רק מאגר,

אבל ה-seed – recycled.

למטרה שלו ב-k רנדומי כי מגיע הולך מסודר.

משפט T הוא (k,ε) strong ext.

כאשר $k = m\cdot 2^{a} + 3\lg\frac{m}{\varepsilon}$

בחירת פרמטרים:

(א) $a=O(1)$, $\varepsilon' = \frac{\varepsilon^2}{2m^2}$

$$\bar{n} = \mathrm{poly}\left(\frac{n}{\varepsilon}\right)$$

$$\ell = O\left(\lg\frac{n}{\varepsilon}\right)$$

$$a = O(1)$$

$$t = O\left(\frac{\ell^2}{a}\right) = O\left(\lg^2\frac{n}{\varepsilon}\right)$$

$$k = O(m) + O\left(\lg\frac{m}{\varepsilon}\right)$$

$$\underset{\text{מספר ביטי הפלט}}{m} = \underset{\text{קבוע, } \alpha<1}{\alpha\cdot k}$$

(ב) $\ell = O\left(\lg\frac{n}{\varepsilon}\right)$, $\bar{n} = \mathrm{poly}\left(\frac{n}{\varepsilon}\right)$, $\varepsilon' = \frac{\varepsilon^2}{2m^2}$

$$t = O\left(\frac{\lg^2\frac{n}{\varepsilon}}{\lg\frac{n}{\varepsilon}}\right) = O\left(\lg\frac{n}{\varepsilon}\right) \qquad a = O\left(\lg\frac{n}{\varepsilon}\right)$$

$$k = 2^{a}\cdot m = \sqrt{n}\cdot m \qquad \boxed{m = \frac{k}{\sqrt{n}}} \qquad a = \frac{1}{2}\lg n \quad \varepsilon = \frac{1}{n}$$

<u>הוכחה:</u> נניח בשלילה.

- תהי X התפלגות שאינה על 2^k איברים עבורה

$$\left| u \circ T(x,u) - U_t \times U_m \right|_1 \geq \varepsilon$$

- לכן יש מבחן $D: \{0,1\}^t \times \{0,1\}^m \to \{0,1\}$ כך ש

$$\Pr_{\substack{x\in X\\ y\in U}} D(y, T(x,y)) = 1 \geq \Pr_{\substack{y\in U\\ z\in U}} (D(y,z)=1) + \varepsilon$$

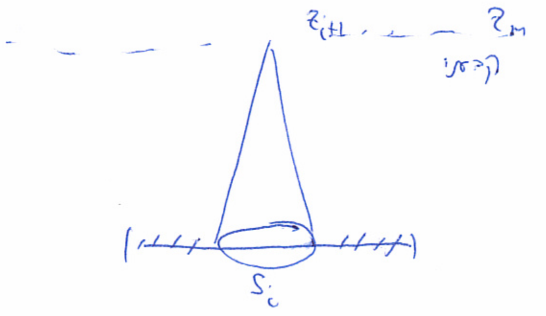
- לכן, יש $1 \le i \le m$ כך ש

$$\Pr_{\substack{x\in X\\ y\in U\\ z\in U}} D(y, T(x,y)_{1..i+1}, z_{i+2}..z_m) = 1 \geq \Pr_{\substack{x\in X\\ y\in U\\ z\in U}} D(y, T(x,y)_{1..i}, z_i..z_m) + \frac{\varepsilon}{m}$$

ולכן ממוצע יש דרך לבחור ולקבע $z_{i+2}..z_m$ שמשמרים כנ"ל סדר.

- נראה שבעזרת, יש $P: \{0,1\}^t \times \{0,1\}^i \to \{0,1\}$ כך ש

$$\Pr_{\substack{x\in X\\ y\in U}} \left[P(y, T(x,y)_{1..i}) = T(x,y)_{i+1} \right] \geq \frac{1}{2} + \frac{\varepsilon}{m}$$



בפרט יש צורך לקבע $y|_{\bar{S_i}}$

שישאר כפי שהוא.

$$\Pr_{\substack{x\in X \\ w\in\{0,1\}^\ell}}\left[\underline{P}(w, T(x,y)_{1..i}) = (C(x))_w\right] \ge \frac{1}{2}+\frac{\epsilon}{m}$$

ומכאן, נסמן x "טוב" $x\in G$ אם

$$\Pr_{w\in\{0,1\}^\ell}\left[P(w, T(x,y)_{1..i}) = (C(x))_w\right] \ge \frac{1}{2}+\frac{\epsilon}{2m}$$

אז $\Pr_{x\in X}[x\in G] \ge \frac{\epsilon}{2m}$

היינו רוצים לקחת את P ולבנות ממנה מילה $P\in\{0,1\}^{\bar{n}}$

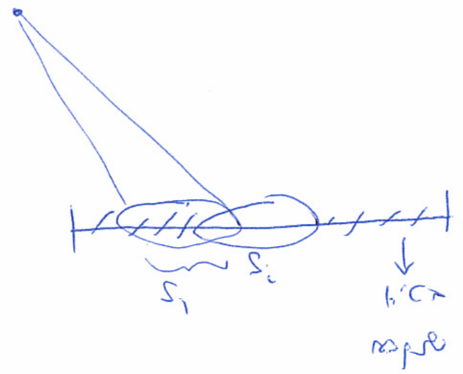
כך שלכל $x\in G$ $C(x)$ קרובה ל P

הבעיה ש ℓ קטן, ואילו $|X|$ גדול, כמו קודם.

הרעיון: ש $\underline{P}$ קובע הגדרה שונה לכל x

ועכשיו $\underline{P}$ תלויה ב- x, דרך $T(x,y)_{1..i}$.

נקודת המפתח היא שאין הרבה אפשרויות ל $T(x,y)_{1..i}$



אינפורמלי: $T(x,y)_1 = C(x)|_{y|_{S_1}}$

נבנה $\bar{n}$ טבלאות: ה-C הראשון של C(x)
השני
ה-n של C(x)

דומה, כיוון ש $y|_{S_1}$ נקבע, אשר קובע הכל שאר הביטים תלוי רק ב- $y|_{S_1 \cap S_2}$

כיוון ש $|S_1 \cap S_2| \le a$, יש רק 2^a ערכים שונים אפשריים.

וכך ל- $T(x,y)_i$, $T(x,y)_2$.

שיכול לחשב את x מ- y. $adv: \{0,1\}^n \to \{0,1\}^A$

גודל עצה
$A = O(m \cdot 2^a)$
ונדרש:

$$\forall_{x \in G} \quad \Pr_{w \in \{0,1\}^\ell} \left[P(w, adv(x)) = (C(x))_w \right] \ge \frac{1}{2} + \frac{\varepsilon}{2m}$$

$adv(x)$ - יכיל לכל $1 \le j \le m$

את כל ערכים של $y|_{S_i \cap S_j}$

על הערך $C(x)_{y|_{S_j}}$

מספיק לשמור: כי הערכים $S_i \cap S_j$ קבועים והכל שאר הביטים של $y|_{S_j}$.

1. $O(m \cdot 2^a)$ ביטים.

bound

$[n, t, (\frac{1}{2}-\varepsilon')\bar{n}]_2$ קוד C

כלומר: C הוא $(\frac{1}{2}-\sqrt{\frac{\varepsilon'}{2}}, \frac{1}{4\varepsilon'}+1)$ l.d.

כלומר: לכל $y \in \{0,1\}^{\bar{n}}$

$$\left|\{c \in C \mid Ag(c,y) \geq (\tfrac{1}{2}-\sqrt{\tfrac{\varepsilon'}{2}})\bar{n}\}\right| \leq L = \frac{1}{4\varepsilon'}+1$$

(תזכורת) $E: \mathbb{F}_2^n \times [\bar{n}] \to \mathbb{F}_2$ strong-ext

$\varepsilon' = \frac{\varepsilon^2}{2}$

בהינתן קוד C $[\bar{n}, n, (\frac{1}{2}-\varepsilon')\bar{n}]_2$ נגדיר E:

$E: \mathbb{F}_2^n \times [\bar{n}] \to \mathbb{F}_2$

$E(x,y) = \underbrace{(C(x))_y}_{\text{הביט ה-}y\text{ של }C(x)}$

טענה: E הוא strong-ext $(k^* = 2\lg\frac{1}{\varepsilon}, \varepsilon^* = \sqrt{2\varepsilon'})$

הוכחה

(1)

אם $adv \in \{0,1\}^A$ נגדיר $P_{adv} \in \{0,1\}^{\bar{n}}$

ע"י $(P_{adv})_w = P(w, adv)$

נגדיר $L = \{c \in C \mid \exists adv \in \{0,1\}^A \quad Ag(c, P_{adv}) \geq \frac{1}{2} + \frac{\varepsilon}{2m}\}$

$\frac{\varepsilon}{2m} = \sqrt{\frac{\varepsilon'}{2}}$

אז (1) $|L| \leq 2^A \cdot \frac{1}{\varepsilon'} = O(2^A \cdot \frac{m^2}{\varepsilon^2})$

(2) $\forall x \in G \quad \exists adv \in \{0,1\}^A \quad Ag(C(x), P_{adv}) \geq \frac{1}{2} + \frac{\varepsilon}{2m}$

$adv = adv(x)$

לכן $C(x) \in L$

ומכאן $|G| \leq |L|$

כלומר $2^k = |X| \leq O(\frac{m}{\varepsilon} \cdot \frac{m^2}{\varepsilon^2} 2^A)$

$k = A + O(\lg \frac{m}{\varepsilon})$

$k = m \cdot 2^a + O(\lg \frac{m}{\varepsilon})$

(10)

הוכ׳ P

נניח:
$$\Pr_{x,y}\left(D(y, T(x,y)_{1..i+1})=1\right) \geq \Pr_{x,y,\, b\in\{0,1\}} D(y, T(x,y)_{1..i}, b)=1 + \delta$$

נסמן
$$P_{x,y,T} = \Pr\left(D(y, T(x,y)_{1..i}, T(x,y)_{i+1}\right) = 1$$
$$P_{x,y,F} = \Pr\left(D(y, T(x,y)_{1..i}, \overline{T(x,y)_{i+1}}\right) = 1$$

אז
$$\Pr_{x,y,b}\left(D(y, T(x,y)_{1..i}, b)=1\right) = \frac{P_{x,y,T}+P_{x,y,F}}{2}$$

ומה שנתון קבלנו
$$P_{x,y,T} \geq \frac{P_{x,y,T}+P_{x,y,F}}{2}+\delta$$

כלומר
$$P_{x,y,T} - P_{x,y,F} \geq 2\delta$$

נגדיר את P עם שבוחר b אקראי, מחשב $D(y, T(x,y)_{1..i}, b)$

אם קיבלנו 1, נחזיר b ~~...~~ $P(y, T(x,y)_{1..i}) = b$ אחרת $1-b$.

אז:
$$\Pr_{x,y}\left(P(y, T(x,y)_{1..i}) = T(x,y)_{i+1}\right) = \underbrace{\frac{1}{2}}_{\text{b היה נכון}} \cdot P_{x,y,T} + \underbrace{\frac{1}{2}}_{\text{b היה שגוי}}\underbrace{(1-P_{x,y,F})}_{\text{ולא נחזיר את הנכון}}$$

$$= \frac{1}{2} + \frac{P_{x,y,T}-P_{x,y,F}}{2} = \frac{1}{2}+\delta$$

.◻