Nisan's generator

[illegible] $H=\{h:[M]\to[M]\}$

כך שלכל $A,B\subseteq[M]$

$$\Pr_{h\in H}\Bigg[\underbrace{\Big|\Pr_{\substack{x\in[M]\\ h\in H}}\big(x\in A \wedge h(x)\in B\big) - \rho(A)\rho(B)\Big| \ge \alpha}_{}\Bigg] \le \frac{1}{\alpha^2 M} = \epsilon$$

[illegible] α [illegible]

– אם $\Big|\Pr_{\substack{x\in[M]\\ h}}\big(x\in A \wedge h(x)\in B\big) - \rho(A)\rho(B)\Big| \le \alpha$

נגיד ש h α-טובה ל (A,B).

– נאמר ש h רעה:

הערות:

1) כבר ראינו כזו בתרגיל והבחנו שזה מתקיים

עבור H משפחה h 2-UF OHF.

(תרגיל 5, שאלה 2) $|H|=M^2$ $h\in\{0,1\}^{2\lg M}$.

2) ראינו תכונה כמו של אקספנדרים

①

שכן הנתון הוא G $[N, D, \lambda]$-graph

$$\forall A,B \quad \left| \frac{E(A,B)}{N \cdot D} - \rho(A)\rho(B) \right| \le \lambda \sqrt{\rho(A)(1-\rho(A))\rho(B)(1-\rho(B))} \quad \text{צ"ל}$$

(תרגיל 7 שאלה ב)

נב תכונה שלא מספיק לנו, לגבי ק מאוד לקחת אותה עבור

לקחת את $h \in_R [M]$, $h(x) = L$

אך (*) מתקיים לא לכל איבר .

ולכן אם לצורך זה מוגדר.

3) התכונה מגדירה כמו ה strong-ext

כאשר לכל seed (h)

$h(A) \approx U$.

מה שבי אומרים זה רואים פה entropy less.

זה בדיוק זה נאמר ה strong ext כלל.

הגנרטור:

$$
\begin{array}{cccc}
\vee & \vee & \vee & \vee \\
\underline{x} & \underline{h_2(x)} & \underline{h_1(x)} & \underline{h_2(h_1(x))} \\
\multicolumn{2}{c}{\underline{x}} & \multicolumn{2}{c}{\underline{h_1(x)}} \\
\multicolumn{4}{c}{\underline{\qquad\qquad}} \\
\multicolumn{4}{c}{x \in_R [M]}
\end{array}
$$

$h_1 \dots h_t \in_R H$

פורמלית:

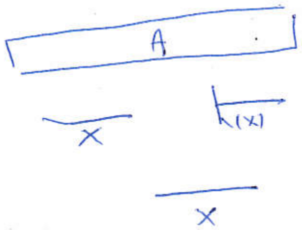
$G_0(x) = x$

$G_t : [M] \times [H]^t \to [M]^{(2^t)}$

$G_t(x; y_1 \dots y_t) = G_{t-1}(x; y_2 \dots y_t)\ G_{t-1}(h_1(x), h_2 \dots h_t)$

נקרא בשם הגנרטור של INW (בקיצור PRG).

③



נכונות-

המקרה $t=2$:

נניח אנו מנסים לרמות- BP A

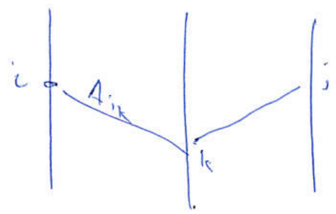
שגודלו $[W, 2, [M]]$

רוחב   א״ב -

נסמן

$$A_{i,k} = \{a\in[M] \mid i \xrightarrow{a} k\}$$

a יעביר מ-i ל-k
ב-A בהסתברות



$$B_{k,j} = \{b\in[M] \mid j \xrightarrow{b} k\}$$

בשכבה השניה

נסמן מטריצה . $A_{w\times w}$

$$A[i,j] = \Pr_{x_1,x_2}\{i \xrightarrow{x_1,x_2} j\}$$

הסתברות ש i יעבור
ל j בדיוק לפי A.

$$A[i,j] = \sum_{k\in W} \Pr_{\substack{x_1\in[M] \\ x_2\in[M]}} (x_1\in A_{ik} \wedge x_2\in A_{kj})$$

④

- נגדיר ש h α-טובה ל (A_{ik}, B_{kj}) אם

$$\left| \Pr_{\substack{x\in[M] \\ h\in H}} \left(x\in A_{ik} \wedge h(x)\in B_{kj}\right) - P(A_{ik})\, P(B_{kj}) \right| \le \alpha$$

- נגדיר ש h α-טובה ל A אם h α-טובה לכל (A_{ik}, B_{kj}) לכל $1\le i,k,j\le M$.

טענה: ① לכל A, $\Pr[h \text{ לא α-טובה ל } A] \le W^3 \delta$

② אם h α-טובה ל A

אז

$$\forall_{i,j} \quad \left| A_h[i,j] - A[i,j] \right| \le W\alpha$$

$$A_h = \Pr_{\substack{x\in[M] \\ h\in H}} \left(\text{מסלול ב } A \text{ מ } i \text{ ל } j \text{ דרך } (x,h(x)) \right) = \sum_{k=1}^{W} \Pr\left(x\in A_{ik} \wedge h(x)\in B_{kj}\right)$$

לכן

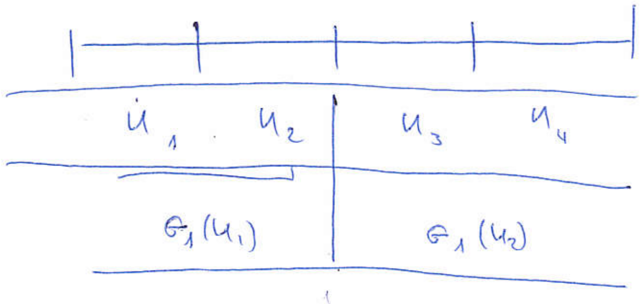
$$\|A_h - A\|_{max} \le W^2 \alpha$$

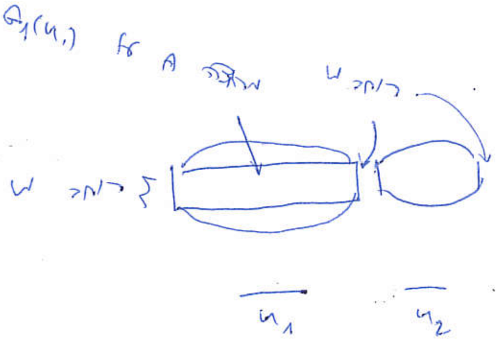
עבור $t=2$

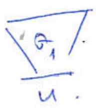
$[w, y, [M]]$

$\downarrow$ רמה, $\downarrow$ אורך, $\downarrow$ ε

נשווה:







עד

הינו יכולים לפרמל את הביטחון.

במקום זה, קודם נבין קצת את ההגדרה

ורק נפרמל.

פישוט

① בה"כ המכונה A מריצה כל שלב רק אחד

אלגוריתם.

למה? נניח שלא. נכניס את המצב לתוך המכונה

כלומר

$$(\sigma, i) \to (J, i+1)$$

$$\Updownarrow$$

קודם ברמה ה i (מצב). $J \to \sigma$.

---

② תחת הפישוט הנ"ל, את מטריצת המעברים ל רמה

אזי היא A

$$A[i,j] = \Pr_{x \in \Sigma}[i \rightsquigarrow j]$$

משתמש ה-i   הולכים לפי x   מגיעים ל-j

אז מטריצת המעברים של T שלבים היא A^T.

$$A^2[i,j] = \sum_{k \in W} A_{ik} A_{kj}$$

בקבוצה הגדולה, מה שראינו קודם עבור $t=1$ הוא:

$$\Pr[A \text{ ל } \text{טוב } h] \geq 1 - W^3\delta$$

ואם h טוב ל A אז

$$\| A^2 - A_h \|_{\text{row}} \leq W^2 \alpha$$

עכשיו עבור $t=2$

(נסמן A_{h_1,h_2} מטריצה $W \times W$.

$$A_{h_1,h_2}[i,j] = \Pr_{\substack{x\in[M] \\ h_1,h_2\in H}}[i \rightsquigarrow j]$$

תחת $G(x,h_1,h_2)$

אז אם h_2 טוב ל A

ואם h_1 טוב ל A_{h_2}

אז!

A_{h_2} - BP $[W,2,[M]]$

i מגיע ל j

אם A מגיע מ i ל

תחת $x, h_2(x)$

$$\|A^4 - A_{h_1,h_2}\|_{row}$$

$$\le \underbrace{\|A^4 - A^2_{h_2}\|_{row}}_{\le\, 2\|A^2 - A_{h_2}\|_{row} \,\le\, 2(W^2\alpha)} + \underbrace{\|A^2_{h_2} - A_{h_1,h_2}\|_{row}}_{\le\, W^2\alpha} \le 3(\underbrace{W^2\alpha}_{\gamma}) = 3\gamma$$

כי h_1 טוב ל A_{h_2}

$$\|A^2 - B^2\|_{row} \le \|A^2 - AB\|_r + \|AB - B^2\|_r \le \underbrace{\|A\|_r}_{\le 1} \cdot \|A-B\|_r + \underbrace{\|B\|_r}_{\le 1} \|A-B\|_r$$

$$\le 2\|A-B\|_r$$

ובאופן כללי:

$k=3$

$$\|A^8 - A_{h_1,h_2,h_3}\| \le \underbrace{\|A^8 - A^2_{h_2,h_3}\|}_{\le\, 2\|A^4 - A_{h_2,h_3}\| \,\le\, 2\cdot(4-1)\gamma} + \underbrace{\|A^2_{h_2,h_3} - A_{h_1,h_2,h_3}\|}_{\gamma}$$

כי $\underline{h_1}$ טוב ל $A_{h_2 h_3}$

$$\le 7\gamma$$

$A \quad r \quad s/c \quad h_t \quad r/c$

$A_{h_t} \quad " \quad " \quad h_{t-1}$

$A_{h_t, h_{t-1}} \quad " \quad h_{t-2}$

$\vdots$

$A_{h_t, \ldots, h_2} \quad r \quad s/c \quad h_1$

s/c

$$\| A^{(2^t)} - A_{h_1 \ldots h_t} \|_r \leq$$

$$\| A^{(2^t)} - A^2_{h_2 \ldots h_t} \|_r + \underbrace{\| A^2_{h_2 \ldots h_t} - A_{h_1 \ldots h_t} \|_r}_{\gamma.}$$

$$\leq 2 \| A^{(2^{t-1})} - A_{h_2 \ldots h_t} \|_r$$

$$\leq 2 \cdot (2^{t-1} - 1)\gamma + \gamma = (2^t - 1)\gamma$$

הגיע הזמן לבחור פרמטרים

אם רצינו עוד להגיע לשגיאה ε

אז אנו רוצים $2^t\gamma \le \varepsilon$ $\qquad T = 2^t$

$$W^2\alpha = \gamma \le \frac{\varepsilon}{T}$$

$$\alpha \le \frac{\varepsilon}{W^2 T}$$

ואנו צריכים:

$$\Pr\begin{bmatrix} A \text{ מנבא } h_t \\ A_{h_t} \quad \cdots \quad h_{t-1} \\ \vdots \\ A_{h_1\ldots h_{t-1}} \text{ מנבא } h_1 \end{bmatrix} \geq 1 - tW^3\delta > 0$$

רוצים $W^3 t\delta < 1$

$$\frac{1}{\alpha^2 M} = \delta < \frac{1}{W^3 t}$$

$$M > \frac{W^3 t}{\alpha^2} \geq \frac{W^3 t\, W^4 T^2}{\varepsilon^2} = \frac{W^7 T^2 t}{\varepsilon^2}$$

אם $W = T = \frac{1}{\varepsilon} = poly(n)$

אז $M = poly(n)$

וכל $x \in [M]$ צריך $O(\lg n)$ ביטים

וכל $h_i \in H$ צריך $2\lg M = O(\lg n)$ ביטים

PRG $\exists$ seed $\to$ T

בסה"כ הטכניקה לוקח

$$\boxed{O\Big(\underbrace{\lg T}_{h_1,\dots,h_t} \cdot \Big(\lg \frac{TW}{\varepsilon}\Big)\Big)}$$

ובפרט לכמות ε-BP $[W=n^{c_1},\ T=n^{c_2},\ \varepsilon]$

עבור $\frac{1}{\varepsilon}=n^{c_3}$

נדרש seed-length $O(\lg^2 n)$ כמו קודם.

מפורש? כן.

בהינתן ה $i_1,\dots,i_t$ נחשב

מחשב את:

$$h_{i_t}(h_{i_{t-1}} \dots h_{i_1}(x))$$

וניתן לחשב (בזמן ‹ $x, h_{i_1} \dots h_t$ כמה קלטים)

בזכרון $O(\log M)$.

היום הראינו משהו דומה לגנרטור הקודם ?

משפט: $RL \subseteq DTimeSpace(poly(n), O(\log^2 n))$

הוכחה:

שלב 1

נמצא $h_t \in H$ טוב ל A

$h_{t-1} \in H$ ... ל A_{h_t}

$\vdots$

h_1 טוב ל $A_{h_t,\dots,h_2}$

איך ? תכף

וכן **שלב 2**

לכל $i, j \in W$

נעבור על כל $x \in [M]$ ונראה האם $j \overset{x}{\leadsto} i$? ב $A_{h_t \dots h_1}$

} לולאה זו — $O(\log n)$ זכרון

כך נמצא את הגרף כולה $A_{h_1 \dots h_t}$

שהוא קרוב מאוד ל A^T

$\|A^t - A_{h_1 \dots h_t}\| \le \epsilon$.

ובפרט $A_{h_1 \dots h_t}[\underset{start}{s}, \underset{accept}{t}]$ קרוב מאוד להסתברות ש M מקבל.. וסיימנו את ההוכ'.

שלב 1:

נניח ממוינו $h_t .. h_1$

נעבור על כל h
אפשרי ל h_{l-1}.

h_{l-1} h_1 .. h_t

לכל אחד מהם נחשב $A_{h_t .. h_{l-1}}$ ($O(n)$ ד)

ונבדוק $\| A_{h_t .. h_{l-1}} - \hat{A}_{h_t .. h_1} \|$

עד שנמצא 1 מתאימה.