$BPL \subseteq DSpace(O(\log^{1.5} n))$ Saks Zhou

<u>נסיון ראשון</u>:

נשתמש עוד פעם ועוד פעם באותו ה h.

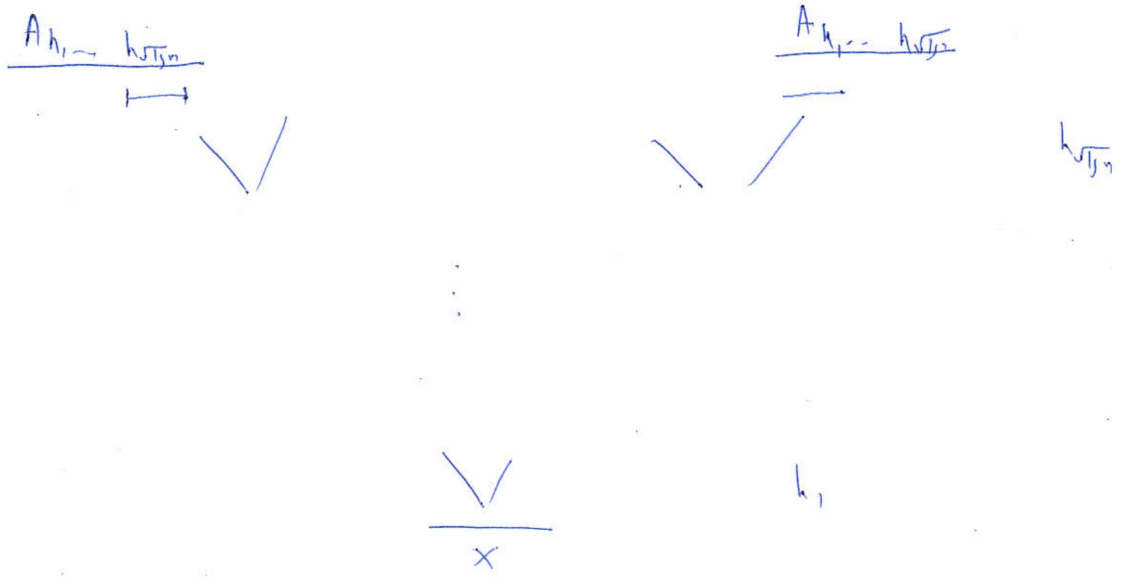
נראה: נמצא $h_1 \ldots h_{\sqrt{\log n}}$ טובים ל A

וגם

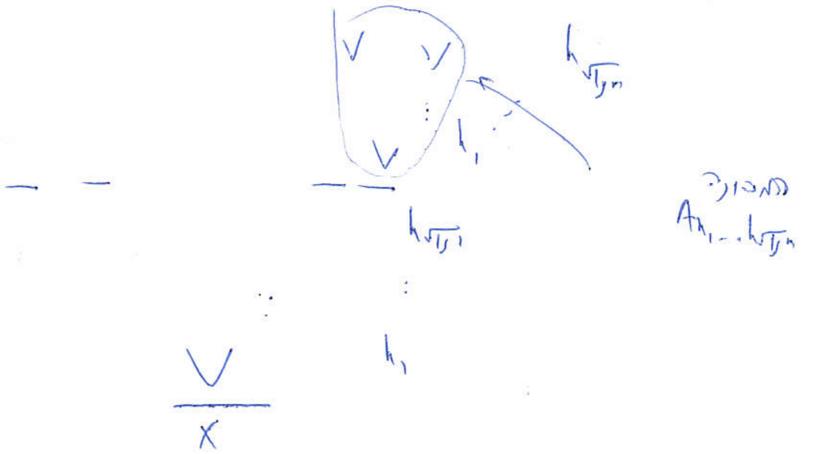
$$\| A^{(2^{\sqrt{\log n}})} - A_{h_1 \ldots h_{\sqrt{\log n}}} \|_{\infty} \le \alpha$$

- אם $h_1 \ldots h_{\sqrt{\log n}}$ אז טובים ל $A_{h_1 \ldots h_{\sqrt{\log n}}}$

אין [illegible]

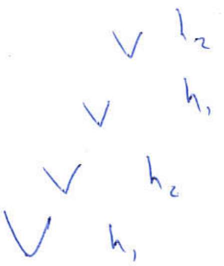


בפועל מה שקורה

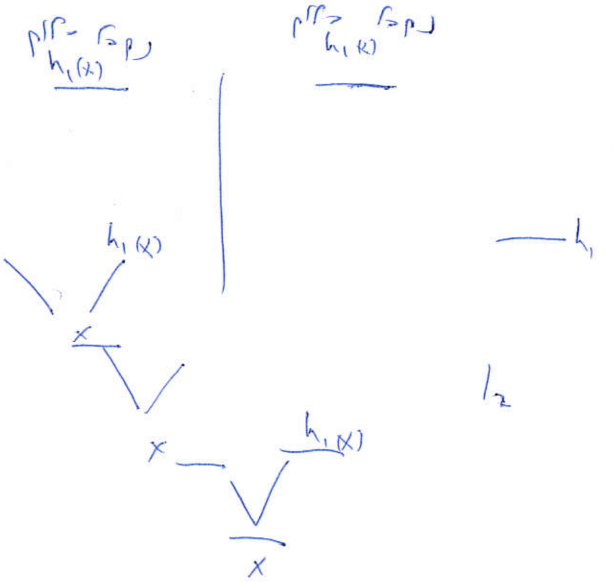


הערה: אין לדבר כזה שום סיכוי.

לפעל, אם נשמש.



נקודה



יש שני דלקים $h_1(x)$

ו-a מכונה בזכרון קטן

שמקבלת מתבלה בין 2

דלקים נכונים / random

נסיון 2:

המבנה $A_{h_1 \ldots h_{\sqrt{n}}}$ מאוד תלוי ב- $h_1 \ldots h_{\sqrt{n}}$

אבל מטריצת המעברים שלה, שהיא מטריצה $W \times W$

(כמעט) זהה,

כי:

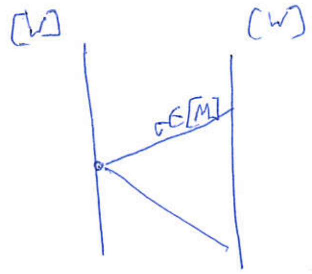
$$\| A_{h_1 \ldots h_{\sqrt{n}}} - \underbrace{A^{2^{\sqrt{n}}}}_{\text{זו מטריצה שאינה תלויה ב-}h_1 \ldots h_{\sqrt{n}}} \|_{\text{נורמה}} \le O(2^{\sqrt{n}} \alpha)$$

לכן, מה שנעשה, זה שכל $\sqrt{n}$ צעדים, נגריל את הגיבוב ונשנה את מטריצת המעבר, ואז מבנה ה-PRG שנוצר ממנה (המסדר), ומבנה זו <u>בלתי-תלויה</u> (כמעט) ב- $h_1 \ldots h_{\sqrt{n}}$, אז בעצ' נוכל להשתמש באותם $h_1 \ldots h_{\sqrt{n}}$ שוב.

מה ראינו עד עכשיו ?

① Branching Program ומטריצות מעבר:

BP: בהינתן את השכבות M BP שמסתכל על אותו כל צעד
בכל זמן



BP M, השרה מטריצת מעבר $A=A(M)$

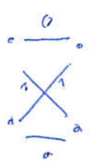
$$
\begin{array}{c|c}
 & \Sigma \\
\hline
\Sigma \;\; \sigma_1 & \left[\begin{array}{c} \\ A_{\sigma_1,\sigma_2} \\ \\ \end{array}\right]
\end{array}
$$

$A_{\sigma_1,\sigma_2} = \Pr\left[\begin{array}{c} \sigma_2 \text{ שנגיע ל} \\ \sigma_2 \text{ לעבור ל} \end{array}\right]$

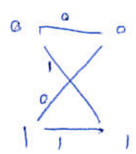
הכיוון ההפוך אינו חח״ע: לכל A יש הרבה מימושי BP

שמימושים רבים. למשל $\Sigma=\{1,2\}$, $A=\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

מימושים מתאימים:



או



וכו׳.

נאמר ש $h:[M]\to[M]$ טובה ל M

אם $\| A(M_h) - (A(M))^2 \|_{row} \le \varepsilon$

M_h - המכונה שעל קלט $x\in[M]$ מריצה את M. שני צע

על הקלט $x, h(x)$.

M^2 - המכונה שמריצה את M שני צעדים אקראיים.

ראינו שיש $H = \{h:[M]\to[M]\}$ 2.u.f $= poly\left(\frac{W}{\varepsilon}\right)$

ש ~~...~~ לכל M $[W,2,[M]]$-BP

כמעט כל h טובה ל M.

האלגוריתם של ניסן:

נגריל h_t טובה ל M

M_{h_t} h_{t-1}

$M_{h_t,h_{t-1}}$ h_{t-2}

$\vdots$

$M_{h_t \dots h_2}$ h_1

הרעיון של Saks Zhou

כמעט לכל n $\|A(M_n) - (A(M))^2\|_{max} \le \varepsilon$

לכן, $A(M_n)$ כמעט לא תלויה ב- n. ובפרט יש "כמעט" $(A(M))^2$.

לצורך הבנין נניח אפילו מכין $(A(M))^2$.

אם נגדיר מכונה M_1 שמכירה ב- המערך של $(A(M))^2$

אז, כמעט לכל n אותה גם ל M_n, וגם ל $(A(M))^2$ ו M_1.

וניתן להשתמש באותה n שוב.

מכונה קנונית למטריצת מעבר

נתונה מטריצת מעבר $A_{W\times W}$

נגדיר מכונה, שמצבה $w \in W$ ובכניסה $\sigma \in \Sigma$

עוברת ל $j \in W$ הקטן הראשון כך ש $\sum_{x \le j} A_{w,x} \ge \frac{|\sigma|}{|\Sigma|}$

כשמתייחסים ל σ כמספר בלב בינארי.

$x \in [M]$ $\quad h_1 \quad h_{\sqrt{\lg n}}$

נקרב

$$\boxed{A(M_{h_1 \ldots h_{\sqrt{\lg n}}})}$$

$M^{(1)} = M(A(M_{h_1 \ldots h_{\sqrt{\lg n}}}))$ ונעבור אל המכונה

① כאשר כל $h_1 \ldots h_{\sqrt{\lg n}}$ טובים ל M.

לכן, $A(M_{h_1 \ldots h_{\sqrt{\lg n}}}) \approx (A(M))^{2^{\sqrt{\lg n}}}$

נניח $A(M_{h_1 \ldots h_{\sqrt{\lg n}}}) = (A(M))^{2^{\sqrt{\lg n}}}$

אבל $M^{(1)}$ לא תלוי ב $h_1 \ldots h_{\sqrt{\lg n}}$!

לכן, כאשר h טובים ל $M, M^{(1)} = M((A(M))^{2^{\sqrt{\lg n}}})$

שוב נבחר $\bar{h} = h_1 \ldots h_{\sqrt{\lg n}}$ ונקרב

$$\boxed{A(M^{(1)}_{h_1 \ldots h_{\sqrt{\lg n}}})}$$

שוב כאשר $A(M^{(1)})^{2^{\sqrt{\lg n}}} = A(M)^{2^{\sqrt{\lg n}} \cdot 2^{\sqrt{\lg n}}}$, שוב אם טובים ל h

ונקבל $M^{(2)} = M(A(M^{(1)}_{h_1 \ldots h_{\sqrt{\lg n}}}))$

וכן הלאה.

כמעט בה $\bar{h}$ איננו $M, M^{(1)}, M^{(2)}$

$\boxed{M^{\sqrt{\lg n}}, A(M^{(\sqrt{\lg n}-1)}_{\bar{h}})}$

כל החישוב מבוצע ע״י וגו $\bar{h}$

$\vdots$

$\boxed{M^{(3)}, A(M^{(2)}_{\bar{h}})}$

$$A(M^{(k)}) \approx A(M^{(k-1)})^{2^{\sqrt{\lg n}}} \approx A(M)^{2^{k\cdot\sqrt{\lg n}}}$$

$\boxed{M^{(2)}, A(M^{(1)}_{\bar{h}\ldots})}$

$$A(M^{\sqrt{\lg n}}) \approx (A(M))^n$$

$\boxed{M^{(1)}, A(M_{h_1,\ldots h_{\sqrt{\lg n}}})}$

$x \in [n]$ $\quad h_1 \ldots \quad h_{\sqrt{\lg n}}$

כמעט בה h יוגדר לבד $M^{(i)}$

החישוב לוקח $\lg n \cdot \sqrt{\lg n}$ לצעדי ה- $h_1, \ldots, h_{\sqrt{\lg n}}$

1 $O(\lg n)$ לעבור מרמה לרמה,

$\sqrt{\lg n}$ רמות

ובסה״כ: $O(\lg n \cdot \sqrt{\lg n})$.

מעבר מרמה לרמה: [illegible] $M^{(k)}$

סבוכיות הזכרון היא [illegible]

① הזכרון r $\quad h = h_1 \dots h_t \quad$ זוכר מקום t זכרון

② c גודל המקום.

(כי פעם צריך לחשב את מכפלת המטריצים).

מספר הכפל של r $\quad M^{\overbrace{(2^t)\cdots(2^t)}^{c\ \text{פעמים}}} = M^{2^{ct}} = M^{2^{\lg n}}$

$ct = \lg n \qquad c = \frac{\lg n}{t}$

לכן מינימום $\quad c = t \quad t = \sqrt{\lg n}$

עכשיו נראה את הנקודה ש $A(M_n)$ תלוי ב n.

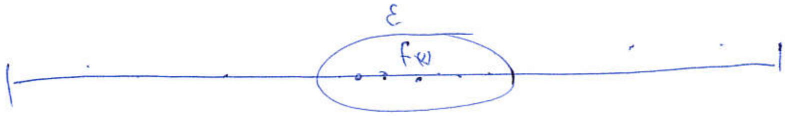
טענה: נניח ש פונק' $f:\{0,1\}^n \to \{0,1\}$ (לא נ...)

יש פרוצדורה אקראית $M(x,y)$

כך של $\epsilon,\delta>0$

משתמשת ב r ביטים $r=O(\lg \frac{n}{\epsilon\delta})$

כך ש: $\forall x \quad Pr_y[|M(x,y)-f(x)|>\epsilon]<\delta$



אני רוצה יש פרוצדורה אקראית (x,y,s)

כך ש $|y|=O(\lg \frac{n}{\epsilon\delta})$, $|s|=O(\lg\frac{1}{\delta})$

והפונק' $f':\{0,1\}^n \times \{0,1\}^s \to$

?כ״ק

המכונה M':

מחלקת את $\mathbb{R}$ המשמ״ם לקטעים באורך ε .. 2ε ε 0

נסמן $[z]$ - אמצע הקטע אליו z שייך.

נניח $\ell=|z|$. נשמור את z כמספר בין 0 ל-$1-2^{\ell}$.

ונגדיר

$$f'(x,z) = \left[\, x - \frac{\varepsilon}{2^{\ell}}\varepsilon \,\right]$$

תכונה ① מ״ב.

~~[illegible]!~~ נראה [illegible] ~~[illegible]~~

~~$f'(x,z)$ [illegible] $\frac{\varepsilon}{2^{\ell}}$ [illegible]~~

ואז: M' תריץ את M עד כיוון $\frac{\varepsilon}{2^{\ell}}$. ותוציא את $\left[M(x,y)-\frac{\varepsilon}{2^{\ell}}\varepsilon\right]$.

~~[illegible] $M(x,y,z)$ [illegible] $\frac{\varepsilon}{2^{\ell}}$~~

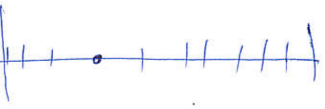
~~ולכן $M(x,y,z)$ [illegible] $f'(x,z)$~~

~~ולכן $[M(x,y,z)]=[f(x,z)]$.~~

עבור תכונה 2

2 אם ל x, אז $f'(x,s)$ רחוק לפחות $\frac{\varepsilon}{2^k}$

תמונה:



זה קורה בהסת. לפחות $\frac{1}{2}$.

עבור s טוב ל x,

כמעט לכל y (חוץ אולי מחלק s)

$|M(x,y)-f(x)| \le \frac{\varepsilon}{2^\lambda}$

ואז $|M'(x,y,s)-f'(x,s)| \le \frac{\varepsilon}{2^\lambda}$

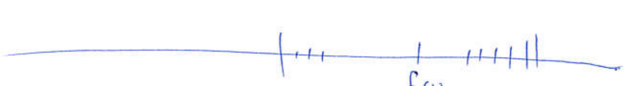
ואם (כיון ש $f'(x,s)$ לפחות $\frac{\varepsilon}{2^\lambda}$ מהקצה)

$M'(x,y,s)$ ו $f'(x,s)$ באותו התחום

ואז $[f'(x,s)] = [M'(x,y,s)]$.

צריך עוד לחשוב על זה: $f(x)$ קבוע.

חלק- המלים ~~של~~-נקודה הדגמה של



פת 3:

· נבחר א' $s_1 \dots s_{\sqrt{\lg n}}$, $s_i \in \{0,1\}^{O(\lg n)}$ לשאו בשגרה הב'.

נבחר ב' $I = h_1 \dots h_{\sqrt{\lg n}}$

משפט:

$$M^{(i+1)} = M\left(\left[A\left(M^{(i)}_{h_1 \dots h_{\sqrt{\lg n}}} \right) \right]_{s_i} \right)$$

כל כניסה במטריצה ($O(n^4)$ כניסות)
poly(n)

לאחר הכפלה shift & truncate את s_i .

ב) סיבוכיות הזכרון:

הזכרון $\left[A\left(M^{(i)}_{I} \right) \right]_{s_i}$

מצבר (ע"י הכפלה דצברון $(O(\lg n))$

יש מטריצה $M^{(i+1)}$: הזכרון $\sum_{\sigma \in \Sigma} |M_\sigma|$

שולחים לו המטריצה על ה M_Σ שמשתל $p = \frac{\sigma}{|\Sigma|}$ מעק.

אלגוריתם גם יפתרו לחשב ב $O(\log n)$

את $G(x, h)$ בהינתן $x, \bar{h}$. $x \in [M]$

ורק אפשר לחשב את $A^{(m+1)}_{\bar{h}}[i,j]$.

ע"י סריקה של כמה $x \in [M]$ מוצאים את i ו- j ש- (x,h)

ואז ניתן לחשב את $A(M^{(i+1)}_{h})$ ב $O(\log n)$

ולכן גם את $[A(M^{(i+1)}_{\bar{h}})]_{S_{i+1}}$ "

ובסה"כ $\sqrt{\log n}$ רמות, כ"א $O(\log n)$ בערך

שזה $O(\log n \sqrt{\log n})$ בערך.

③ עבור סדרה z יחידה - <u>נקבע את הסדרה z</u>

ועבור h יחיד, הקרוב אחרי הפעלת truncate + shift נותן

בדיוק את הסדרה $B_0, B_1, \ldots$

<u>מה קורה?</u>

① $G(x, h, h)$ לא <u>עובדת</u>

המבנה M_h מאוד תלוי ב- h.

② אבל ל- M_h יש <u>ייצוג קנוני</u> $M(A(M_h))$

שהוא מאוד קרוב ל- A^2, ולכן כמעט ולא תלוי ב- h

ואחרי truncate + shift — כבר לא תלוי ב- h.

המחיר על ייצוג קנוני, הוא בעצם שלב צריך לעבור לחשב

את המטריצה ולהעביר מטריצה חדשה.

המינימום מושג ב- $h_1, \ldots, h_{\sqrt{n}}$ וחישוב דומה

והעבודה היא $O(\log n \cdot \sqrt{\log n})$

ה) נכונה!

נגדיר את המטריצות

$$B_0 = A$$

$$B_1 = \left[A^{\left(2^{\sqrt{\lg n}}\right)}\right]_{s_1}$$

$$B_{i+1} = \left[B_i^{\left(2^{\sqrt{\lg n}}\right)}\right]_{s_{i+1}}$$

1) $$\| B_{\sqrt{\lg n}} - A^n \|_{row} \le \frac{1}{poly(n)}$$

2) s_1 אקראי, אחוז מ הביטים ב $A^{2^{\sqrt{\lg n}}}$ רחוקים מעיגול.

s_2 " " " " $B_1^{2^{\sqrt{\lg n}}}$ " "

במעט כל $\bar{s}$ אקראי.

3) נגדיר את המכונה $N_i = M(B_i)$ [פה שאלה 2 !]

$N_0 \ldots N_{\sqrt{\lg n}}$ קבועת מרחב

במעט כל $\bar{s}$ אקראי יחזיר את מצב.