סיבוכיות - תרגול

אלגוריתמים הסתברותיים.

תרגיל: המחלקה MA מוגדרת באופן אנלוגי ל- NP כאשר המודל הוא מ"ט הסתברותית.

נגדיר את המחלקה $MA_{2/3,1/3}$ להיות המחלקה שמכילה את השפות L כך שקיימת מ"ט הסתברותית M הרצה בזמן פולינומי, ומתקיים:

$$x\in L \Rightarrow \exists y \; Pr_r[M(x,y,r)=1]\geq \frac{2}{3}$$

$$x\notin L \Rightarrow \forall y \; Pr_r[M(x,y,r)=1]\leq \frac{1}{3}$$

כאשר אורך y חסום פולינומית ב- x.

באופן דומה, נגדיר את המחלקה $MA_{1,\frac{1}{3}}$ להיות המחלקה המכילה את השפות L כך שקיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומתקיים:

$$x\in L \Rightarrow \exists y \; Pr_r[M(x,y,r)=1]=1$$

$$x\notin L \Rightarrow \forall y \; Pr_r[M(x,y,r)=1]\leq \frac{1}{3}$$

הוכיחו כי $MA_{1,1/3}=MA_{2/3,1/3}$.

<u>הוכחה</u>-

כיוון אחד ברור, נראה כי אם $L\in MA_{2/3,1/3} \Rightarrow L\in MA_{1,1/3}$.

אם $L\in MA_{2/3,1/3}$ אזי קיים מודל הסתברותי כזה V כך ש-

$$x\in L \Rightarrow \exists y \; Pr_r[M(x,y,r)=1]\geq \frac{2}{3}$$

$$x\notin L \Rightarrow \forall y \; Pr_r[M(x,y,r)=1]\leq \frac{1}{3}$$

ע"י הרצות חוזרות וקחת רוב, ניתן לקבל מודל שמשתמש ב- $n^{O(1)}$ מטבעות רנדומיים והסתברות השגיאה היא $\frac{1}{2^n}$ (לפי חסם צ'רנוף)

בדומה להוכחה מהרצאה ש- $BPP\subseteq\Sigma_2$, ניתן להראות שאם $x\in L$ אזי קיימת $k=poly(n)$ מחרוזות $r_1,r_2,\dots,r_k$ באורך פולינומי m (קטן מ- k) כך ש-

$$\forall r_0 \; \exists i\in\{1,2,\dots,k\} \text{ s.t. } V^*(x,y,r_0\oplus r_i)=1$$

מדוע?

ההוכחה באמצעות "שיטת הסתברות". עבור $x\in L$ ניתן להראות כי: (כאשר r הוא שרשור כל המחרוזות r_i עבור $i>0$).

$$(*) \quad Pr_r\left[\forall r_0 \left(\bigvee_{i=1}^{k} V^*(x,y,r_0\oplus r_i)\right)=1\right]\geq\frac{1}{2}$$

נוכיח כאן באינדוקציה.

בס"ד

← הרעיון בשטח ההסתברותי הוא להראות שמשהו קרוב קיים, אבל ולהראות גם בדומה ההסתברותי כאשר ההסתברות שלו ל- 0 קצרה ~~ההסתברות~~ הישרדים ההסתברותיים.

כדי להוכיח את ⊕ מתקיים הקדם נסתכל בהסתברות לאורך המשלים:

$$Pr_r[\exists r_0 (\bigvee_{i=1}^{k} V^*(x,y,r_0 \oplus r_i)) = 0]$$

לפי חסם האיחוד, ההסתברות הנ"ל קטנה שווה מ-

$$\leq \sum_{r_0 \in \{0,1\}^m} Pr_r[(\bigvee_{i=1}^{k} V^*(x,y,r_0 \oplus r_i) = 0)] = \sum_{r_0 \in \{0,1\}^m} Pr_r[\bigwedge_{i=1}^{k} (V^*(x,y,r_0 \oplus r_i) = 0)]$$

נשים ♥ שהמאורעות שאנו מעשים בינהם "חסם" הם בת"ל ולכן ההסתברות הנ"ל שווה ל:

$$= \sum_{r_0 \in \{0,1\}^m} \prod_{i=1}^{k} Pr_r[V^*(x,y,r_0 \oplus r_i) = 0] \leq \sum_{r_0 \in \{0,1\}^m} \prod_{i=1}^{k} \frac{1}{2^m} = \sum_{r_0 \in \{0,1\}^m} \left(\frac{1}{2^n}\right)^k = 2^m \cdot \frac{1}{2^{nk}} < \frac{1}{2}$$

כי הרחנו את m קטן מ- k.

~~לאחר הכפלת שקלול~~

לכן נניח לרגע מודל V' שמקבל את x ו- $y' = \overbrace{y \cdot r_1 \cdot r_2 \cdots r_k}^{\text{שרשור של } y \text{ עם } k \text{ המחרוזות.}}$ ומחרוזת רנדומית r_0

ומדגם הבדל של $V^*(x,y,r_0 \oplus r_i)$ אם באחת ההרצות V^* החזיר 1, V' יחזיר 1.

אחרת V' מחזיר 0.

עבור $x \in L$ הוכחנו לעיל שבהכרח עבור i מסוים $V^*(x,y,r_0 \oplus r_i)$ יחזיר 1 ולכן V'

מחזיר 1 בהסתברות 1 עבור y'.

עבור $x \notin L$ הגרף $r_0 \oplus r_i$ הוא רנדומי לכל i כיוון ש- r_0 רנדומי.

$$Pr_r[V^*(x,y,r_0 \oplus r_i) = 1] \leq \frac{1}{2^n}$$

ולכן, נקבל שההסתברות ש- V' יחזיר 1 במקרה זה הוא:

$$Pr_r[V^*(x,y,r_0 \oplus r_i) = 1 \text{ for some } i] \leq k \cdot \frac{1}{2^n} < \frac{1}{3}$$

□

~~$\exists r_0 \; \exists i \in \{1,2,\dots,k\} \; s.t. \; V^*(x,y,r_0 \oplus r_i) = 1$~~

תרגיל: הוכיחו $P^{\#P} \subseteq PSPACE$

הוכחה-

$L \in P^{\#P}$ ולכן קיימת מכונה M בעלת גישה אורקל לפונק' $f_R \in \#P$ המכריעה את L

בזמן פולינומי.

נבנה מכונה 'M אשר בהינתן x, עם גישה לאורקל עם מחרוזת a_i, האורקל יחזיר לנו

את מספר ה- y-ים המתאימים לאות a_i, כאשר $R(a_i,y)$. כאשר עם a_i ועם y

חסומים פולינומית ב- x ולכן נעבור על כל $y \in \{0,1\}^{p(|x|)}$ ונשמור מונה שיראה כמה יהיה פולי.