סיבוכיות- תרגול 10

<u>תזכורת:</u> לכל פונקציה $s(n) \geq \log n$ ולכל $c \in \mathbb{N}$ מתקיים $DSPACE(s(n)^c) \subset DSPACE(s(n)^{c+1})$.

<u>תרגיל:</u> הוכיחו כי $P \neq DSPACE(n)$.

<u>פתרון:</u> נניח בשלילה כי $P = DSPACE(n)$ ונראה כי $DSPACE(n^2) \subseteq DSPACE(n)$ בסתירה למשפט היררכית המקום. תהי $S \in DSPACE(n^2)$. לכן קיימת מ"ט M המכריעה את S תוך שימוש בלכל היותר $O(n^2)$ מקום.

נגדיר שפה חדשה $S' = \left\{x10^{|x|^2} \mid x \in S\right\}$. נשים לב כי $S' \in DSPACE(n)$, כי בהנתן קלט y, ניתן לבדוק אם הוא מהצורה $y = x10^{|x|^2}$, ואם כן, לסמלץ את את $M(x)$ ולהחזיר את תשובתה. המקום הנדרש סה"כ הוא $O(|x|^2) = O(|y|)$.

לפי ההנחה, מתקיים כי $S' \in P$. לכן קיימת מ"ט פולינומית M' המכריעה את S'. כעת, נראה כי $S \in P$. נבנה מ"ט M'' הפועלת באופן הבא: בהנתן קלט x, M'' יוצרת את המחרוזת $y = x10^{|x|^2}$ ומסמלצת את $M'(y)$. זמן הריצה של M'' פולינומי ב-$|y| = O(|x|^2)$ ולכן גם פולינומי ב-$|x|$. לכן $S \in P$.

לפי ההנחה נקבל כי $S \in DSPACE(n)$. כלומר, $DSPACE(n^2) \subseteq DSPACE(n)$ בסתירה.

אלגוריתמים רנדומיים

שתי הגדרות שקולות למ"ט הסתברותית:

1) מודל אונליין- מ"ט ל"ד, כך שבכל מעבר שאינו מוגדר באופן יחיד, המכונה מטילה מטבע ובהסתברות שווה בוחרת אחת מהאפשרויות.
2) מודל אופליין- מ"ט דטר' המקבלת קלט נוסף, שהוא סדרת הטלות מטבע אקראיות.

טעות חד-כיוונית

<u>הגדרה:</u> נאמר כי בעית הכרעה S שייכת למחלקה RP אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומקיימת:

$$x \in S \Longrightarrow \Pr[M(x) = 1] \geq 1\backslash 2$$

$$x \notin S \Longrightarrow \Pr[M(x) = 0] = 1$$

<u>הגדרה:</u> נאמר כי בעית הכרעה S שייכת למחלקה $coRP$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומקיימת:

$$x \in S \Longrightarrow \Pr[M(x) = 1] = 1$$

$$x \notin S \Longrightarrow \Pr[M(x) = 0] \geq 1/2$$

טעות דו-כיוונית

<u>הגדרה:</u> נאמר כי בעית הכרעה S שייכת למחלקה BPP אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומקיימת:

$$\forall x, \Pr[M(x) = \chi_S(x)] \geq 2/3$$

הערות

- ניתן להקטין את ההסתברות לטעות (בכל המחלקות הנ"ל) ל-$\frac{1}{2^{p(|x|)}}$ עבור כל פולינום p.
- $RP \subseteq NP$.
- $RP \subseteq BPP$.
- היחס בין BPP ל-NP לא ידוע.
- $BPP \subseteq PSPACE$.

דוגמה לאלגוריתם הסתברותי

נגדיר את השפה הבאה:

MAT-VERIFY = $\{(A,B,C)$ | A,B,C הן מטריצות בגודל $n{\times}n$ המקיימות $A \cdot B = C\}$.

ניתן להכריע את השפה באופן נאיבי בזמן $O(n^3)$. נראה אלגוריתם הסתברותי פשוט הרץ בזמן $O(n^2)$ ומראה כי MAT-VERIFY $\in coRP$. האלגוריתם יפעל באופן הבא:

בהנתן קלט (A,B,C), נבחר באקראי וקטור $r \in \{0,1\}^n$, נחשב את $\big(A\cdot(Br)\big)$ ואת Cr ונחזיר 1 אם הם שווים.

עבור קלטים בשפה מתקיים $A \cdot B = C$, ולכן $\big(A\cdot(Br)\big) = (A\cdot B)r = Cr$ והאלגוריתם תמיד יחזיר 1.

עבור קלטים שלא בשפה מתקיים $A \cdot B \neq C$. נחשב את ההסתברות לטעות. נסמן $D = A\cdot B - C$, ונשים לב כי האלגוריתם טועה אם"ם מתקיים $Dr = 0$. מכיוון ש-$AB \neq C$, אזי $D \neq 0$, ולכן קיים $d_{ij} \neq 0$. נניח בה"כ כי $d_{11} \neq 0$.

$$\Pr[Dr = 0 | D \neq 0] \le \Pr[(Dr)_1 = 0 | d_{11} \neq 0] = \Pr[(d_{11}, \dots d_{1n})(r_1, \dots, r_n) = 0 | d_{11} \neq 0] =$$

$$\Pr[d_{11}r_1 + \cdots + d_{1n}r_n = 0 | d_{11} \neq 0] = \Pr[d_{11}r_1 = -(d_{12}r_2 + \cdots + d_{1n}r_n) | d_{11} \neq 0] =$$

$$\Pr\left[r_1 = -\frac{d_{12}r_2 + \cdots + d_{1n}r_n}{d_{11}} | d_{11} \neq 0\right] \le \frac{1}{2}$$

אי-השיוויון האחרון נכון כי אחרי שבחרנו את $r_2, \dots, r_n$, הערך בצד ימין נקבע והוא או 0 או 1 או משהו אחר. אם הערך הנ"ל אינו 0 או 1, אז ההסתברות הנ"ל שווה 0, אחרת היא ½.