סיבוכיות- תרגול 11

תרגיל: הוכיחו כי אם $NP \subseteq BPP$ אזי $NP \subseteq RP$.

פתרון: נניח כי $NP \subseteq BPP$, ובפרט $SAT \in BPP$. נראה כי $SAT \in RP$.

$SAT \in BPP$, ולכן קיימת מ"ט פולינומית הסתברותית M כך שלכל x:

$$\Pr[M(x) = \chi_{SAT}(x)] \geq 2/3$$

ראינו כי ניתן להקטין את הסתברות השגיאה, כלומר, קיימת מ"ט פולינומית הסתברותית M^* כך שלכל x:

$$\Pr[M^*(x) = \chi_{SAT}(x)] \geq 1 - \frac{1}{2(n+1)}$$

נראה מ"ט פולינומית הסתברותית N המכריעה את SAT לפי הדרישות של RP. כלומר, נרצה שעבור קלטים שלא בשפה, N תמיד תדחה, ועבור קלטים בשפה, N תאשר בהסתברות לפחות ½. הרעיון יהיה לבצע רדוקציה עצמית ל-SAT ע"י שימוש במכונה M^* בתור המכונה המכריעה את SAT.

$N(\phi)$:

1. אם $M^*(\phi)$ החזירה 0- החזר 0.
2. נסמן ב-n את מספר המשתנים ב-ϕ.
3. עבור i מ-1 עד n:
   a. הצב $x_i \leftarrow T$ וצמצם את ϕ ל-ϕ_T.
   b. אם $M^*(\phi_T) = 1$ המשך עם ϕ_T.
   c. אחרת, הצב $x_i \leftarrow F$, צמצם את ϕ ל-ϕ_F והמשך עם ϕ_F.
4. בדוק אם השמת האמת $x_1, \ldots, x_n$ שהתקבלה מספקת את ϕ המקורית. אם כן החזר 1, אחרת החזר 0.

אם $\phi \notin SAT$, לא קיימת השמת אמת המספקת את ϕ ולכן N תמיד תחזיר 0.

אם $\phi \in SAT$, קיימת השמת אמת המספקת את ϕ. נשים לב כי אם M^* החזירה תשובה נכונה בכל הקריאות ש-N קראה לה, אז N תמצא השמה מספקת ותחזיר 1. לכן, ההסתברות ש-N טועה חסומה ע"י ההסתברות שלפחות אחת מתוך $n+1$ הקריאות ל-M^* החזירה תשובה לא נכונה. הסתברות לטעות בכל קריאה כזאת היא לכל היותר $\frac{1}{2(n+1)}$, ולכן:

$$\Pr[N(\phi) = 0] \leq (n+1) \cdot \frac{1}{2(n+1)} = \frac{1}{2}$$

קיבלנו כי N עומדת בדרישות של RP, ולכן $SAT \in RP$. מכיוון ש-SAT היא NP-שלמה, קיבלנו כי $NP \subseteq RP$.

הגדרה: נגדיר את המחלקה ZPP באופן הבא: נאמר כי $S \in ZPP$ אם קיימת מ"ט הסתברותית פולינומית M כך שלכל x:

1. $\Pr[M(x) = \chi_S(x)] \geq 1/2$.
2. $\Pr[M(x) \in \{\chi_S(x), \perp\}] = 1$.

תרגיל: הוכיחו כי $ZPP = RP \cap coRP$.

פתרון:

($\subseteq$): תהי $S \in ZPP$. כלומר, קיימת מ"ט הסתברותית פולינומית M העונה על דרישות ZPP. נגדיר את המכונה N באופן הבא: בהנתן קלט x, N תסמלץ את $M(x)$. אם $M(x)$ החזירה 1, N תחזיר 1, אחרת תחזיר 0. מתקיים כי:

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

$$x \notin S \Longrightarrow \Pr[N(x) = 0] = \Pr[M(x) \neq 1] = \Pr[M(x) \in \{0, \perp\}] = 1$$

N עונה לדרישות של RP ולכן $S \in RP$.

באופן דומה ניתן להגדיר מכונה N' שתחזיר 0 אמ"ם M מחזירה 0. ניתוח דומה יראה כי N' עונה לדרישות של $coRP$, ולכן $S \in coRP$.

סה"כ קיבלנו כי $ZPP \subseteq RP \cap coRP$.

($\supseteq$): תהי $S \in RP \cap coRP$. כלומר, קיימות מ"ט M, M' המכריעות את S לפי הדרישות של RP ו-$coRP$ בהתאמה. נגדיר את המכונה N באופן הבא:

<u>$N(x)$:</u>

1. הרץ את $M(x)$ ואם החזירה 1- החזר 1.
2. הרץ את $M'(x)$ ואם החזירה 0- החזר 0.
3. החזר $\perp$.

נשים לב כי N אף פעם לא מחזירה תשובה לא נכונה, ולכן תנאי 2 של ZPP מתקיים.

בנוסף, עבור $x \in S$ מתקיים $\Pr[N(x) = 1] = \Pr[M(x) = 1] \geq 1/2$, ועבור $x \notin S$ מתקיים

$$\Pr[N(x) = 0] = \Pr[M(x) = 0 \wedge M'(x) = 0] \geq 1/2$$

סה"כ $\Pr[N(x) = \chi_S(x)] \geq 1/2$. קיבלנו כי N עונה לדרישות של ZPP ולכן $S \in ZPP$.

<u>תרגיל:</u> הוכיחו כי $S \in ZPP$ אמ"ם קיימת מ"ט הסתברותית M המקיימת $\Pr[M(x) = \chi_S(x)] = 1$ ותוחלת זמן הריצה שלה פולינומית.

<u>פתרון:</u>

($\Longleftarrow$): תהי $S \in ZPP$. כלומר, קיימת מ"ט הסתברותית M העונה לדרישות של ZPP. נגדיר מכונה N שתריץ את M שוב ושוב עד שתחזיר תשובה שאינה $\perp$. ברור כי N בסופו של דבר תחזיר תשובה נכונה. נסמן במשתנה המקרי T את מספר הפעמים ש-N מריצה את M. נחשב את התוחלת של T:

$$\mathbb{E}[T] = \sum_{t=1}^{\infty} t \cdot \Pr[T = t] = \sum_{t=1}^{\infty} \Pr[T \geq t] \leq \sum_{t=1}^{\infty} \left(\frac{1}{2}\right)^{t-1} \leq 2$$

לכן, תוחלת זמן הריצה של N הוא פי 2 מזמן הריצה של M, ובפרט פולינומי.

($\Longrightarrow$): תהי M מ"ט הסתברותית המקיימת $\Pr[M(x) = \chi_S(x)] = 1$, ותוחלת זמן הריצה שלה $p(|x|)$ עבור פולינום p כלשהו. נגדיר מכונה N שתריץ את M למשך $2p(|x|)$ צעדים. אם החזירה תשובה, תחזיר את תשובתה, אחרת תחזיר $\perp$. ברור כי $\Pr[N(x) \in \{\chi_S(x), \perp\}] = 1$. נסמן במשתנה המקרי T את מס' הצעדים ש-M מבצעת על קלט x. מתקיים כי $\mathbb{E}[T] = p(|x|)$, ולכן לפי אי-שיוויון מרקוב:

$$\Pr[N(x) = \perp] = \Pr[M(x) \text{ doesn't halt in } 2p(|x|) \text{ steps}] = \Pr\big[T > 2\mathbb{E}[T]\big] \leq 1/2$$