בס״ד

<u>תרגול השלמה</u>

<u>תרגיל</u>

הוכיחו שאם $NP\subseteq BPP$ אזי $NP=RP$.

<u>פתרון</u>

הכיוון הראשון - $RP\subseteq NP$ מתקיים תמיד, והוכח בהרצאה. נראה שאם $NP\subseteq BPP$ אזי $NP\subseteq RP$.

נניח ש-$NP\subseteq BPP$ בפרט $SAT\in BPP$. כלומר, קיימת מ״ט פולינומית הסתברותית M' המכריעה את SAT, כך שמתקיים לכל x:

$$Pr_r[M'(x,r)=\chi SAT(x)]\geq 2/3$$

ע״י מספר פולינומי של הרצות ובחירת רוב נקטין את ההסתברות לטעות, ונקבל מכונה M כך שמתקיים לכל x:

$$Pr_r[M(x,r)=\chi SAT(x)]\geq 1-1/4n$$

כעת, נראה מכונה הסתברותית M^* המכריעה את SAT בדרישות ההסתברות של RP. בהינתן קלט ϕ ומחרוזת רנדומית $r=(r_1,r_2,\dots,r_{n+1})$ המכונה M^* תפעל באופן הבא:

1. בדוק האם $M(\phi,r_1)=0$, אם כן – החזר 0.
2. אחרת
   a. עבור כל משתנה v_i בנוסחה:
      i. הצב 0 במשתנה v_i וצמצם את ϕ ל-ϕ_0.
      ii. אם $M(\phi_0,r_{i+1})=1$ – המשך עם ϕ_0.
      iii. אחרת – הצב 1 במשתנה v_i וצמצם את ϕ ל-ϕ_1. המשך עם ϕ_1.

   b. הצב את השמת האמת שהתקבלה מהשלב הקודם בנוסחה המקורית ובדוק אם השמה זו מספקת את ϕ. אם כן – החזר 1, אחרת – החזר 0.

אם $\phi\notin SAT$, אז מכיוון ש-M^* בודקת עבור כל השמת אמת שהתקבלה האם היא מספקת את ϕ, בהכרח ש-M^* תחזיר 0, כיוון שזו נוסחה שאינה ניתנת לסיפוק.

אם $\phi\in SAT$, אז אם כל אחת מ-$n+1$ הקריאות ל-M החזירה תשובה נכונה, M^* תמצא השמת אמת שמספקת את ϕ, ולכן תחזיר 1. לכן ההסתברות ש-M^* תחזיר תשובה שגויה חסומה ע״י ההסתברות שלפחות אחת מתוך $n+1$ ההרצות של M החזירה תשובה שגויה. ההסתברות לטעות של M היא לכל היותר $1/4n$, ולכן ההסתברות של טעות בהרצה כלשהי מבין $n+1$ ההרצות חסומה ע״י $(n+1)/4n\leq 1/2$.

לכן קיבלנו:

$\phi \in SAT \Rightarrow Pr_r[M^*(\phi,r)=1] \geq 1/2$

$\phi \notin SAT \Rightarrow Pr_r[M^*(\phi,r)=0] = 1$

קיבלנו אם כן ש-$SAT \in RP$, ומכיוון ש- SAT היא NP-שלמה, הרי ש-$NP \subseteq RP$ כנדרש.

<u>תרגיל</u>

המחלקה ZPP

<u>הגדרה 1</u>:

$L \in ZPP$ אם קיימת מ״ט הסתברותית פולינומית M כך שמתקיים:

$\forall x: Pr_r[M(x,r)=\perp] \leq 1/2$

$\forall x: Pr_r[M(x,r)=\chi_L(x) \text{ or } M(x,r)=\perp] = 1$

<u>הגדרה 2</u>:

$L \in ZPP$ אם קיימת מ״ט הסתברותית M המחזירה תמיד את התשובה הנכונה (0 או 1), ותוחלת זמן הריצה שלה פולינומית.

<u>הגדרה 3</u>:

$ZPP=RP \cap co\text{-}RP$

משפט: כל ההגדרות של ZPP שקולות.

שקילות הגדרות 1 ו-2:

($1 \Rightarrow 2$) תהי $L \in ZPP$ לפי הגדרה 1. כלומר, קיימת מ״ט פולינומית הסתברותית M המקיימת את ההסתברויות של הגדרה 1. נניח שהחסם על זמן הריצה של M הוא פולינום $p(\cdot)$. נבנה מ״ט M' שתריץ את M שוב ושוב עד לקבלת תשובה שונה מ-$\perp$ שתוחזר כפלט. ברור ש-M' תמיד מחזירה את התשובה הנכונה. מס׳ הפעמים ש-M' תריץ את M עד לקבלת תשובה שאינה $\perp$ הוא משתנה גאומטרי עם פרמטר $p \geq 1/2$. לכן תוחלת מס׳ ההרצות של M תהיה לכל היותר 2 $(1/p)$. מכאן שתוחלת זמן הריצה של M' היא לכל היותר $2p(n)$ עבור קלט באורך n – כלומר, תוחלת זמן ריצה פולינומית.

($2 \Rightarrow 1$) תהי $L \in ZPP$ לפי הגדרה 2. כלומר, קיימת מ״ט הסתברותית M הרצה בתוחלת זמן פולינומית. נניח שתוחלת זמן הריצה של M חסומה ע״י הפולינום $p(\cdot)$. נבנה מכונה M' שתריץ את M למשך $2p(n)$ צעדים עבור קלט באורך n. אם M לא השלימה את ריצתה M' תחזיר $\perp$, אחרת M' תחזיר את מה ש-M מחזירה. ברור אם כן שזמן הריצה של M הוא פולינומי והיא תמיד מחזירה תשובה נכונה או $\perp$. נסמן במשתנה המקרי X את מס׳ הצעדים של המכונה M עם קלט x (באורך n) ומחרוזת רנדומית r ונקבל ע״פ אי-שיוויון מרקוב:

$$Pr[M'(x,r)=\perp]=Pr[M(x,r) \text{ does not halt after } 2p(n)] = Pr[X \geq 2p(n)] \leq E[X]/2p(n) = p(n)/2p(n) = 1/2$$

שקילות הגדרות 1 ו-3 :

$3 \Rightarrow 1$) תהי $L \in ZPP$ לפי הגדרה 1. כלומר, קיימת מ״ט פולינומית הסתברותית M המקיימת את ההסתברויות של הגדרה 1. נבנה מכונה 'M שתריץ את המכונה M ובמידה וזו החזירה $\perp$ המכונה תחזיר 0, אחרת היא תחזיר את מה ש-M מחזירה. מתקיים שעבור $x \notin L$ המכונה תחזיר תמיד 0 (בין אם M החזירה 0 ובין אם החזירה $\perp$), ועבור $x \in L$ המכונה תחזיר 1 בהסתברות 1/2 לכל הפחות, שכן M מחזירה $\perp$ בלכל היותר הסתברות 1/2, ובכל מקרה אחר תוחזר התשובה הנכונה. כלומר המכונה 'M מכריעה את L בהסתברויות של RP. באופן דומה ניתן ליצור מכונה ''M שתריץ את המכונה M ובמידה וזו החזירה $\perp$ המכונה תחזיר 1, אחרת היא תחזיר את מה ש-M מחזירה. ניתוח דומה למה שהצגנו יראה כי ''M מכריעה את L בהסתברויות של co-RP ולכן $L \in RP \cap co\text{-}RP$.

$1 \Rightarrow 3$) תהי $L \in RP \cap co\text{-}RP$. כלומר, קיימת מ״ט פולינומית הסתברותית M המכריעה את L בהסתברויות של RP וקיימת מ״ט הסתברותית 'M המכריעה את L בהסתברויות של co-RP. נבנה מ״ט ''M שתריץ את המכונה M על הקלט שלה עם חצי מהביטים של המחרוזת r ובמידה וזו החזירה 1 ''M תחזיר 1. לאחר מכן (אם טרם הוחזרה תשובה), ''M תריץ את המכונה M על הקלט שלה עם החצי השני של הביטים של המחרוזת r ובמידה וזו החזירה 0 ''M תחזיר 0. אם ''M לא החזירה תשובה עד כה היא תחזיר $\perp$.

מתקיים שאם M החזירה 1 בוודאות $x \in L$, ואילו אם 'M החזירה 0 בוודאות $x \notin L$. לכן ''M לא תחזיר לעולם תשובה שגויה.

בנוסף, אם $x \in L$ M תחזיר 1 בהסתברות לפחות 1/2. ואם $x \notin L$ אז 'M תחזיר 0 בהסתברות לפחות 1/2. כלומר, בהסתברות לפחות 1/2 ''M תחזיר תשובה החלטית כלשהי, ולכן ההסתברות שיוחזר $\perp$ היא לכל היותר 1/2.

<u>תרגיל</u>

המחלקה MA מוגדרת באופן אנלוגי ל-NP כאשר המוודא הוא מ״ט פולינומית **הסתברותית**.

נגדיר את המחלקה $MA_{2/3,1/3}$ להיות המחלקה שמכילה את השפות L כך שמתקיים :

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

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

(האורך של y חסום פולינומית באורך x).

באופן דומה נגדיר את המחלקה $MA_{1,1/3}$ להיות המחלקה שמכילה את השפות L כך שמתקיים :

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

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

הוכיחו כי $MA_{1,1/3} = MA_{2/3,1/3}$