סיבוכיות- תרגול 6

תרגיל: נאמר כי בעית הכרעה S היא PH-שלמה אם:

1) $S \in PH$.
2) לכל $S' \in PH$ מתקיים $S' \leq_m^p S$.

הוכיחו כי אם קיימת שפה PH-שלמה, אזי קיים k עבורו $PH \subseteq \Sigma_k$.

פתרון: תהי S שפה PH-שלמה. $S \in PH$ ולכן, לפי הגדרה, קיים k כך ש-$S \in \Sigma_k$. לכן, קיימים פולינום p ואלגוריתם פולינומי דטר' V המקיימים:

$$x \in S \Leftrightarrow \exists y_1 \forall y_2 \dots Q y_k, \forall i \; |y_i| \leq p(|x|), V(x, y_1, y_2, \dots, y_k) = 1$$

תהי $S' \in PH$. קיימת פונקציה f חשיבה בזמן פולינומי כך ש-$x \in S' \Leftrightarrow f(x) \in S$. נגדיר את הפולינום $q = p \cdot p'$, עבור p' הפולינום החוסם את זמן ריצת המכונה המחשבת את f, ונגדיר $V'(x, y_1, \dots, y_k) = V(f(x), y_1, \dots, y_k)$. זהו אלגוריתם דטר' פולינומי, ומתקיים:

$$x \in S' \Leftrightarrow f(x) \in S \Leftrightarrow \exists y_1 \forall y_2 \dots Q y_k, \forall i \; |y_i| \leq p(|f(x)|) \leq q(|x|), V'(x, y_1, y_2, \dots, y_k) = 1$$

לכן $S' \in \Sigma_k$.

תרגיל: הוכיחו כי $NP^{PH} \subseteq PH$.

פתרון: תהי $S \in NP^{PH}$. לכן, קיימת מ"ט ל"ד פולונימות M^A עם גישת אורקל ל-$A \in PH$ המכריעה את S. $A \in PH$ ולכן קיים k כך ש-$A \in \Sigma_k$. כלומר, $S \in NP^{\Sigma_k}$. לפי משפט $NP^{\Sigma_k} = \Sigma_{k+1} \in PH$, ולכן $S \in PH$.

תרגיל: הוכיחו בעזרת מכונות אורקל ל"ד כי אם $\mathrm{NP} = \mathrm{coNP}$ אזי $\mathrm{NP}^{\mathrm{NP}} = \mathrm{NP}$.

פתרון: ההכלה $\mathrm{NP} \subseteq \mathrm{NP}^{\mathrm{NP}}$ ברורה. נוכיח את הכיוון השני. תהי $S \in \mathrm{NP}^{\mathrm{NP}}$. קיימת מ"ט ל"ד פולינומית M^A עם גישת אורקל לבעית הכרעה $A \in NP$ המכריעה את S.

$A \in NP$ ולכן קיימת מ"ט ל"ד פולינומית M' המכריעה את A. בנוסף, הנחנו כי $NP = coNP$, ולכן גם $\bar{A} \in NP$. כלומר, קיימת מ"ט ל"ד פולינומית M'' המכריעה את $\bar{A}$.

נראה מ"ט ל"ד פולינומית M המכריעה את S. M תפעל בדיוק כמו M^A, פרט למקומות בהם M^A מבצעת שאילתא לאורקל שלה. עבור כל שאילתא מהצורה "$a \in A$?", M תסמלץ את $M'(a)$, אם החזירה 1, M תמשיך כמו ש-M^A הייתה ממשיכה אילו האורקל היה מחזיר 1. אחרת, M תסמלץ את $M''(a)$, אם החזירה 1, M תמשיך כמו ש-M^A הייתה ממשיכה אילו האורקל היה מחזיר 0. אחרת, M תחזיר 0 ותסיים.

הוכחת נכונות: ראשית, נשים לב כי בכל מקום ש-M^A שואלת את האורקל שאילתא מהצורה "$a \in A$?" וממשיכה לפי תשובת האורקל, קיים חישוב של M בו היא ממשיכה באותו אופן (כי אם $a \in A$, קיים חישוב של $M'(a)$ שמחזיר 1 ואז M תמשיך כפי ש-M^A הייתה ממשיכה, ואם $a \notin A$, בהכרח $M'(a) = 0$ וקיים חישוב של $M''(a)$ שמחזיר 1, ובמקרה זה M תמשיך כפי ש-M^A הייתה ממשיכה).

עבור $x \in S$, קיים חישוב של $M^A(x)$ שמסתיים במצב מקבל. נתבונן בחישוב של $M(x)$ בו היא בוחרת את אותן בחירות ל"ד של M^A, ובנוסף בכל מקום ש-M^A שואלת שאילתא לאורקל, M בוחרת בחישוב בו היא ממשיכה באותו אופן. במקרה זה M פועלת בדיוק כמו M^A ולכן מגיעה למצב מקבל.

עבור $x \notin S$, כל חישוב של $M^A(x)$ מחזיר 0. נבחין בין שני מקרים בחישוב של $M(x)$:

א. קיימת שאילתת אורקל של M^A, עבורה כש-M מסמלצת את המכונות M' ו-M'', שתיהן מחזירות 0. במקרה זה M מחזירה 0 ומסיימת.
ב. לכל שאילתת אורקל של M^A, בסימולציה ש-M מבצעת, אחת מהמכונות M' או M'' החזירו 1. במקרה זה, M פועלת בדיוק כפי ש-M^A הייתה פועלת ולכן תחזיר 0.

כלומר, קיבלנו שבכל חישוב של $M(x)$ היא מחזירה 0.

סה"כ M היא מ"ט ל"ד פולינומית המכריעה את S ולכן $S \in NP$.

<u>תרגיל:</u> תהי EXP מחלקת כל בעיות ההכרעה S כך שקיימת מ"ט דטר' המכריעה את S ועובדת בסיבוכיות זמן $O\left(2^{p(n)}\right)$ עבור פולינום $p(\cdot)$ כלשהו. הוכיחו כי $PH \subseteq EXP$.

<u>פתרון:</u> תהי $S \in PH$. כלומר, קיים k כך ש-$S \in \Sigma_k$. נסמן ב-p וב-V את הפולינום והמוודא המובטחים מהגדרת Σ_k. נגדיר מ"ט M המכריעה את S באופן הבא: M תעבור על כל האפשרויות עבור $y_1 \in \{0,1\}^{p(|x|)}, y_2 \in \{0,1\}^{p(|x|)}, \dots, y_k \in \{0,1\}^{p(|x|)}$ ותחזיר 1 אמ"ם $\exists y_1 \forall y_2 \dots Q y_k, V(x, y_1, \dots, y_k) = 1$.
ברור ש-M מכריעה את S, וזמן הריצה שלה הינו

$$\underbrace{2^{p(|x|)} \cdots 2^{p(|x|)}}_{k\ times} p'(|x|) \leq 2^{kp(|x|)p'(|x|)}$$

כאשר p' הינו הפולינום החוסם את זמן הריצה של V. זהו זמן אקספוננציאלי ולכן $S \in EXP$.