סיבוכיות- תרגול 5

<u>הסבר אינטואיטיבי (לא פורמלי):</u> במחלקה NP נמצאות בעיות מהצורה "קיים", ובמחלקה coNP נמצאות בעיות מהצורה "לכל" (=לא קיים). כלומר, ב-NP יש בעיות כך שקלט בשפה אם ורק אם **קיימת** לכך הוכחה קצרה, וב-coNP יש בעיות שקלט בשפה אם ורק אם **לא קיימת** לכך הפרכה קצרה.

<u>תזכורת:</u> $S \in \mathrm{NP}$ אם:

1) לקלטים בשפה קיימת הוכחה קצרה.
2) לקלטים שלא בשפה לא קיימת הוכחה.

<u>דוגמה:</u> $\mathrm{VC} = \{(G,k) \mid$ קיים ב-G כיסוי קודקודים בגודל $\leq k\} \in \mathrm{NP}$.

<u>תזכורת:</u> $S \in \mathrm{coNP}$ אם:

1) לקלטים בשפה לא קיימת הפרכה.
2) לקלטים שלא בשפה קיימת הפרכה קצרה.

<u>דוגמה:</u> $\overline{\mathrm{VC}} = \{(G,k) \mid$ כל כיסוי קודקודים ב-G בגודל $> k\} \in \mathrm{coNP}$.

[התרגול מתחיל מפה]

<u>תזכורת:</u>

$\mathrm{MIN\text{-}VC} = \{(G,k) \mid$ כיסוי הקודקודים המינימלי ב-G בגודל $k\} =$
$\{(G,k) \mid$ קיים ב-G כיסוי קודקודים בגודל $\leq k$ וגם כל כיסוי קודקודים ב-G בגודל $\geq k\} \in \Sigma_2$.

[NP לבד לא מספיק (כי לא ברור איך להגדיר הוכחה לכך שכל כיסוי קודקודים בגודל $\geq k$), ו-coNP לבד לא מספיק (כי לא ברור איך להגדיר הפרכה לכך שקיים כיסוי קודקודים בגודל $\leq k$).]

<u>הגדרה:</u> $S \in \Sigma_k$ אם קיימים פולינום p ואלגוריתם פולינומי V כך ש-

$$x \in S \Leftrightarrow \exists y_1 \forall y_2 \exists y_3, \dots Q y_k, \forall i |y_i| \leq p(|x|), V(x, y_1, y_2, \dots y_k) = 1$$

כאשר $Q = \exists$ אם k אי-זוגי, ו-$Q = \forall$ אם k זוגי.

<u>הגדרה:</u> $\Pi_k = \mathrm{co}\Sigma_k$. לפי זה, $S \in \Pi_k$ אם קיימים פולינום p ומוודא פולינומי V כך ש-

$$x \in S \Leftrightarrow \forall y_1 \exists y_2 \forall y_3, \dots Q y_k, \forall i |y_i| \leq p(|x|), V(x, y_1, y_2, \dots y_k) = 1$$

כאשר $Q = \forall$ אם k אי-זוגי, ו-$Q = \exists$ אם k זוגי.

<u>תכונות מיידיות:</u>

1. לפי ההגדרות הנ"ל: $\Sigma_0 = \Pi_0 = \mathrm{P}$. $\Sigma_1 = \mathrm{NP}$. $\Pi_1 = \mathrm{coNP}$.
2. $\Sigma_k \subseteq \Sigma_{k+1}$.
3. $\Sigma_k \subseteq \Pi_{k+1}$.
4. $\Pi_k \subseteq \Sigma_{k+1}$.

<u>הגדרה:</u> ההירככיה הפולינומית מוגדרת ע"י $\mathrm{PH} = \bigcup_{k=0}^{\infty} \Sigma_k$.

משערים שזו אכן היררכיה. כלומר, לכל $k \geq 0$ מתקיים $\Sigma_k \subset \Sigma_{k+1}$ (מוכל ממש).

<u>תרגיל:</u> הוכיחו כי השפה הבאה שייכת ל-Π_2.

MIN-CNF = $\{\phi$ | (ϕ בצורת CNF מינימלית (לא קיימת נוסחה קצרה יותר בצורת CNF השקולה ל-ϕ)$\}$.

<u>פתרון:</u> נשים לב ש-$\phi \in$ MIN-CNF אמ"ם מתקיימים התנאים הבאים:

1. ϕ בצורת CNF.
2. לכל ϕ' בצורת CNF, אם $|\phi'| < |\phi|$ אז קיימת השמת אמת v כך ש-$\phi(v) \neq \phi'(v)$.

נגדיר מוודא V המקבל (ϕ, ϕ', v) ומחזיר 1 אמ"ם מתקיימים שני התנאים הנ"ל. $|\phi'|$ ו-$|v|$ חסומים ע"י $|\phi|$, וכל הבדיקות מתבצעות בזמן פולינומי. לכן MIN-CNF $\in \Pi_2$.

<u>מכונות עם גישת אורקל</u>

<u>הגדרה:</u> מ"ט M עם גישת אורקל לשפה A (מסומנת M^A) היא מ"ט בעלת סרט נוסף המכונה "סרט אורקל". המכונה יכולה לכתוב על סרט האורקל מחרוזת x ולקבל תוך צעד אחד תשובה האם $x \in A$.

<u>הגדרה:</u> תהי A בעית הכרעה. נאמר כי $A \in P^B$ אם קיימת מ"ט דטר' פולינומית עם גישת אורקל לשפה B המכריעה את A. נאמר כי $A \in NP^B$ אם קיימת מ"ט ל"ד פולינומית עם גישת אורקל לשפה B המכריעה את A.

<u>הערה:</u> עבור בעיות הכרעה A, B מתקיים $A \in P^B \Leftrightarrow A \leq_T^p B$.

<u>הגדרה:</u> עבור מחלקה של בעיות הכרעה C, נגדיר $P^C = \bigcup_{A \in C} P^A$ ו-$NP^C = \bigcup_{A \in C} P^A$.

<u>משפט (מההרצאה):</u> לכל $k \geq 0$ מתקיים $\Sigma_{k+1} = NP^{\Sigma_k}$.

<u>תרגיל:</u> הוכיחו כי MIN-CNF $\in \Pi_2$ בעזרת מכונת אורקל ל"ד.

<u>פתרון:</u> צריך להראות כי $\overline{\text{MIN-CNF}} \in \Sigma_2 = NP^{NP}$. כלומר, שקיימת שפה $A \in NP$ ומ"ט ל"ד M עם גישת אורקל ל-A המכריעה את $\overline{\text{MIN-CNF}}$.

נגדיר את השפה NOT-EQ = $\{(\phi_1, \phi_2) \mid \phi_2$ לא שקולה ל-$\phi_1\}$. קל לראות כי NOT-EQUI $\in NP$ (אם הן לא שקולות, קיימת השמת אמת v כך ש-$\phi_1(v) \neq \phi_2(v)$). כעת, נגדיר את המכונה M:

<u>$M^{\text{NOT-EQ}}(\phi)$:</u>

1. אם ϕ לא בצורת CNF, החזר 1.
2. נחש באופן ל"ד נוסחה ϕ' בצורת CNF קצרה יותר מ-ϕ.
3. אם $(\phi, \phi') \in$ NOT-EQ החזר 0.
4. החזר 1.

<u>נכונות:</u> אם $\phi \in \overline{\text{MIN-CNF}}$, או ש-$\phi$ לא בצורת CNF ואז האלגוריתם יחזיר 1, או שקיימת נוסחה קצרה יותר ϕ' השקולה ל-ϕ ($(\phi, \phi') \notin$ NOT-EQ). עבור חישוב המנחש את ϕ', M תחזיר 1. אם $\phi \notin \overline{\text{MIN-CNF}}$, המכונה תמיד תחזיר 0. לכן $M^{\text{NOT-EQ}}$ מכריעה את $\overline{\text{MIN-CNF}}$ ולכן MIN-CNF $\in \Pi_2$.

תרגיל: הוכיחו כי לכל בעית הכרעה S מתקיים $S \in P^{\bar{S}}$.

פתרון: נראה מ"ט דטר' פולינומית עם גישת אורקל ל-$\bar{S}$ המכריעה את S. המכונה תקבל קלט x, תבצע שאילתא לאורקל אם $x \in \bar{S}$ ותחזיר תשובה הפוכה.

תרגיל: הוכיחו כי לכל בעית הכרעה S מתקיים $P^S = P^{\bar{S}}$.

פתרון: תהי $S' \in P^S$. כלומר, קיימת מ"ט דטר' פולינומית M עם גישת אורקל ל-S המכריעה את S'. נראה מ"ט דטר' פולינומית M' עם גישת אורקל ל-$\bar{S}$ המכריעה את S'. M' תפעל בדיוק כמו M, ובכל פעם ש-M מבצעת שאילתא לאורקל, M' תבצע בדיוק אותה שאילתא ואז תהפוך את תשובת האורקל. מכיוון ש-$x \in S \Leftrightarrow x \notin \bar{S}$, הפיכת תשובת האורקל ל-$\bar{S}$ שקולה לתשובת האורקל ל-S. לכן M' עובדת בדיוק כמו M ולכן מכריעה את S'.

קיבלנו כי $P^S \subseteq P^{\bar{S}}$. ומכאן גם ש-$P^{\bar{S}} \subseteq P^{\bar{\bar{S}}} = P^S$, ולכן $P^S = P^{\bar{S}}$.