סיבוכיות- תרגול 4

<u>טענה:</u> יהי R יחס כך ש-$S_R \in P$. אם $R \notin PF$, אזי R לא ניתן לרדוקציה עצמית.

<u>הוכחה:</u> נראה כי אם R ניתן לרדוקציה עצמית אזי $R \in PF$. נניח ש-R ניתן לרדוקציה עצמית. כלומר, קיים אלגוריתם פולינומי A שפותר את בעית החיפוש R בעזרת שימוש בקופסה שחורה המכריעה את S_R. בנוסף, $S_R \in P$, ולכן קיים אלגוריתם פולינומי D המכריע את S_R. נראה אלגוריתם פולינומי A' הפותר את בעית החיפוש R ללא שימוש בקופסה השחורה. A' יפעל בדיוק כמו A, ובכל קריאה לקופסה השחורה עבור שאלה מהצורה "$x \in S_R$?", A' יריץ את $D(x)$ וישתמש בתשובה שלו. A' אלגוריתם פולינומי הפותר את R ולכן $R \in PF$.

<u>דוגמא ליחס קונקרטי שלא ניתן לרדוקציה עצמית:</u>

נגדיר את היחס $R = \{(N, Q) \mid N$ מחלק לא טריוויאלי של $Q\}$. $R \in PC$, כי בהנתן זוג (N, Q) ניתן לבדוק בזמן פולינומי אם Q מחלק את N. $S_R \in P$ כי קיים אלגוריתם פולינומי שבהנתן מספר טבעי N, מכריע אם N ראשוני. אבל משערים כי $R \notin PF$, ולכן R לא ניתן לרדוקציה עצמית.

<u>תזכורת:</u> $S \in NP$ אם קיימים פולינום $p(\cdot)$ ואלגוריתם פולינומי V המקיימים:

$x \in S \Leftrightarrow$ קיים y, $|y| \leq p(|x|)$, כך ש-$V(x, y) = 1$.

<u>תזכורת:</u> $S \in coNP$ אם $\bar{S} \in NP$.

<u>הגדרה שקולה:</u> $S \in coNP$ אם קיימים פולינום $p(\cdot)$ ואלגוריתם פולינומי V המקיימים:

$x \in S \Leftrightarrow$ לכל y, $|y| \leq p(|x|)$, $V(x, y) = 1$.

<u>לא פורמלי:</u> המחלקה NP מכילה בעיות שעבור קלטים בשפה קיימת הוכחה קצרה, ו-$coNP$ מכילה בעיות שעבור קלטים בשפה אין הפרכה קצרה.

<u>דוגמאות:</u>

1. $\text{VC} = \{(G, k) \mid$ קיים ב-G כיסוי קודקודים בגודל $k \geq\} \in NP$.
   המוודא מקבל זוג (G, k) ותת-קבוצה של קודקודים S ומחזיר 1 אם ורק אם $|S| \leq k$ וגם S כיסוי קודקודים ב-G.

2. $\overline{\text{VC}} = \{(G, k) \mid$ כל כיסוי קודקודים ב-G בגודל $k <\} \in coNP$.
   המוודא מקבל זוג (G, k) ותת-קבוצה של קודקודים S ומחזיר 1 אם ורק אם $|S| > k$ או S לא כיסוי קודקודים ב-G.

<u>שאלה:</u> לאיזו מחלקה שייכת הבעיה הבאה:

$\text{MIN-VC} = \{(G, k) \mid k$ בגודל G-כיסוי הקודקודים המינימלי ב$\}$.

<u>הגדרה:</u> תהי S בעית הכרעה. נאמר כי $S \in \Sigma_2$ אם קיים פולינום $p(\cdot)$ ואלגוריתם פולינומי V המקיימים:

$x \in S \Leftrightarrow$ קיים y_1, $|y_1| \leq p(|x|)$, כך שלכל y_2, $|y_2| \leq p(|x|)$ מתקיים $V(x, y_1, y_2) = 1$.

<u>טענה:</u> $\text{MIN-VC} \in \Sigma_2$.

<u>הוכחה:</u> נגדיר את המוודא V באופן הבא:

V מקבל כקלט זוג (G,k), תת-קבוצה של קודקודים S, ותת-קבוצה של קודקודים S' ומחזיר 1 אם ורק אם מתקיים:

1. $|S| = k$.
2. S כיסוי קודקודים ב-G.
3. $|S'| \geq k$ או S' לא כיסוי קודקודים ב-G.

$|S|$ ו-$|S'|$ פולינומים ב-$|(G,k)|$, כל הבדיקות מתבצעות בזמן פולינומי ומתקיים:

MIN-VC $\ni (G,k) \Leftrightarrow$ קיים $S \subseteq V(G)$ כך שלכל $S' \subseteq V(G)$ מתקיים $V\big((G,k),S,S'\big) = 1$.

<u>הגדרה:</u> $\Pi_2 = co\Sigma_2$. כלומר, $S \in \Pi_2$ אם קיימים פולינום $p(\cdot)$ ואלגוריתם פולינומי V המקיימים:

$x \in S \Leftrightarrow$ לכל y_1, $|y_1| \leq p(|x|)$, קיים y_2, $|y_2| \leq p(|x|)$ כך ש-$V(x,y_1,y_2) = 1$.

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

MIN-CNF = {ϕ | ϕ בצורת CNF, ולא קיימת נוסחה קצרה יותר בצורת CNF השקולה ל-ϕ}.

<u>פתרון:</u> נגדיר את המוודא V באופן הבא:

V מקבל כקלט נוסחה ϕ, נוסחה ϕ' והשמת אמת v ומחזיר 1 אם ורק אם מתקיים:

1. ϕ בצורת CNF.
2. אם $|\phi'| < |\phi|$ ובצורת CNF אזי $\phi(v) \neq \phi'(v)$.

$|\phi'|$ ו-$|v|$ פולינומים ב-$|\phi|$, כל הבדיקות מתבצעות בזמן פולינומי ומתקיים:

MIN-CNF $\ni \phi \Leftrightarrow$ לכל ϕ' קיים v כך ש-$V(\phi,\phi',v) = 1$.