סיבוכיות- תרגול 3

<u>הגדרה:</u> $coNP = \{S \mid \bar{S} \in NP\}$.

<u>לא פורמלי:</u> כל הבעיות עבורן קיימת הוכחה קצרה לכל קלט שאינו בשפה.

<u>דוגמאות:</u>

1. $\overline{SAT} = \{\phi \mid \phi$ נוסחה בצורת CNF שאינה ספיקה$\} \in coNP$.
2. $\overline{Clique} = \{(G,k) \mid G$ לא מכיל תת-גרף מלא בגודל $k\} \in coNP$.

<u>תרגיל:</u> הוכיחו:

א. לכל בעית הכרעה S קיימת רדוקצית קוק למשלים שלה.
ב. לכל בעית הכרעה $S \in P$ כך ש-$S \neq \emptyset, \Sigma^*$ קיימת רדוקצית קארפ למשלים שלה.

<u>פתרון:</u>

א. הוכחה: בהנתן קופסה שחורה $A_{\bar{S}}$ המכריעה את $\bar{S}$, נבנה אלגוריתם פולינומי A_S המכריע את S. A_S יריץ את $A_{\bar{S}}$ ויחזיר תשובה הפוכה. ברור כי A_S רץ בזמן פולינומי, ומתקיים:

$$A_S(x) = 1 \Leftrightarrow A_{\bar{S}}(x) = 0 \Leftrightarrow x \notin \bar{S} \Leftrightarrow x \in S$$

ב. הוכחה: יהיו $x_1 \in S$ ו-$x_2 \notin S$. נגדיר את הפונקציה הבאה:

$$f(x) = \begin{cases} x_2 & x \in S \\ x_1 & x \notin S \end{cases}$$

f ניתנת לחישוב בזמן פולינומי ע"י הרצת האלגוריתם הפולינומי המכריע את S והחזרת x_1 או x_2 בהתאם לתשובה. כמו כן, מתקיים:

$$x \in S \Longrightarrow f(x) = x_2 \in \bar{S}$$

$$x \notin S \Longrightarrow f(x) = x_1 \notin \bar{S}$$

<u>טענה:</u> בהנחה ש-$P \neq NP \cap coNP$, קיימת בעית חיפוש ב-PC שלא ניתנת לרדוקציה עצמית.

<u>הוכחה:</u> תהי $S \in (NP \cap coNP) \setminus P$. $S \in NP$ ולכן קיים פולינום $p_S(\cdot)$ ומוודא פולינומי V_S כך שלכל x מתקיים:

1. $x \in S \Longrightarrow \exists y, |y| \leq p_S(|x|), V_S(x,y) = 1$.
2. $x \notin S \Longrightarrow \forall y, V_S(x,y) = 0$.

בנוסף, $S \in coNP$, ולכן $\bar{S} \in NP$. לכן קיים פולינום $p_{\bar{S}}(\cdot)$ ומוודא פולינומי $V_{\bar{S}}$ כך שלכל x מתקיים:

1. $x \in \bar{S} \Longrightarrow \exists y, |y| \leq p_{\bar{S}}(|x|), V_{\bar{S}}(x,y) = 1$.
2. $x \notin \bar{S} \Longrightarrow \forall y, V_{\bar{S}}(x,y) = 0$.

נסמן $q = \max\{p_S, p_{\bar{S}}\}$ ונגדיר את היחס הבא:

$$R = \{(x,y) \mid |y| \leq q(|x|), (V_S(x,y) = 1 \vee V_{\bar{S}}(x,y) = 1)\}$$

לפי הגדרת היחס, R חסום פולינומית וניתן להשתמש במוודאים $V_S, V_{\bar{S}}$ להכרעה האם זוג (x,y) שייך ל-R. לכן $R \in PC$. נראה כי R לא ניתן לרדוקציה עצמית. כלומר, בהנתן אלגוריתם המכריע את S_R, לא קיים אלגוריתם פולינומי הפותר את בעית החיפוש R.

נשים לב כי עבור $x \in S$ קיים $y, |y| \le q(|x|)$ כך ש-$V_S(x,y) = 1$, ועבור $x \notin S$ קיים $y, |y| \le q(|x|)$ כך ש-$V_{\bar{S}}(x,y) = 1$, ולכן $S_R = \Sigma^*$. כלומר, אם קיימת רדוקציה עצמית עבור R, אזי $R \in PF$, כי ניתן להחליף כל קריאה לקופסה השחורה המכריעה את S_R במכונה המחזירה תמיד 1.

נניח בשלילה כי $R \in PF$. כלומר, קיים אלגוריתם פולינומי A_R הפותר את בעית החיפוש R. נבנה אלגוריתם פולינומי A_S המכריע את S ובכך נראה כי $S \in P$ בסתירה.

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

1. $y \leftarrow A_R(x)$.
2. החזר את $V_S(x,y)$.

A_R ו-V_S פולינומיים ולכן גם A_S פולינומי. A_S מכריע את S כי עבור $x \in S$ מתקיים:

1. קיים y, $|y| \le q(|x|)$ כך ש-$V_S(x,y) = 1$
2. לכל y, $V_{\bar{S}}(x,y) = 0$.

לכן, כאשר $A_R(x)$ יחזיר y עבורו $(x,y) \in R$, בהכרח מתקיים כי $V_S(x,y) = 1$ (לפי הגדרת R), ולכן $A_S(x) = 1$. באופן דומה, עבור $x \notin S$ מתקיים:

1. קיים y, $|y| \le q(|x|)$ כך ש-$V_{\bar{S}}(x,y) = 1$.
2. לכל y, $V_S(x,y) = 0$.

לכן, כאשר $A_R(x)$ יחזיר y עבורו $(x,y) \in R$, בהכרח מתקיים כי $V_S(x,y) = 0$ ולכן $A_S(x) = 0$. סה"כ קיבלנו כי $S \in P$ בסתירה. לכן $R \notin PF$, כלומר R לא ניתן לרדוקציה עצמית.