קורס מודלים חישוביים – עבודת בית מס' 6

שאלה 1:

הגדרה: $co - NP = \{L \subseteq \Sigma^* : \bar{L} \in NP\}$.

א. <u>טענה:</u> $P \subseteq co - NP$.

<u>הוכחה:</u> תהא $L \in P$. הוכחנו בכיתה ש- P סגורה למשלים, אזי $\bar{L} \in P$.

מכך ש: $P \subseteq NP$ נובע $\bar{L} \in NP$. אזי מההגדרה, $L \in co - NP$ כנדרש.

ב. <u>טענה:</u> אם $P \neq NP$, אזי $P \neq co - NP$.

מכך ש: $P \subseteq NP$ וגם $P \neq NP$ נובע שקיימת שפה L המקיימת:

$L \notin P, L \in NP$. כמו כן, מכך ש: $L \in NP$ נובע $\bar{L} \in co - NP$. ובנוסף,

מכך ש: $L \notin P$, ומכך ש- P סגורה למשלים, נובע: $\bar{L} \notin P$.

הראנו $P \neq co - NP$ כנדרש.

ג. <u>טענה:</u> אם $NP \neq co - NP$ אזי $SAT \notin co - NP$.

נניח $NP \neq co - NP$. נחלק למקרים:

1. קיימת שפה L המקיימת: $L \in NP$ וגם $L \notin co - NP$.

   מההגדרה נובע $\bar{L} \notin NP$.

   הראנו בכיתה שמתקיים $SAT \in NPC$, אזי $L \leq_P SAT$ ומכאן ש

   $\bar{L} \leq_P \overline{SAT}$. ממשפט הרדוקציה נובע $\overline{SAT} \notin NP$, אזי מההגדרה

   $SAT \notin co - NP$ כנדרש.

2. קיימת שפה L המקיימת $L \notin NP$ וגם $L \in co - NP$.

   מההגדרה נובע $\bar{L} \notin co - NP$, וגם $\bar{L} \in NP$.

   הראנו בכיתה שמתקיים $SAT \in NPC$, אזי $\bar{L} \leq_P SAT$ ומכאן ש

   $L \leq_P \overline{SAT}$. ממשפט הרדוקציה נובע $\overline{SAT} \notin NP$, אזי מההגדרה

   $SAT \notin co - NP$ כנדרש.

שאלה 2:

לכל $k \in \mathbb{N}$ נגדיר:

$$k - Clique = \{G: G\ is\ an\ undirected\ graph\ that\ contains\ a\ clique\ of\ size\ k\}$$

א. נציג אלגוריתם פולינומיאלי לשפה $11 - Clique$:

1. <u>לולאה:</u> לכל תת קבוצה $C \subseteq V$, המקיימת $|C| = 11$, בצע:

- לכל $v, u \in C$: בדוק אם $\{u, v\} \in E$. אם התשובה היא "לא" – חזור לצעד 1. אחרת, תמשיך.
- אם התשובה היא "כן" – תסיים ותענה "כן". אחרת, תחזור לצעד 1.

2. <u>אחרת,</u> תסיים ותענה "לא".

ניתוח זמן ריצה: המעבר על כל תתי הקבוצות של V בגודל 11 דורש $O(|V|^{11})$. בנוסף, פעולת בדיקת הצלעות דורש מעבר כל הזוגות מתוך קבוצה בגודל 11 – זו בדיקה בזמן קבוע, ולכן אין לה השפעה על זמן הריצה.

סה"כ $O(|V|^{11})$ – פולינומי בגודל הקלט G.

ב. נראה רדוקציה $4 - Clique \leq_p 8 - Clique$ המקבלת גרף G עם n קודקודים ומחזירה גרף $f(G)$ עם $O(n^2)$ קודקודים, בזמן ריצה שאינו עולה על $O(n^4)$.

נגדיר $f: \Sigma^* \to \Sigma^*$, כאשר: $f(G) \to G'$.

נגדיר $G' = (V', E')$, כך ש:

$$V' = \{v_{i,j}: \{v_i, v_j\} \in E\}$$

$$E' = \{\{v_{i,j}, v_{k,l}\}: v_i, v_j, v_k, v_l\ are\ clique\ of\ size\ 4\ in\ G\}$$

נוכיח ש- f רדוקציה מ- $8 - Clique$ ל- $4 - Clique$:

1. f חשיבה בזמן פולינומי:

בניית V': מעבר על כל זוגות הקודקודים ב – G = $O(n^2)$.

בניית E': מעבר על כל רביעיות הקודקודים ב – G = $O(n^4)$.

סה"כ $O(n^4)$ כנדרש.

2. f תקפה: $x \in 8-Clique$ אמ"מ $f(x) \in 4-Clique$:

$\Leftarrow$ נניח $x \in 8-Clique$, אזי $x = G = (V,E)$ כאשר קיימת ב- G קליקה בגודל 8. נסמן את קודקודי הקליקה הזו ע"י $\{v_1, v_2, \dots, v_8\}$.

מהגדרת קליקה, בין כל זוג v_i, v_j כאשר $1 \le i \ne j \le 8$, מתקיים $\{v_i, v_j\} \in E$. מכאן, עפ"י בניית V' נקבל כי: $v_{1,2}, v_{3,4}, v_{5,6}, v_{7,8} \in V'$.

בנוסף, מכך שכל קבוצת קודקודים שמוכלת בקליקה מהווה קליקה בעצמה, עפ"י בניית E' נקבל כי:

$\{v_{1,2}, v_{3,4}\}, \{v_{1,2}, v_{5,6}\}, \{v_{1,2}, v_{7,8}\}, \{v_{3,4}, v_{5,6}\}, \{v_{3,4}, v_{7,8}\}, \{v_{5,6}, v_{7,8}\} \in E'$

נשים לב שקבוצת קשתות אלה מראה ש: $v_{1,2}, v_{3,4}, v_{5,6}, v_{7,8}$ מהווים קליקה בגודל 4 ב- G' כנדרש.

$\Rightarrow$ נניח $f(x) \in 4-Clique$, אזי $f(x) = G' = (V', E')$ כאשר קיימת ב- G' קליקה בגודל 4. נסמן את קודקודי הקליקה הזו ע"י $C_4 = \{v_{i_1,i_2}, v_{i_3,i_4}, v_{i_5,i_6}, v_{i_7,i_8}\}$. עפ"י בניית G' נובע שכל זוג קודקודים מ- C_4 מהווה קליקה בגודל 4 ב- G, אזי מכאן נובע שכל קודקוד מ- C_4 מייצג 2 קודקודים שונים ב- G. בנוסף לכך, לא ייתכן שאותו קודקוד מ- G מיוצג ע"י יותר מקודקוד אחד ב- C_4, כיוון שאחרת נקבל סתירה לכך שזוג קודקודים אלה מהווה קליקה בגודל 4 ב- G.

לאור כל זאת, קודקודי C_4 מייצגים 8 קודקודים **שונים** ב- G נסמנם ע"י $\{v_{i_1}, v_{i_2}, \dots, v_{i_8}\}$.

נסתכל על שני קודקודים שונים v_{i_k}, v_{i_l} מקבוצה זו.

אם v_{i_k}, v_{i_l} מיוצגים ע"י אותו הקודקוד ב- C_4 אזי מהגדרת G' יש ביניהם קשת ב- G.

אחרת, v_{i_k}, v_{i_l} מיוצגים ע"י שני קודקודים שונים ב- C_4, ומכיוון שקיימת בין שני הקודקודים המייצגים אותם קשת ב- G' (הם חלק מהקליקה C_4) עפ"י בניית E' נובע שהם חלק מקליקה בגודל 4 ב- G אזי קיימת ביניהם גם כן קשת ב- G.

בסה״כ מצאנו כי בין כל שני קודקודים ב $\{v_{i_1}, v_{i_2}, \dots, v_{i_8}\}$ קיימת קשת ב- G, ולכן קבוצה זו מהווה קליקה מגודל 8 ב- G כנדרש.

ג. נציג אלגוריתם פולינומיאלי לשפה $k - Clique$:

1. לולאה: לכל תת קבוצה $C \subseteq V$, המקיימת $|C| = k$, בצע:
- לכל $v, u \in C$: בדוק אם $\{u, v\} \in E$. אם התשובה היא ״לא״ – חזור לצעד 1. אחרת, תמשיך.
- אם התשובה היא ״כן״ – תסיים ותענה ״כן״. אחרת, תחזור לצעד 1.
2. אחרת, תסיים ותענה ״לא״.

ניתוח זמן ריצה: המעבר על כל תתי הקבוצות של V בגודל k דורש $O(|V|^k)$. בנוסף, פעולת בדיקת הצלעות דורשת מעבר כל הזוגות מתוך קבוצה בגודל k – זו בדיקה בזמן קבוע, ולכן אין לה השפעה על זמן הריצה.

סה״כ זמן הריצה הינו $O(|V|^k)$ – פולינומי בגודל הקלט G.

שאלה 3:

א. טענה: $BI \in NP$.

נציג אלגוריתם אימות פולינומיאלי עבור הבעיה BI.

העד עבור הקלט הינו השמה בינארית למשתני המערכת.

אלגוריתם האימות:

1. בדוק את תקינות הקלט:
   a. בדוק שההשמה הנתונה הינה בינארית.
   b. עבור על משוואות המערכת וודא שלכל משתנה קיימת השמה.
2. לכל משוואה במערכת:
   a. הצב את ההשמה הנתונה ובדוק שהמשוואה מתקיימת.
3. אם התשובה לצעד 1 או לצעד 2 הינה ״לא״ החזר ״לא״, אחרת החזר ״כן״.

הוכחת פולינומיאליות:

1. העד פולינומי כיוון שחסום ע״י אורך המשוואות במערכת.

2. האלגוריתם פולינומי כיוון שבצעד הראשון עובר מעבר לינארי על הקלט, ובצעד השני עובר על העד כמספר המשוואות במערכת – פולינומי.

ב. <u>טענה</u>: $BI \in NPC$.

בסעיף א' הראנו $BI \in NP$, לכן נותר להראות $BI \in NPH$.

נראה רדוקציה $IS \leq_p BI$, ומכך ש: $IS \in NPH$ (הוכחנו בכיתה) ממשפט הרדוקציה נקבל $BI \in NPH$ כנדרש.

נגדיר $f: \Sigma^* \to \Sigma^*$, כך ש: $f(G,k) = P$, כאשר P מערכת אי שוויוניים המוגדרת כך:

ראשית, לכל קדקוד v_i נגדיר משתנה x_i.

שנית, המשוואות הן:

1. $\sum_{i=1}^{|V|} x_i \geq k$.
2. לכל קשת $\{v_i, v_j\} \in E$, $x_i + x_j \leq 1$.

נוכיח ש: f רדוקציה מ- IS ל- BI:

1. f חשיבה בזמן פולינומי:

המשוואה $\sum_{i=1}^{|V|} x_i \geq k$ באורך לכל היותר $|V|$. כמו כן, נותרו $|E|$ משוואות, שכל אחת מהן באורך 2.

בסה"כ זמן יצירת המשוואות דורש $O(|V| + |E|)$ – לינארי בגודל הקלט G.

2. f תקפה: $x \in IS$ אמ"מ $f(x) \in BI$.

$\Leftarrow$ נניח $x \in IS$, אזי $x = (G,k)$ כאשר ב- G קיימת קבוצת קודקודים בלתי תלויה בגודל לפחות k, נסמנה ב- I.

נגדיר את ההשמה הבינארית הבאה לכל $v_i \in V$:

אם $v_i \in I$ נגדיר $x_i = 1$. אחרת, $x_i = 0$.

נראה שהשמה זו מספקת את $f(x)$:

המשוואה $\sum_{i=1}^{|V|} x_i \geq k$ בהכרח מתקיימת מכיוון ש: $|I| \geq k$. כמו כן, מחוקיות I, לכל קשת $\{v_i, v_j\} \in E$ מתקיים $v_i \in I, v_j \notin I$ או

$v_j \in I, v_i \notin I$, ובפרט, לכל היותר אחד מבין x_i, x_j קיבל השמה 1.

הראנו שלכל קשת $\{v_i, v_j\} \in E$ מתקיים $x_i + x_j \leq 1$.

הגדרנו השמה בינארית המקיימת כל אחת מהמשוואות ב- $f(x)$, אזי $f(x) \in BI$.

$\Longrightarrow$ נניח $x \notin IS$ אזי $x = (G, k)$ כך שב- G לא קיימת קבוצת קודקודים בלתי תלויה בגודל לפחות k.

נניח בשלילה שקיימת השמה בינארית B המקיימת את $f(x)$. ובפרט, מקיימת את כל אחת מהמשוואות ב- $f(x)$.

אזי, המשוואה $\sum_{i=1}^{|V|} x_i \geq k$ מתקיימת, כלומר – לפחות k משתנים קיבלו השמה 1 ב- B, נסמנם ב- B_1. מכך שלא קיימת ב- G קבוצת קודקודים בלתי תלויה בגודל לפחות k, מעקרון שובך היונים נובע שקיימים משתנים $x_i, x_j \in B_1$ שקיימת קשת ביניהם. אזי, המשוואה $x_i + x_j \leq 1$ ב- $f(x)$ אינה מתקיימת. סתירה.

מ.ש.ל

שאלה 4:

נוכיח $VC \leq_p DomSet$.

נגדיר $f: \Sigma^* \to \Sigma^*$, כך ש: $f(G, k) = (G', k)$, כאשר G' מוגדר כך:

בהינתן $G = (V, E)$. נגדיר $G' = (V', E')$:

$$V' = V \cup \{v_{e_i} : e_i \in E\}$$

$$E' = E \cup \{\{v_{e_i}, v_i\}, \{v_{e_i}, v_j\} : e_i = \{v_i, v_j\} \in E\}$$

נוכיח ש- f רדוקציה מ- VC ל- $DomSet$:

1. f חשיבה בזמן פולינומי: בניית הגרף G': הגדרת V' דורשת מעבר יחיד על הקבוצות V, E - $O(|V| + |E|)$. הגדרת E' דורשת שני מעברים על הקבוצה E - $O(|E|)$. ובסה״כ $O(|V| + |E|)$ – לינארי בגודל הקלט G.

2. f תקפה: $x \in VC$ אמ"מ $f(x) \in DomSet$.

$\Leftarrow$ נניח $x \in VC$, אזי $x = (G, k)$ כאשר קיימת ב- G קבוצת כיסוי בקודקודים בגודל לכל היותר k, נסמנה ב- C.

יהי $v \in V'$ כך ש $v \notin C$.

נחלקים למקרים:

אם $v \in V$ ומכך ש G קשיר קיים $u \in V$ כך ש $\{u, v\} \in E$. (וזאת בהנחה ש $|V| > 1$, אחרת – מתקיים באופן טריוויאלי). C כיסוי בקודקודים ב – G ומכיוון ש $v \notin C$ נבין כי $u \in C$.

אם $v \in V' \backslash V$ אזי קיימים $u_1, u_2 \in V$ כך ש $\{u_1, u_2\} \in E$ וגם $\{v, u_1\}, \{v, u_2\} \in E'$. $\{u_1, u_2\} \in E$ וגם C כיסוי בקודקודים ב $G -$ אזי $u_1 \in C$ או $u_2 \in C$.

בסה"כ הראינו כי לכל $v \in V'$ כך ש $v \notin C$, קיים $u \in V'$ כך ש $\{v, u\} \in E'$ וגם $u \in C$, ומכאן שקיימת ב - G' קבוצה שלטת בגודל לכל היותר k.

$\Rightarrow$ נניח $f(x) \in DomeSet$, אזי $f(x) = (G', k)$ כאשר קיימת ב- G' קבוצה שלטת בגודל לכל היותר k, נסמנה ב- D.

אם לכל $\{u, v\} \in E$ מתקיים $u \in D$ או $v \in D$ אזי D כיסוי בקודקודים ב- G, וכן ראינו ש D בגודל לכל היותר k. כנדרש.

אחרת, נסמן ב- $\{u_1, v_1\}, \dots, \{u_m, v_m\} \in E$ את קבוצת הקשתות כך שלכל $1 \leq i \leq m$ מתקיים $u_i \notin D$ וגם $v_i \notin D$. מכיוון ש D קבוצה שלטת נבחין כי לכל $1 \leq i \leq m$, אם נסמן $e_i = \{u_i, v_i\}$ אזי בהכרח $v_{e_i} \in D$, אחרת נקבל סתירה לכך ש D קבוצה שלטת מכיוון שלא ייתכן ש v_{e_i} ושני שכניו היחידים אינם ב D. כעת, נגדיר קבוצה D' כך $D' = D \backslash \{v_{e_1}, \dots, v_{e_m}\} \cup \{u_1, \dots, u_m\}$. מתקיים $|D'| = |D| \leq k$, וכן עבור כל צלע ב E אחד מקודקודיה שייך ל- D', אזי D' קבוצת כיסוי בקודקודים ב- G בגודל לכל היותר k. כנדרש.