מטלה 3

כל הנחיות המטלות הקודמות תקפות גם כאן.

תרגילים

1. לחדר מסוים באוניברסיטה יש 7 מנעולים בעלי חור כפול (חור אחד עבור המפתח, וחור אחד עבור המפתח הנגדי)

אברהם מחזיק את מפתחות $A, \neg B, E$
בנימין מחזיק את מפתחות $\neg B, \neg F, G$
גד מחזיק את מפתחות $B, \neg C, \neg D, \neg F, G$
דן מחזיק את מפתחות $E, \neg G$
הגר מחזיקה את מפתחות $C, \neg E, \neg F$
ופסי מחזיק את מפתחות $A, C, \neg E, \neg F$
זבולון מחזיק את מפתחות $A, \neg B, \neg C, D, \neg E$

כדי לפתוח את החדר, יש לסובב מפתח אחד מכל זוג חורים, במקביל.
א. כתבו נוסחת CNF מתאימה לבעיה.
ב. המירו אותה לצורת $3CNF$ בעזרת הרדוקציה שלמדנו.
ג. אברהם איבד את מפתח $\neg B$. האם עדיין ניתן לפתוח את החדר?

פתרון

א. הנוסחה הרלוונטית היא:

$$\phi(A,B,C,D,E,F,G) = (A \vee \neg B \vee E) \wedge (\neg B \vee \neg F \vee G) \wedge (B \vee \neg C \vee \neg D \vee \neg F \vee G) \wedge (E \vee \neg G) \wedge (C \vee \neg E \vee \neg F) \wedge (A \vee C \vee \neg E \vee \neg F) \wedge (A \vee \neg B \vee \neg C \vee D \vee \neg E)$$

ב. נמיר את הפסוקיות כפי שלמדנו. פסוקית בעלת 3 משתנים תישאר כפי שהיא, בפסוקית בעלת 2 משתנים נשכפל את אחד המשתנים. בפסוקית ארוכה יותר – נפצל לתתי-פסוקיות עם משתנים חדשים.

$$\phi'(A,B,C,D,E,F,G,z_1,z_2,z_3,z_4,z_5) = (A \vee \neg B \vee E) \wedge (\neg B \vee \neg F \vee G) \wedge (B \vee \neg C \vee z_1) \wedge (\neg z_1 \vee \neg D \vee z_2) \wedge (\neg z_2 \vee \neg F \vee G) \wedge (E \vee \neg G \vee E) \wedge (C \vee \neg E \vee \neg F) \wedge (A \vee C \vee z_3) \wedge (\neg z_3 \vee \neg E \vee \neg F) \wedge (A \vee \neg B \vee z_4) \wedge (\neg z_4 \vee \neg C \vee z_5) \wedge (\neg z_5 \vee D \vee \neg E)$$

ג. כעת בפסוקית הראשונה לא מופיע $\neg B$ אלא נותר רק $A \vee E$. זה לא ישפיע הרבה, כי עדיין קיימת השמה מספקת: (T,T,T,T,T,F,T).

2. הוכיחו כי השפות הבאות הן NPC:
א. $CNF-IS = \{< G,k,\phi > | G \text{ has a size } k \text{ IS or } \phi \text{ is a satisfiable CNF formula}\}$
ב. $Partition = \{< S > | S \text{ is a set of numbers}, \exists S' \subset S \text{ such that } \sum_{x\in S'} x = \sum_{x\notin S'} x\}$
הנחיה: מהו סכום כל איברי S?
ג. הגדרה: קבוצה שולטת (Dominating Set) היא תת קבוצה של קודקודים, שכל שאר קודקודי הגרף שכנים של קבוצה זו. $S \subseteq V: V \setminus S \subseteq \Gamma(S)$.

$$DS = \{< G,k > | G \text{ is an undirected graph with a size } k \text{ dominating set}\}$$

(הנחיה: היעזרו ב VC- מה יקרה אם לכל צלע תייצרו קודקוד? באופן חריג, אפשר להניח כי בגרף אין יחידונים ולכן לא צריך לטפל בהם)
ד. $DoubleHC = \{< G > | G \text{ is undirected graph with two different Hamilton cycles}\}$

פתרון

תחילה נראה בכל שפה כי היא במחלקה NP, ולאחר מכן נראה רדוקציה מתאימה משפה ב NPh (או ב NPC).

א. המכונה M על הקלט $< G, k, \phi >$:
- מנחשת קבוצת קודקודים בגודל k והשמה בגודל n (כמות המשתנים בנוסחה ϕ).
- בודקת האם קבוצת הקודקודים אכן מהווה IS. אם כן, מקבלת.
- מציבה את ההשמה בנוסחה ϕ ומוודאת שערך הנוסחה הוא T.
אם כן, מקבלת, אחרת, דוחה.

המכונה רצה בזמן פולינומי בגודל הקלט:
ניחוש קבוצת הקודקודים $\leq |V(G)|$
ניחוש ההשמה באורך $\phi \geq n$
וידוא IS- מעבר על מטריצת השכנויות ווידוא כי אין צלעות $k^2 \leq |V(G)|^2$
וידוא ספיקות הנוסחה $|\phi| = O(m)$.

נכונות:

אם $< G, k, \phi > \in CNF - IS$ אזי קיימת IS בגודל k או שהנוסחה ספיקה. לכן, המכונה תנחש את קבוצת הקודקודים הנכונה או את ההשמה הנכונה, ובראשון מביניהם היא תזהה שהקלט בשפה ותקבל.

אם $< G, k, \phi > \notin CNF - IS$ אזי אין IS בגודל k, ואין השמה מספקת. לכן, לכל ניחוש של קבוצת קודקודים בגודל k המכונה לא תקבל (כי הקבוצה לא תהווה IS) ולכל ניחוש של השמה המכונה תדחה (הנוסחה לא תסופק).

$CNF - IS \in NPh$:

נראה רדוקציה מ $CNF - SAT$.

$$f(\phi) = (< G = (\{v_1, v_2\}, \{v_1 v_2\}, 2), \phi)$$

הרדוקציה מחושבת בזמן פולינומי בקלט: העתקה של הנוסחה, וייצור גרף בעל שני קודקודים וצלע אחת.

תקפות:

אם $\phi \in CNF - SAT$ אזי קיימת לה השמה מספקת. לכן גם ל $f(\phi)$ קיימת השמה מספקת ולכן $< G, k, \phi > \in CNF - IS$.
אם $\phi \notin CNF - SAT$ אזי לא קיימת לה השמה מספקת. היות והגרף G מכיל שני קודקודים וצלע אחת, אין בו קבוצה ב"ת בגודל 2 וגם הנוסחה ϕ אינה ספיקה ולכן $< G, k, \phi > \notin CNF - IS$.

ב. $Partition \in NP$:

המכונה M על הקלט S:
- תנחש תת קבוצה של מספרים T.
- תבדוק האם $\sum_{x \in T} x = \sum_{x \in S \setminus T} x$. אם כן תקבל, אחרת תדחה.

המכונה פולינומית: ניחוש תת קבוצה של מספרים (אפשר לנחש את המספרים עצמם או את האינדקסים שלהם, זה גם יספיק כדי לא להסתבך עם ייצוג עשרוני/בינארי/הקסה-דצימאלי) חסום בכמות המספרים בקלט, וסכימת איברי שתי הקבוצות מתבצעת בזמן פולינומי בכמות המספרים בקבוצה.

נכונות:

אם $S \in Partition$ אזי קיימת חלוקה לשתי תתי קבוצות שסכומן זהה. לכן, המכונה M תנחש את אחת הקבוצות, ותזהה שסכומה זהה לסכום הקבוצה המשלימה.

אם $S \notin Partition$ אזי כל חלוקה לשתי קבוצות תגרום לכך שיהיה הפרש בין הסכומים. לכן, כל ניחוש של תת קבוצה לא יפיק סכום זהה לתת הקבוצה המשלימה, והמכונה תדחה.

$Partition \in NPh$:

נראה רדוקציה מ $SubsetSum$.

$$f(< S, t >) = (S')$$

יהי $x = \sum_{y \in S} y$. הקבוצה S' תכיל את כל המספרים המקוריים מהקבוצה S וגם את האיבר החדש $x - 2t$.

הרדוקציה פולינומית: חישוב סכום כל איברי הקבוצה פולינומי בכמות האיברים. חישוב $x - 2t$ מתבצע ב $O(1)$.

תקפות:

אם $< S, t > \in SubsetSum$ אזי קיימת תת קבוצה של איברים (T) שסכומה בדיוק t. לכן, סכום שאר איברי הקבוצה הוא $x - t$. לכן, נוכל לבצע חלוקה של הקבוצה החדשה לשתי קבוצות שסכומן זהה:

$$\{S \setminus T\}, \{T \cup \{x - 2t\}\}$$

יהי $< S' > \in Partition$ אזי קיימת חלוקה לשתי קבוצות שסכומן זהה. סכום כל איברי הקבוצה S' הוא $x + x - 2t$ ולכן החלוקה השיוויונית מכריחה את שתי תתי הקבוצות להגיע לסכום $x - t$.
תהי B הקבוצה שמכילה את האיבר $x - 2t$. אזי, איברי הקבוצה B ללא האיבר $x - 2t$ מסתכמים בדיוק ל t, ולכן $< S, t > \in SubsetSum$ כנדרש.

ג. $Dominating\ Set \in NP$:
נגדיר את היחס R_{DS} על הזוגות $\big((G, k), y\big)$ כך:
העד y בגודל k הינו תת קבוצה של קודקודים בגרף G. $(|y| \leq |V(G)|)$
המאמת V על הקלט $\big((G, k), y\big)$:
1. עבור על כל קודקוד שאינו ב-y: אם אף אחד משכניו לא ב-y – דוחה.
2. מקבל.

שלב 1 פולינומי (לכל קודקוד עובר לכל היותר על כל שכניו. כמות הקודקודים $|V(G)| - k$, ולכל היותר $|V(G)|$ שכנים לכל אחד. סה"כ, ריבועי במקרה הגרוע). שלב 2 פולינומי – טריוויאלי.

$Dominating\ Set \in NPh$:

נראה רדוקציה מ VC.

$$f(< G, k >) = (< G', k >)$$

לכל צלע $\{uv\} \in E(G)$ נוסיף קודקוד חדש בשם uv. את הקודקוד נחבר גם ל-u וגם ל-v. הפרמטר k נשאר זהה.

הרדוקציה פולינומית: עברנו על $|E(G)|$ צלעות, לכל אחת הוספנו קודקוד ושתי צלעות.

תקפות:

אם $< G, k > \in VC$ אזי קיים כיסוי בקודקודים בגודל k בגרף G. כלומר, מכל צלע uv לקחנו לפחות קודקוד אחד לכיסוי. הקודקודים שהוספנו מחוברים גם ל-u וגם ל-v, ולכן הכיסוי בקודקודים מהווה

קבוצה שולטת בגרף G', שכן כל הקודקודים שכנים של הכיסוי. (כאן השתמשנו בהנחה שאין יחידונים בגרף)
אם $< G,k >\notin VC$ אזי לא קיים כיסוי בקודקודים בגודל k. כלומר, דרושים יותר מ-k קודקודים בשביל לכסות את כל הצלעות. היות וייצרנו לכל צלע קודקוד חדש, לא נוכל לשלוט בכל הקודקודים החדשים ב-k קודקודים בלבד, שכן אחרת היה כיסוי.
ניתן גם לנסח את הכיוון הזה "בכיוון החיובי". כלומר, שאם בגרף G' קיימת קבוצה שולטת בגודל k, היא מכילה לפחות קודקוד אחד מכל "משולש" חדש שיצרנו, וזה לא משנה איזה קודקוד במשולש, כך שנוכל לבחור את הקודקודים המקוריים (ולאו דווקא את החדשים שיצרנו), והם יהוו כיסוי של הגרף המקורי.
ד. $DoubleHC \in NP$:

נגדיר את היחס $R_{DoubleHC}$ על הזוגות (G,y) כך:
העד y בגודל $2|V(G)|$ הינו שני סידורים של הקודקודים בגרף G.
$(|y| = 2|V(G)| \cdot \log(|V(G)|) = O(|G|^2))$. (חסום מלמעלה. הלוג כתשלום על הביטים של ייצוג מספר הקודקוד)
המאמת V על הקלט (G,y):
1. עבור על החצי הראשון של קודקודי y: אם קיימת חזרה על קודקוד דחה.
2. עבור על החצי הראשון של קודקודי y: אם קיים זוג קודקודים רצוף ב-y שאין ביניהם צלע- דחה. אם אין צלע בין האחרון לבין הראשון דחה.
3. עבור על החצי השני של קודקודי y: אם קיימת חזרה על קודקוד דחה.
4. עבור על החצי השני של קודקודי y: אם קיים זוג קודקודים רצוף ב-y שאין ביניהם צלע- דחה. אם אין צלע בין הראשון לבין האחרון דחה.
5. אם החצי הראשון של קודקודי y זהה לחצי השני של קודקודי y – דחה.
6. קבל.

המאמת רץ בזמן פולינומי: עובר על $|y|$ כמה פעמים (פולינומי), מוודא לכל זוג קודקודים סמוכים קיום צלע (פולינומי). משווה שני חצאי y (פולינומי).

נכונות:

$< G >\in DoubleHC$ אזי קיימים שני מעגלי המילטון שונים. העד יכיל אותם, והמאמת יוודא שכל הצלעות הנדרשות קיימות ויקבל.
$< G >\notin DoubleHC$ אזי לא קיימים שני מעגלי המילטון שונים. העד יכיל שני מעגלים זהים (ייפול בסעיף 5) או שחסרה צלע (לפחות אחת) לפחות לאחד המעגלים (ייפול ב 2 או ב 4).

$DoubleHC \in NPh$:

נראה רדוקציה מ HC.

$$f(< G >) = (< G' >)$$

אם $|V(G)| \leq 2$ – לא לשנות. אחרת, פונקציית הרדוקציה תייצר גרף חדש G' המכיל שלושה קודקודים חדשים.

יהי קודקוד $v \in V(G)$ (קודקוד שרירותי). ניצור שלושה קודקודים חדשים v', u_1, u_2. ניצור קליקה $\{v, v', u_1, u_2\}$, ונחבר את כל השכנים של v גם אל v'.

הרדוקציה פולינומית (העתקת הגרף, הוספת $O(1)$ קודקודים, וצלעות).

תקפות:

אם $< G >\in HC$ אזי קיים לפחות מעגל המילטון אחד. יהי זה $v_1, v_2, \dots w, v, x, \dots, v_{n-3}, v_1$ (בה"כ. לחלוטין לא משנה). נרחיב את המעגל לשני מעגלים שונים:
$$C_1 = v_1, v_2, \dots w, v', u_1, u_2, v, x, \dots v_{n-3}, v_1$$
$$C_2 = v_1, v_2, \dots w, v', u_2, u_1, v, x, \dots, v_{n-3}, v_1$$

ולכן $< G' >\in DoubleHC$.

אם $< G' >\in DoubleHC$ אזי קיימים שני מעגלים שונים. המעגלים עוברים בהכרח בקודקודים החדשים v', u_1, u_2, אך לפי בניית הרדוקציה, ניתן להגיע לשם רק דרך v ושכניו. לכן, נוכל "לקצר" את המעגל ולדלג על קודקודים אלו, שכן v מחובר גם לקצה השני שלהם. מכאן, בגרף G קיים מעגל המילטון.

3. הוכיחו את המשפטים הבאים שפיזרנו עבורכם בהרצאות:
א. אם $L_1 \leq_P L_2$ וגם $L_2 \in NP$ אזי $L_1 \in NP$.
ב. אם $L_1 \leq_P L_2$ וגם $L_1 \in NPh$ אזי $L_2 \in NPh$.
ג. תהי $L_1 \in NPC$. אזי $L_1 \in P \leftrightarrow P = NP$.

פתרון:

א. נתון כי $L_2 \in NP$ ולכן קיימת מכונה אי דטרמיניסטית M_2 המכריעה אותה בזמן פולינומי. היות ומתקיים $L_1 \leq_P L_2$, קיימת מכונה לחישוב הרדוקציה M_f הרצה בזמן פולינומי. נבנה בעזרתן מכונה א"ד המכריעה את L_1 בזמן פולינומי:
המכונה M על קלט x:
- מריצה את $M_f(x)$ ומקבלת פלט y.
- מריצה את M_2 על הקלט y ועונה כמונה.

המכונה פולינומית, שכן M_f, M_2 פולינומיות. נכונות נובעת מתקפות הרדוקציה ומנכונות M_2.

בנינו מכונה א"ד פולינומית לשפה L_1 ולכן $L_1 \in NP$.

ב. נתון כי $L_1 \leq_P L_2$ ולכן קיימת מכונה לחישוב הרדוקציה M_f הרצה בזמן פולינומי.
נתון בנוסף כי $L_1 \in NPh$ ולכן לכל שפה $L \in NP$ מתקיים $L \leq_P L_1$. במילים אחרות, לכל שפה $L \in NP$ קיימת מכונה M_{f_L} פולינומית לרדוקציה ממנה אל L_1. לכן, לכל שפה $L \in NP$ קיימת רדוקציה לשפה L_2: הרדוקציה תהיה $M_f\left(M_{f_L}\right)$. ומכאן ש $L_2 \in NPh$ לפי הגדרה.

ג. $\rightarrow$: היות ו-$L \in NPC$ אזי גם $L \in NP$. אך $P = NP$ ולכן $L \in P$.
$\leftarrow$: מהגדרת NPC, לכל $L' \in NP$ מתקיים $L' \leq_P L$. לכן, ממשפט הרדוקציה נקבל $L' \in P$, ולכן $P = NP$.

על שאלה 4 יש לענות רק לאחר הרצאה 8.

4. נניח כי קיים אלגוריתם פולינומי המכריע את השפה $SubsetSum$, נקרא לו A. כתבו בעזרתו אלגוריתם לחיפוש פתרון לשפה $SubsetSum$.

פתרון:

להלן אלגוריתם למציאת פתרון לשפה $SubsetSum$ בהינתן אלגוריתם פולינומי A להכרעתה.
תזכורת: $SubsetSum = \{< S, t > | \exists S' \subseteq S: \sum_{x \in S} x = t\}$

- הרץ את $A(< S, t >)$. אם התקבל 0 החזר "אין פתרון".
- אתחל קבוצה ריקה S'.
- אתחל סוכם $c = 0$.
- לכל $i = 1 \ldots |S|$ (פסודו קוד איננו $Java$!):
  - $c += S_i$.
  - $S' = S' \cup \{S_i\}$.
    - הרץ $A(< S \setminus S', t - c)$. אם A ענה 1-
      המשך לאיטרציה הבאה $(i++)$

- אחרת: $S' = S' \setminus \{S_i\}$,
  $c -= S_i$,
  המשך לאיטרציה הבאה $(i++)$
- אם הגענו לאיטרציה בה $t - c = 0$ – עצור.

- החזר את S'.

הסבר: אם הקלט בשפה, קיימת תת קבוצה שסכומה בדיוק t. כל איבר ניסינו לקחת לקבוצת הפתרון, ובדקנו האם שאר הבעיה עדיין פתירה. אם כן, האיבר אכן חלק מהפתרון. אם לא, לא ניקח אותו לקבוצת הפתרון ונעבור לאיבר הבא.
אם הקלט לא בשפה, כבר בהרצה הראשונה נחזיר "אין פתרון".

האלגוריתם פולינומי, שכן לכל איבר הרצנו בדיקה פולינומית, ויש כמות פולינומית (ליניארית) של איברים.

בהצלחה!