חישוביות וסיבוכיות – תרגיל 4

1)א)

נוכיח שקילות לבעיה הפתוחה $P = NP \cap CO-NP$

$(\rightarrow)$

$P \subseteq P^{NP \cap CO-NP}$ נריץ את אותו אלגוריתם של P ולא נשתמש בגישה לאורקל.

$(\leftarrow)$ (שקילות לבעיה הפתוחה)

$P^{NP \cap CO-NP} \subseteq P$, ידוע כי $P \subseteq NP \cap CO-NP$ אך לא ידוע אם ההכלה היא שלמה (שוויון).

- אם $P = NP \cap CO-NP$ - אזי $P^{NP \cap CO-NP} = P^P = P$ מכיוון שלא יעזור להשתמש באורקל (נבצע את מה שהאורקל מבצע במקום לקרוא לו) כי האורקל יחסוך זמן פולינומי ואנו יודעים כי פולינומי בחזקת פולינומי זה עדיין זמן פולינומי, ולכן במקרה ש $P = NP \cap CO-NP$ קיבלנו שוויון.
- אם $P \neq NP \cap CO-NP$ - יהי $S' \in \left(NP \cap CO-NP\right) \setminus \mathrm{P}$ ועל פי הגדרת הבעיה $S' \notin \mathrm{P}$ (בהכרח קיימת כזאת כי החיתוך לא שווה) כעת נרצה להראות כי $S' \in P^{NP \cap CO-NP}$.
האלגוריתם יוגדר באופן הבא: יקרא לאורקל של S' (קיים אורקל כי $S' \in NP \cap CO-NP$) ותחזיר את התשובה.
כמובן שאלגוריתם זה פולינומי ולכן $P \neq P^{NP \cap CO-NP}$

1)ב)

הוכחה

ראינו בתרגולים כי קיימת רדוקציה מכל בעיה בco-NP לבעיה משלימה בNP (באופן דומה בכיוון השני), לכן נרצה להראות שיוויון בין $NP^{NP} = NP^{NP \cap CONP}$.

$(\rightarrow)$

$NP^{NP} \subseteq NP^{NP \cap CONP}$ - ברור

$(\leftarrow)$

$NP^{NP} \supseteq NP^{NP \cap CONP}$

בכל פעם שהמוודא יקרא לאורקל שבCONP, המוודא שלנו יבצע רדוקציה לבעיה המתאימה בNP (בהכרח יש כזאת),ישאל את האורקל ויחזיר את התשובה ההפוכה, בכל פעולה אחרת של המוודא נחזיר את אותה התשובה.

לכן הראינו $NP^{NP} = NP^{NP \cap CONP}$

לכן נשאר להראות כי $NP^{NP} = NP$ (מצד שמאל לימין ברור) מצד ימין לשמאל, בכל פעם שהיינו קוראים לאורקל ב NP^{NP}) המוודא שלנו יבצע זאת בעצמו וזה יישאר בזמן פולינומי כי האורקל עצמו הוא בעיה בNP שהיא פולינומית.

1)ג(

הוכחה

נראה כי לכל K מתקיים, $NP^{\Sigma k+1} = \Pi_{k+1}$

$S \in NP^{\Sigma_K}$ זאת אומרת כי קיים אלגוריתם פולינומי V ופולינום P כך ש

$$X \in S \Leftrightarrow \exists y_1 \mid y_1 \le P\left(|x|\right) \wedge V\left(x, y_1\right) = 1$$

ולV יש גישת אורקל לבעיות Σ_k ,מכיוון שלV יש גישת אורקל לבעיות ב Σ_k נבנה

(להעתיק מאופיר את התמונה)

ולכן $S \in \Sigma_{k+1}$ ולכן $NP^{\Sigma k+1} = \Pi_{k+1}$

כעת נראה שלכל K קיים $P^{\Pi_t} = \Pi_{t+1}$

$S \in P^{\Pi_{t+1}}$ זאת אומרת כי קיים אלגוריתם פולינומי V בעל גישת אורקל ל Π_{t+1} ופולינום P כך ש

$$X \in S \Leftrightarrow \exists y_1 \mid y_1 \le P\left(|x|\right) \wedge V\left(x, y_1\right) = 1$$

ולV יש גישת אורקל לבעיות ב Π_{t+1}, מכיוון שלV יש גישת אורקל לבעיות ב Π_{t+1} נבנה v' מתאים שלא משתמש באורקל ונקבל

$$x \in S \Leftrightarrow \underbrace{\exists y_1}_{\in NP} \forall_{y2} \exists y_3 \ldots. Q_{k+1} y_{k+1} :| y_1 |\le p\left(|\mathrm{x}|\right) : \mathrm{v}'\left(x_1, \mathrm{y}_1, y_2 \ldots. y_{k+1}\right) = 1$$

לכן $S \in \Pi_{t+1}$ (זה עובד ל2 הכיוונים כי זאת המרה שיכולה להיות דו-כיוונית ל2 הכיוונים)

כעת נראה בצורה דומה שלכל K מתקיים $S \in NP^{\Pi_K}$ קיים Q כך ש $S \in P^{\Pi_Q}$

מכיוון ש $\Pi_K \subseteq \Sigma_{K+1} \to S \in NP^{\Sigma_{K+1}}$ ולכן בצורה דומה למה שעשינו להעיל, נקבל ש $S \in \Pi_{K+2} \to S \in P^{\Pi_{K+2}}$ ולכן $Q = K + 2$, ונעשה בצורה דומה ל $S \in NP^{\Pi_K}$.

ובכך הראינו שתמיד קיים T מתאים לכל Σ_k או Π_k

2)

צריך להראות כי אם $S \in \Sigma_K$ אזי קיימים p',v' כך ש:

$$x \in S^* \Leftrightarrow \exists y_1 ... Q_k y_k \mid \forall \mathrm{y}_i \le p'(|x|) \wedge V(x, y....) = 1$$

נבנה את v' באופן הבא:

(בעזרת תכנות דינמי) כך ש'v יפצל את הקלט x לכל האופציות ששייכות לS, באופן הבא:

נתחיל מהמקום הראשון ונבדוק לכל $i \ge 2 \wedge i < x$ אם המילה מ $x_1 - x_i$ שייכת לS (בעזרת הרצת V – נדע את כל yi של הקלט לV כי אלו הyi של v' שמתאימים לו). נסמן במערך את כל המקומות j כך שמילה מסתיימת בהן ושייכת לS ומהן נמשיך לניסיון החלוקה הבאה, באותה צורה. (תמיד נלך לj הכי קרוב שנמצא אחרינו).

האלגוריתם יסיים כאשר הוא מצא מילה שמסיימת בסוף x או שהוא סיים את כל הj מהשלב הקודם ולא מצא שום מילה מתאימה לשלב הבא.

בכך נבצע מקסימום זמן פולינומי של בדיקות וכל בדיקה תהיה גם כן היא זמן פולינומי (הרצה של V אשר הוא פולינומי) ולכן V' יהיה פולינומי.

נקבע את $p' = p * x^2$

__הוכחת נכונות:__

אם אין חלוקה לx j מתאימים, ברור שלא נמצא אחת לא נכונה.

אם קיימת חלוקה לx j מתאימים, בשלב הראשון בין היתר האלגוריתם ימצא את המילה x1 המתאימה, וימשיך ממנה אל המילה הבאה המתאימה וכך הלאה.

(3

הוכחה, נראה הכלה דו-כיוונית

$P/ploy' \to P/poly$ - נבנה את העצות שינתנו ל $P/poly$ באופן הבא:

לכל i נקבע כי $a'_i = a_{i+1}$ והאלגוריתם 'A יהיה זהה לA.

<u>הוכחת נכונות:</u>

לכל קלט X נצטרך ש $\mathrm{A}\left(\mathrm{a}_{|x|}', x\right)=1$ וזה בהכרח נכון מכיוון שעל פי הגדרת העצה $a_{|x|}' = a_{|x|+1}$ ו $A\left(a_{|x|+1}\right)=1$ מהגדרת $P/poly'$.

נבנה את העצות שינתנו ל $P/ploy'$, העצה $a'_i =$ שרשור כל ה $a_j \mid j \le i$ ולכל אחד שנשרשר נרפד אותו באפסים כך שאורכו יהיה p (הפולינום שצריכים להיות חסומים ב $P/poly$)

$p' = p^* \mid x \mid$ וזה כמובן פולינומי, האלגוריתם 'A יבדוק כי אורך העצה לפחות p*|x|-1 (אם לא, יחזיר 0) , יבדוק את העצה הx (ניתן לעשות זאת כי כל העצות באותו האורך) אם $A\left(a_x, x\right)=1$ יחזיר 1 נחזיר 1 אחרת אחזר 0.

<u>הוכחת נכונות:</u>

ברור כי האלגוריתם הינו פולינומי.

צ"ל את התנאים של $P/ploy'$.

תנאי (1) - מתקיים מכיוון שכך בנינו את העצות והגדרנו את p'

תנאי (2) – מתקיים מכיוון שנחלק את העצה ה a_x המקורית ונבדוק האם $A\left(a_x, x\right)=1$ וזה בדיוק הקביעה האם $x \in S$

(4א

נרצה להראות כי אם $S \in \Sigma\Pi_2$ אזי $\overline{S} \in \Sigma\Pi_2$.

נגדיר את הרדוקציה באופן הבא – p’=p ו’v יריץ את v (אם החלפת הy והz) ויחזיר את התשובה ההפוכה.

__הוכחת נכונות:__

$x \in \overline{S}$ לכן $x \notin S$ ולכן על פי הנתון מתקיים תנאי 2 ולכן קיים z באורך המתאים שלכל y באורך המתאים V מחזיר 0 ולכן V’ עם החלפה של y וz התשובה שתחזור היא 1.

בסימטריות למקרה ההפוך כאשר $x \in S$.

4)ב

נראה הכלה של $\Sigma\Pi_2 \subseteq \Sigma_2$ והכלה של $\Sigma\Pi_2 \subseteq \Pi_2$ ונקבל על פי חוקי בדידה כי $\Sigma\Pi_2 \subseteq \Pi_2 \cap \Sigma_2$

נראה $\Sigma\Pi_2 \subseteq \Sigma_2$ - (נצטרך להראות רק שייכות של כיוון אחד לשני)

יהי $S \in \Pi\Sigma_2$ אזי קיים פולינום p ואלגוריתם דטרמיניסטי V כך ש תנאי (1) ו(2) מתקיימים, צ"ל ש:

$$x \in S \mid \exists_{y1} \forall_{y_2} \,|:|\, \mathrm{y}_i \,|\leq \mathrm{P}(|\,\mathrm{x}\,|) : V'(x, \mathrm{y}_1, y_2) = 1$$

כמובן שתנאי זה מתקיים P’=P וv’=v ואז עבור אותו y וz שהתאימו לתנאי (1) הם יתאימו לy1 וy2 בהתאמה.

4)ג

נוכיח הכלה דו-כיוונית.

- $\Sigma\Pi_2 \subseteq PH$ ראינו בהרצאה כי אם $NP \subseteq P/\mathrm{poly}$ אזי $PH = \Sigma_2 = \Pi_2$ ולכן על פי מה שהוכחנו בסעיף ב' מתקיים כי $\Sigma_2 \cap \Pi_2 = PH$ ולכן $\Sigma\Pi_2 \subseteq PH$.

- נוכיח כי $PH \subseteq \Sigma\Pi_2$, שוב על פי מה שלמדנו בהרצאה אנו יודעים כי $PH = \Sigma_2$ ולכן אם נראה כי $\Sigma_2 \subseteq \Sigma\Pi_2$ נסיים.
(בדוגמה לסעיף ב, נראה הכלה של כיוון אחד) לפי ההגדרה של התנאי של Σ_2 הוא שקול לתנאי (1) של $\Sigma\Pi_2$ ולכן כל X שיתאים לתנאי של Σ_2 אזי גם יתאים ל $\Sigma\Pi_2$ ולכן הראינו הכלה של שייכות.

ולכן אם $PH \subseteq \Sigma\Pi_2$ וגם $\Sigma\Pi_2 \subseteq PH$ אזי $\Sigma\Pi_2 = PH$ וסיימנו.