

CO-NP

הגדרה

$$CO - NP = \{\{0, 1\}^* \setminus L \mid L \in NP\}$$

דוגמה

$SAT \in NP$ אוסף הנוסחאות הספיקות.
 $\overline{SAT} \in CO - NP$ - אוסף הנוסחאות שאינן ספיקות
יהי R יחס שהינו ב- PC , ובעיית ההכרעה שלו היא לכן ב- NP :

$$NP \ni L_R \{x \mid \exists y (x, y) \in R\}$$

$$CO - NP \ni \{0, 1\}^* \setminus L_R = \{x \mid \forall y (x, y) \notin R\}$$

השערה 1

$$P \neq NP$$

השערה 2

$$NP \neq CO - NP$$

נשים \heartsuit כי השערה 2 \iff השערה 1.

הסבר: עבור P , ידוע $P = CO - P$ שכן

$$CO - P = \{\{0, 1\}^* \setminus L \mid L \in P\}$$

שכן אם אפשר להכריע בזמן פולינומי, אפשר להפוך את ההכרעה ולקבל הכרעה הפוכה בזמן פולינומי, ולכן אם $NP \neq CO - NP$ אזי אפשר להסיק $NP \neq P$.

אבחנה 1

לא תמיד קיימת רדוקציית קארפ בין L ל- \overline{L} $L \in NP$

הסבר

ניזכר כי קיימת רדוקציית קארפ מ L ל \bar{L} אם קיימת פונקציה חשיבה פולינומיאלית $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ כך ש $x \in L \iff f(x) \in \bar{L}$.

עבור $L = \emptyset$ לא קיימת רדוקציה כזאת, שכל לכל x מתקיים $f(x) \in \{0, 1\}^*$ $x \notin \emptyset$.

אבחנה 2

עבור $L \in NP$ תמיד קיימת רדוקציית קוק מ L ל \bar{L} .

הסבר

ניזכר כי רדוקציית קוק מ L ל \bar{L} היא מכונה פולינומית עם גישת אורקל ל \bar{L} , ולכן בהנתן קלט x עבורו צריך להכריע האם $x \in L$, הרדוקציה תבצע שאילתת אורקל ל \bar{L} ותהפוך את התשובה.

הערה

$$P \subseteq NP \cap CO - NP$$

השערה 3

$$P \subsetneq NP \cap CO - NP$$

טענה

אם $NP \cap CO - NP$ מכיל קבוצות שהן $NP - Hard$ אזי $NP = CO - NP$

משפט Lander (ראינו בפעם שעברה)

אם $P \neq NP$ אזי קיימת $A \in NP$ כך ש $A \notin P$ ו $A \notin NPC$.

נשים

השערה 3 והטענה לעיל מובילים למסקנה דומה למשפט Lander. ע"פ השערה 3 קיימת $A \in NP \cap CO - NP$ (ולכן $A \in NP$) וכן $A \notin P$. אם A כזו היא אינה NP -שלמה, אז מצאנו A העונה על תנאי משפט Lander:

$$A \notin P \quad A \notin NPC \quad A \in NP$$

אם A כזו היא כן NP -שלמה אזי ע"פ הטענה $NP = CO - NP$.
 לסיכום, אם $NP \neq CO - NP$ וכן השערה 3 מתקיימת אזי קיימת A ע"פ תנאי משפט Lander.

הוכחת הטענה

נניח כי קיימת $L \in NP \cap CO - NP$ שהינה NP -שלמה. נראה כי זה גורר $CO - NP \subseteq NP$. אח"כ נראה כי $(CO - NP = NP) \iff (CO - NP \subseteq NP)$.
 תהי $L' \in CO - NP$ כלשהי. מטרתנו להראות כי $L' \in NP$ (ומכך נסיק כי $CO - NP \subseteq NP$). ראשית נשי לב כי קיימת רדוקציה מ' L' ל' L .

הסבר: קיימת רדוקציה מ' $L' \in CO - NP$ ל' $L \in NP$ (כפי שהסברנו קיימת רדוקציה קוק משפה למשלימתה, זוהי רדוקציה ההופכת את תשובת האורקל) קיימת רדוקציה מ' $L \in NP$ ל' L היא NP -קשה. ולכן מטרנזיטיביות רדוקציות יש רדוקציה מ' L ל' L .

כדי להוכיח ש' $L' \in NP$, נגדיר יחס R שהוא ב' PC וכן $L' = L_R$ - כלומר L' תהיה בעיית ההכרעה המתאימה ל' R ומכך נסיק ש' $L' \in NP$.
 R יוגדר באופן הבא:

$$R = \{ (x, [(z_1, b_1, w_1), \dots, (z_t, b_t, w_t)]) | \dots \}$$

כאשר הרדוקציה מ' L ל' L מקבלת את x לאחר סדרת השאלות z_1, \dots, z_t , סדרת ותשובות b_1, \dots, b_t וכן:

- אם $b_i = 1$ - כלומר אם התשובה היא ש' $z_i \in L$ - אזי w_i יהיה עד לכך ש' $z_i \in L$.
- אם $b_i = 0$ - כלומר אם התשובה היא ש' $z_i \notin L$ (כלומר $z_i \in \bar{L}$) - אזי w_i יהיה עד לכך ש' $z_i \notin L$ - כלומר $z_i \in \bar{L}$. נזכור ש' $\bar{L} \in NP$.

$R \in PC$ בשל ההסבר הבא:
 בהנתן קלט R מהצורה $(x, [(z_1, b_1, w_1), \dots, (z_t, b_t, w_t)])$ אפשר לוודא בזמן פולינומי שהרדוקציה מ' L ל' L אכן תקבל את x עבור סדרת השאלות והתשובות האמורה. כדי לוודא זאת צריך להשתכנע בשני דברים:

א. שעבור סדרת השאלות z_i וסדרת התשובות b_i הרדוקציה מ' L ל' L אכן מקבלת את x . זאת ניתן לעשות בזמן פולינומי כי הרדוקציה היא פולינומית.

ב. צריך להשתכנע בכך שסדרת התשובות b_i אכן מתאימה לסדרת תשובות של האורקל ל' L עבור השאלות z_i . זאת ניתן לעשות בזמן פולינומי ע"י שימוש בעדים w_i וכן ע"י שכנוע ש' $L \in NP \cap CO - NP$, ולכן ישנם עדים קצרים גם לכך ש' $z_i \in L$, וגם לכך ש' $z_i \notin L$ - כלומר $z_i \in \bar{L}$.

ולכן $L' \in NP$ (כי היא בעיית ההכרעה המתאימה ל' R) ולכן הסקנו ש' $CO - NP \subseteq NP$.
 כעת נראה כי $CO - NP = NP$. נניח בשלילה כי השוויון לא מתקיים, ולכן קיימת $a \in NP \setminus CO - NP$:

$$\bar{a} \in CO - NP \subseteq NP$$

$$\bar{a} \in NP$$

$$a \in CO - NP$$

וזו סתירה להנחה ש $a \in NP \setminus CO - NP$, ולכן קיבלנו שאם $CO - NP \subseteq NP$ אז למעשה $CO - NP = NP$.

תזכורת(מחישוביות): NP סגור לרדוקציות קארפ

כלומר אם קיימת רדוקציית קארפ מ' L ל' L' , וכן $L \in NP$, אזי $L' \in NP$.

הסבר

כזכור רדוקציית קארפ מ' L ל' L' היא f חשיבה פולינומית $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ כך ש:

$$f(x) \in L \iff x \in L' \iff \text{קיים מוודא } V' \text{ ופולינום } P' \text{ כך ש}$$

$$\exists_y |y| < P'(|f(x)|), V'(f(x), y) = 1$$

$$L' \in NP \iff \boxed{\exists_y |y| < P(|x|), V(x, y) = 1} \iff \begin{matrix} V(x, y) = V'(f(x), y) \\ P(|x|) = P'(|f(x)|) \end{matrix} \text{ נגדיר } NP$$

NP אינו סגור(כנראה) לרדוקציות קוק

ז"א אם קיימת רדוקציית קוק מ' L ל' L' וכן $L \in NP$, אזי לא ניתן להסיק $L' \in NP$.

הסבר

תהי $L = \overline{SAT}$. אזי $\bar{L} = SAT$. קיימת רדוקציית קוק מ' \overline{SAT} ל' SAT (כמקודם, זוהי רדוקציה שהופכת את תשובת האורקל). כמו כן $SAT \in NP$. אילו NP היה סגור לרדוקציות קוק אז היינו מסיקים כי $\overline{SAT} \in NP$ ולכן $SAT \in CO-NP \cap NP$. אבל SAT היא NP -שלמה וזה גורר ע"פ הטענה שהראינו ש $CO-NP = NP$ (ומשערים שזהו אינו המצב).

- Polynomial-time Heirarchy - PH

ההיררכיה הפולינומית

PH הינה מחלקה שמכלילה את NP ואת $CO - NP$. PH סגורה לרדוקציות קוק, וכן נראה כי מתקיים ש $PH = P \iff NP = P$.

הגדרה

עבור $k \in \mathbb{N}$ נגדיר Σ_k באופן הבא:
נאמר $A \in \Sigma_k$ אם קיים מוודא פולינומי V ופולינום $P(\cdot)$ כך שלכל $x \in \{0, 1\}^*$ מתקיים

$$\underbrace{\exists y_1 \forall y_2 \exists y_3 \cdots Q_k y_k}_{|y_i| < P(|x|)} V(x, y_1, y_2, \dots, y_k) = 1 \iff x \in A$$

כאשר $Q_k = \exists$ אם k אי זוגי, $Q_k = \forall$ אם k זוגי.

אבחנה

$$NP = \Sigma_1 \quad P = \Sigma_0$$

הגדרה

$$PH = \bigcup_{k=0}^{\infty} \Sigma_k$$

נשים \heartsuit ש PH היא אכן היררכיה - לפחות במובן חלש, כלומר $\Sigma_k \subseteq \Sigma_{k+1}$ (נובע מהגדרה).

דוגמה

$$\text{Clique} = \{ \langle G, k \rangle \mid G \text{ is a graph with } k\text{-sized clique} \}$$

$$\text{Clique} \in NP = \Sigma_1$$

$$\text{Max-Clique} = \{ \langle G, k \rangle \mid G \text{ is a graph where the maximal clique is of size } k \}$$

Max-Clique לא ידוע להיות שייך ל Σ_1 .

$$\text{Max-Clique} \in \Sigma_2 \quad \text{טענה:}$$

הסבר: קיים V ופולינום $P(\cdot)$ כך ש

$$\underbrace{\exists c_1 \forall c_2}_{|c_i| < P(|\langle G, k \rangle|)} V(\langle G, k \rangle, c_1, c_2) = 1 \iff \langle G, k \rangle \in \text{Max-Clique}$$

$V(\langle G, k \rangle, c_1, c_2) = 1$ אם c_1 הוא קליק בגודל k ו c_2 אינו קליק, או שהוא קליק בגודל קטן או שווה ל k .

הגדרה

עבור $k \in \mathbb{N}$ נגדיר את Π_k להיות:

$$\Pi_k = CO - \Sigma_k = \{ \{0, 1\} \setminus L \mid L \in \Sigma_k \}$$

אבחנה

$$\Pi_0 = P \quad \Pi_1 = CO - NP$$

הסבר 1

נשים לב כי:

$$x \notin \bar{A} \iff x \in A \text{ ש } P(\cdot) \text{ ופולינום } V \text{ קיים מוודא פולינומי } V \iff A \in \Pi_k$$

\iff

$$\neg \left(\underbrace{\exists y_1 \forall y_2 \dots Q_k y_k}_{|y_i| < P(|x|)} V(x, y_1, y_2, \dots, y_k) = 1 \right)$$

\iff

$$\underbrace{\forall y_1 \exists y_2 \dots Q_k y_k}_{|y_i| < P(|x|)} V(x, y_1, y_2, \dots, y_k) = 0$$

ע"י סדרת k כמתים שמתחילה בכמת \forall .
התכונות הבאות נובעות מההגדרה של Π_k ו Σ_k :

1. $\Pi_k \subseteq \Pi_{k+1}$

2. $\Pi_k \subseteq \Sigma_{k+1}$

3. $\Sigma_k \subseteq \Pi_{k+1}$

הסבר 2

$P(\cdot), V, A \in \Pi_k$

$$\underbrace{\forall y_1 \exists y_2 \dots Q_k y_k}_{|y_i| < P(|x|)} V(x, y_1, \dots, y_k) \iff x \in A$$

נגדיר:

$$V'(x, y_1, \dots, y_{k+1}) = V(x, y_2, \dots, y_{k+1})$$

$$P'(|x|) = P(|x|)$$

$$\exists_{y_1} \forall_{y_2} \cdots Q_{k+1} y_{k+1} V(x, y_1, \dots, y_{k+1}) \iff x \in A$$

מסקנה

$$PH = \bigcup_{k=0}^{\infty} \Pi_k$$