סיבוכיות – הרצאה 2

כל העולם הוא חישוב אחד גדול

1.3.11

רדוקציות

רדוקציות הן מונח מתמטי לטענה "שפה A קלה יותר משפה B" ($A \leq B$).

רדוקצית Karp (מיפוי)

רדוקצית $Karp$ משפה $A \subseteq \{0,1\}^*$ לשפה $B \subseteq \{0,1\}^*$ היא פונקציה $f : \{0,1\}^* \to \{0,1\}^*$ המקיימת:

$$\forall x \in \{0,1\}^* \quad x \in A \Leftrightarrow f(x) \in B$$

זה לא חוכמה כי הרדוקציה יכולה להכריע קודם את A ותחזיר תמיד קלט שרירותי מ-B.
נסמן $A \underset{\text{P}}{\leq} B$ אם קיימת רדוקציית $Karp$ מ־A ל-B שניתן לממש בזמן פולינומיאלי.
כל פעם שנאמר רדוקציה (אלא אם כן מצויין אחרת) נתכוון לרדוקציית $Karp$.

תזכורת.

1. אם $A \underset{\text{P}}{\leq} B, B \underset{\text{P}}{\leq} C$ אז $A \underset{\text{P}}{\leq} C$.
2. אם $A \underset{\text{P}}{\leq} B$ אז $\overline{A} \underset{\text{P}}{\leq} \overline{B}$ (ע"י אותה הרדקוציה).
3. המחלקה $P = \bigcup_{k=1}^{\infty} Time(n^k)$ סגורה תחת רדוקציות פולינומיאליות. כלומר,

$$\forall A, B \quad A \underset{\text{P}}{\leq} B, B \in P \quad \Rightarrow \quad A \in P$$

הסבר: נניח שקיימת מ"ט שרצה בזמן פולינומיאלי ומכריעה את B. כמו כן, תהא f רדוקציה פול' מ-A ל-B. נכריע את A באופן הבא: בהינתן קלט x נחשב את $f(x)$ ונפעיל את מכונת הטיורינג שנכריעה את B על $f(x)$ ונחזיר את תשובתה. הנכונות נובעת מכך ש- $x \in A \Leftrightarrow f(x) \in B$. זמן הריצה הוא פול' מאחר שהרכבת פולינומים (פולינום זמני הריצה של f ושל הכרעת B) היא פולינום.

דוגמא. ניקח את בעיית מעגל המילטון:

$$HamCycle = \{G | \text{G גרף מכוון שיש בו מעגל המילטון}\}$$

ובעיית מסלול המילטון:

$$HamCycle = \{G|\text{G גרף מכוון שיש בו מסלול המילטון}\}$$

נראה $HamPath \leq_{\text{p}} HamCycle$. הרדוקציה: בהינתן קלט גרף $G = (V, E)$ הרדוקציה תחזיר את $G' = (V', E')$ כאשר $V' = V \cup \{u\}$, $E' = E \cup (V \times \{u\}) \cup (\{u\} \times V)$.
נכונות: $G \in HamPath \Leftrightarrow G' \in HamCycle$. אם ב-$G$ יש מסלול המילטון $v_1 \to v_2 \to \ldots \to v_n$ אז ב-G' יש מעגל המילטון: $v_1 \to v_2 \to \ldots \to v_n \to u \to v_1$.
אם ב-G' יש מעגל המילטון $v_1 \to \ldots \to v_n \to u \to v_1$ אז $v_1 \to \ldots \to v_n$ הוא מסלול המילטון ב-G.
ניתן לממש את הרדוקציה בזמן פולינומיאלי בגודל הקלט.

רדוקציית Cook (פול')

רדוקציית $Cook$ משפה $A \subseteq \{0,1\}^*$ לשפה $B \subseteq \{0,1\}^*$ היא אלגוריתם (בזמן ריצה פולינומיאלי) שמכריע את A תוך שימוש באלגוריתם נתון שמכריע את B כאשר זמן הריצה להכרעת קלט של B הוא צעד אחד.
סימון: $A \underset{Cook}{\leq} B$.
נשים לב כי: $A \underset{Cook}{\leq} \Leftrightarrow A \in P^B$.

הערה. רדוקציית $Karp$ היא למעשה מקרה פרטי של רדוקציית $Cook$ כי ברדוקציית $Karp$ לצורך הכרעת A ניתן להשתמש בשאילתא אחת לאורקל ולהחזיר תשובה כמו שהיא.

דוגמא. נראה כי $HamCycle \underset{\text{Cook}}{\leq} HamPath$
או באופן שקול $HamCycle \leq P^{HamPath}$. נתאר אלגוריתם שמכריע את $HamCycle$. קלט $G = (V, E)$. לכל קשת $(u, v) \in E$ נבדוק האם $(V \cup \{z, w\}, E \cup \{(w, v), (u, z)\})$
אם נקבל כן בלפחות אחת מהקריאות נקבל ואחרת נדחה.

דוגמא. כזכור עבור שפה $A \subseteq \{0,1\}^*$ מגדירים:

$$A^* = \{y|\exists k \in \mathbb{N}_0 \quad y = x_1 \ldots x_k, \forall i \in \{1, \ldots, k\} x_i \in A\}$$

למשל אם $A = \{00, 01, 10, 11\}$. אז $A^* = \{x \in \{0,1\}^* : |x| \in \mathbb{N}_{even}\}$

טענה. לכל A, $A^* \in P^A$ (כלופר) $A^* \underset{\text{Cook}}{\leq} A$.

הוכחה. נראה אלגוריתם שמכריע את A^* בעזרת גישה לאורקל A. נסמן את הקלט ב-$x = x_1 x_2 \ldots x_n \in \{0,1\}^*$. נגדיר גרף מכוון G_x על קבוצת הצמתים $V = \{0, \ldots, n\}$ ונחבר בקשת מכוונת $i \to j$ אם תת המילה $x_{i+1} x_{i+2} \ldots x_j \in A$. כעת נבדוק (למשל ע"י BFS) אם יש ב- G_x מסלול מכוון מ-0 ל-n. אם כן נקבל ואחרת נדחה.
נכונות: $x \in A^*$ קיימים $0 = i_1 < i_2 < \ldots < i_k = n$ כך שלכל j, $x_{i_j+1} \ldots x_{i_{j+1}} \in A$
$\Leftrightarrow$ קיים מסלול מכוון ב- G_x מ-0 ל-n.
זמן הריצה: פולינומיאלי בגודל הקלט n משום שדרושות $O(n^2)$ קריאות לאורקל וכן הרצת BFS מצריכה זמן לינארי בגודל הגרף ולכן פול' ב- n. □

חישוב אי-דטרמיניסטי

במ"ט דטרמיניסטית יש פונקציית מעברים $\delta : Q \times \Gamma \to Q \times \Gamma \times \{R, L\}$. במכונת טיורינג אי דטרמיניסטית: $\delta : Q \times \Gamma \to P(Q \times \Gamma \times \{R, L\})$.
מ"ט אי-דטרמיניסטית מכריעה שפה A אם לכל x, $x \in A$ אם ורק אם קיים תסריט ריצה של M על x שמוביל אותה למצב מקבל (כאשר $x \notin A$ כל תסריט ריצה יוביל למצב דחייה).

הערה. כל הדיון הוא לגבי מכונות טיורינג שעוצרות על כל קלט.

הגדרה. $NTime(f)$ מחלקת השפות שניתן להכריע ע"י מכונת טיורינג אי דטרמיניסטית בזמן $f(n) \leq$ על קלט באורך n.

הגדרה.

$$NP = \bigcup_{k=1}^{\infty} NTime(n^k)$$

כזכור $SAT = \{\varphi | \varphi$ היא נוסחאת בולאנית מצורת CNF ספיקה$\}$, $SAT \in NP$.
הגדרה שקולה:

הגדרה. מחלקת השפות $A \in \{0,1\}^*$ עבורן קיימים מ"ט דטרמיניסטית שרצה בזמן פוינומיאלי ופולינום p כך ש-

$$\forall x \in \{0,1\}^* . x \in A \Leftrightarrow \exists w \in \{0,1\}^{p(|x|)} . M(x,w) = T$$

הביטוי לעובדה שהעד שלנו צריך להיות פולינומיאלי במכונה האי דטרמיניסטית הוא שמספר הצעדים במכונה הוא ופלינומיאלי, עד משכנע הוא הניחושים שעשינו ולכן לכל היותר פולינומיאלי.

חיפוש לעומת הכרעה

גרסת החיפוש של SAT מוגדרת כך: $SAT - Search$ קלט - נוסחאת CNF φ.
מטרה: למצוא השמה מספקת ל- φ או להחזיר שאין כזו.

טענה. $SAT \in P$ אם ורק אם קייס אלגוריתם עם זמן ריצה פולינומיאלי בגודל הקלט שפותר את $SAT - Search$.

הוכחה. ברור שאם ניתן לפתור את $SAT - Search$ הזמן פולינומיאלי אז ניתן גם להכריע בזמן כזה את SAT (נריץ אותו האלגוריתם, אם מצא השמה נקבל ואחרת נדחה).
כעת נראה רדוקצית $Cook$ מבעיית החיפוש לבעיית ההכרעה. נסמן את הקלט ב- φ. תחילה נבדוק האם $\varphi \in SAT$ ואם לא נחזיר שאין השמה מספקת. נסמן משתני φ ב- $x_1, \ldots, x_n$.
כעת נגדיר שתי נוסחאות φ_0, φ_1 המתקבלות מ- φ ע"י הצבה $x_1 = true$, $x_1 = false$ בהתאמה. נשים לב שלפלחות אחרת מהשתיים ספיקות (כי בהשמה מספקת של φ יש ל- x_1 ערך אמת כלשהו. נקבע את ערכו של x_1 לפי זו שספיקה ונמשיך עם $n-1$ המשתנים שנותרות.
נמשיך כך הלאה. מספר הקריאות להכרעת SAT הוא לכל היותר $2n$ ולכן פולינומיאלי בגודל הקלט.

□

תזכורת. שפה A היא C-קשה אם $\forall B \in C, B \leq_{\mathrm{P}} A$.

תזכורת. שפה A היא C שלמה אם $A \in C$ וגם A היא C - קשה.

משפט. *Cook-Levin*
SAT היא NP שלמה.

דוגמא. נגדיר שפה,

$$TMSAT =$$
$$= \{\langle M, x, 1^n, 1^t\rangle | \text{ קיים } u \in \{0,1\}^* \text{ עבורו מ"ט } M \text{ מקבלת את } \langle x, u\rangle \text{ תוך } t \text{ צעדים } \}$$

הוכחה. תחילה נראה ש- $TMSAT \in NP$. עבור קלט $\langle M, x, 1^n, 1^t\rangle$
ניקח כעד $u \in \{0,1\}^n$ ונסתכל על מ"ט דט' M' שמסמלצת את t הצעדים בראשונים של ריצת M על $\langle x, u\rangle$ אם M תקבל תוך t צעדים M' תקבל ואחרת תדחה. מהגדרת $TMSAT$ ברור שקיים u כזה אם ורק אם הקלט בשפה.
נשים לב ש- M' מצריכה $O(t^2)$ צעדים ולכן זמן פולינומיאלי בגודל הקלט (שארוך מ- t).
כעת נראה ש- $TMSAT$ היא NP קשה. תהא $A \in NP$ אזי קיימת מכונת טיורינג M דטרמיניסטית שרצה בזמן $q(n)$ על קלט באורך n (q פולינום) וקיים פולינום עבורו

$$\forall x \in A \Leftrightarrow \exists w \in \{0,1\}^{p(|x|)}.M(x, w) = T$$

נוכיח $A \leq_{\text{p}} TMSAT$. הרדוקציה: קלט x ל- A ימופה ל- $\langle M, x, 1^{p(|x|)}, 1^{q(|x|)}\rangle$
נשים לב ש- $x \in A \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} M(x, u) = 1$ וכן זמן ריצת M על $\langle x, u\rangle$ לכל היותר $q(|x|) \Leftrightarrow \langle M, x, 1^{p(|x|)}, 1^{q(|x|)}\rangle$ ב- $TMSAT$.
זמן ריצת הרדוקציה פולינומיאלי ב- $|x|$: $O(1) + O(|x|) + O(p(|x|)) + O(q(|x|))$.
□

שאלה: האם NP סגורה לרדוקציות $Karp$ פול'? האם היא סגורה לרדוקציות $Cook$ פול'?
סגירות -
$$\forall A, B.B \in NP, A \leq B \Rightarrow A \in NP$$

אכן סגורה לרדוקציות $Karp$. תהא f רדוקציה פול' מ-A ל-B כעד לכך ש- $x \in A$ ניקח את העד ש- $f(x) \in B$. ניתן לחשב את $f(x)$ ולוודא שייכותו ל-B בזמן פול'.
שאלה: האם $P^{SAT} = NP$?
נשים לב ש- $\overline{SAT} \in P^{SAT}$ כי בהינתן φ ניתן לשאול את האורקל אם φ ספיקה ולהחזיר את התשובה ההפוכה. ואילו לא יודע אם $\overline{SAT} \in NP$.
אז אנחנו לא יודעים להוכיח את הסגירות לרדוקציות $Cook$.

המחלקה $coNP$

עבור מחלקת סיבוכיות C מגדירים את $coC = \{\overline{A} | A \in C\}$.
תכונות:

1. $co(coC) = C$.
2. $C_1 \subseteq C_2 \Rightarrow coC_1 \subseteq coC_2$. מדוע? נניח $C_1 \subseteq C_2$. תהא $A \in coC_1$ לכן $\overline{A} \in C_1$ לכן $\overline{A} \in C_2$ כלומר $A \in coC_2$.

אבחנה. $coP = P$.

שאלה פתוחה ידועה היא האם $NP = coNP$? או באופן שקול האם $\overline{SAT} \in NP$?

הערה. אם $NP \subseteq coNP$ אז $NP = coNP$. נניח $NP \subseteq coNP$ נפעיל co על שני האגפים: $coNP \subseteq co(coNP)$ ולכן $coNP \subseteq NP$.

אבחנה. $\overline{SAT}$ היא $coNP$ שלמה.

הסבר: NP SAT שלמה:

$$\begin{cases} SAT \in NP \\ \forall A \in NP \quad A \underset{\text{P}}{\leq} SAT \end{cases}$$

לכן,

$$\begin{cases} \overline{SAT} \in coNP \\ \forall A \in NP \quad \overline{A} \underset{\text{P}}{\leq} \overline{SAT} \end{cases}$$

ולכן נוכל לכתוב:

$$\begin{cases} \overline{SAT} \in coNP \\ \forall A' \in coNP \quad A' \underset{\text{P}}{\leq} \overline{SAT} \end{cases}$$

טענה. $P^{SAT} = NP$ אם ורק אם $NP = coNP$.

רעיון: כדי להוכיח שאם $NP = coNP$ אז $P^{SAT} = NP$ עלינו לסמלץ מכונת טיורינג שמשתמשת באורקל ל- SAT תוך שימוש בעד. העד יכיל את תשובות האורקל לאורך הריצה ועדויות לנכונותן (במקרה של נוסחא ספיקה זו ההשמה המספקת) ועבור נוסחא לא ספיקה גם יש עד קצר שניתן למצוא בגלל ההנחה $NP = coNP$