סיבוכיות - הרצאה 5

כל העולם הוא חישוב אחד גדול

22.3.11

ההירכיה הפולינומיאלית

תזכורת.

$$IS = \{(G,k) | k \text{ יש קבוצה ב"ת בגודל } G\text{–ב}\}$$

$(G,k) \in IS \Leftrightarrow$ קיימת קבוצה של k צמתים שכל שניים מהם אינם מחוברים. וזה תכונה שאפשר לבדוק בזמן פולינומיאלי.

$(G,k) \in IS \Leftrightarrow$ לכל קבוצה של k צמתים שניים מהם מחוברים בקשת. גם זאת תכטנה שאפשר לבדוק בזמן פולינומיאלי.

ראינו גם בעיות שההגדרה שלהם משתמשת ביותר מכמת אחד:

$$MAX - IS = \{(G,k) | k \text{ גודל הקובצה הב"ת הגדולה ביותר ב–} G \text{ הוא}\}$$

$(G,k) \in MAX-IS \Leftrightarrow$ קיימת קבוצה של k צמתים שכל שניים מהם אינם מחוברים ולכל קבוצה של $k+1$ צמתים יש שניים שמחוברים.

הגדרה. Σ_2 היא מחלקת השפות $A \subseteq \{0,1\}^*$ עבורן קיימים מ"ט דטרמיניסטית שרצה בזמן פולינומיאלי M ופולינום p כך ש–

$$\forall x \in \{0,1\}^* \qquad x \in A \Longleftrightarrow \exists u \in \{0,1\}^{p(|x|)}.\forall v \in \{0,1\}^{p(|x|)}.M(x,y,v) = T$$

נשים לב, $NP \subseteq \Sigma_2$, $coNP \subseteq \Sigma_2$, $MAX-IS \in \Sigma_2$.

הגדרה. $\Pi_2 = co\Sigma_2$ כלומר, $\Pi_2 = \{\overline{A} | A \in \Sigma_2\}$.

או באופן שקול: Π_2 היא מחלקת השפות $A \subseteq \{0,1\}^*$ עבורן קיימים מ"ט דטרמיניסטית שרצה בזמן פולינומיאלי M ופולינום p כך ש–

$$\forall x \in \{0,1\}^* \qquad x \in A \Longleftrightarrow \forall u \in \{0,1\}^{p(|x|)}.\exists v \in \{0,1\}^{p(|x|)}.M(x,y,v) = T$$

הערה. שלילה של הפסוק המתאר את Σ_2 דורש להחליף את הערך של המכונה ל–F. אבל המכונה דטרמיניסטית לכן זה לא באמת משנה.

נשים לב: $MAX-IS \in \Pi_2$, $NP \cup coNP \subseteq \Pi_2$.

דוגמא.

$$MIN-CIRCUIT=\left\{C \middle| \begin{array}{l} C \text{ מעגל בוליאני קטן ביותר בגודלו} \\ \text{שמחשב את הפונקציה } x\mapsto C(x) \end{array} \right\}$$

כאשר קטן ביותר מתייחס לגדול קידוד המעגל - כולל את מספר השערים ומספר הצמתים.
נראה ש- $MIN-CIRCUIT\in\Pi_2$.
$C\in MIN-CIRCUIT \Leftrightarrow$ לכל מעגל בוליאני C' שקטן מ- C, המעגלים C ו- C' אינם מחשבים את אותה הפונקציה $\Leftrightarrow$ לכל C' מעגל שקטן מ-C קיים קלט x למעגלים עבורו $C(x)\neq C'(x)$.
נגדיר מכונת טיורינג M שבהינתן (C,u,v) היא מפרשת את u כמעגל בוליאני C' ו-v כקלט למעגלים הללו ובודקת ש- $|C|\geq|C'|$ או ש- $C(x)\neq C'(x)$.
נשים לב, שדי לקחת את p מהגדרת Π_2 להיות פונקציה לינארית. u שהוא מתיימר המעגל הקטן יותר הוא בברור לינארי בגודל מעגל הקלט ו- v הוא קלט לכן לא עולה על גודל המעגל.

הגדרה. Π_2SAT:
קלט: נוסחאת CNF φ מעל שתי קבוצות משתנים $u=u_1,\dots,u_n$, $v=v_1,\dots,v_n$.
שאלה: האם $\forall u\exists v\varphi(u,v)$ פסוק אמת?

הערה. בעזרת הוכחה דומה לזו של משפט Cook אפשר להראות ש- Π_2SAT היא Π_2 שלמה (תחת רדוקציות פולינומיאליות כמובן).

שתי המחלקות Σ_2, Π_2 מגדירות את הרמה הראשונה של ההירכיה. לעיתים מסמנים: $NP=\exists P$, $coNP=\forall P$. באופן דומה: $\Sigma_2=\exists\forall P$, $\Pi_2=\forall\exists P$, $\Sigma_3=\exists\forall\exists P$, $\Pi_3=\forall\exists\forall P$, ...

אבחנה. לכל i:

$$\Sigma_i\subseteq\Sigma_{i+1}\quad \Sigma_i\subseteq\Pi_{i+1}$$

$$\Pi_i\subseteq\Pi_{i+1}\quad {\scriptstyle \Pi_i\subseteq\Sigma_{i+1}}$$

פשוט אם נתעלם מהכמת הראשון.
כמו כן, $\Pi_i=co\Sigma_i$.

הגדרה.

$$PH=\bigcup_{i\geq 1}\Sigma_i$$

באופן שקול,

$$PH=\bigcup_{i\geq 1}\Pi_i$$

וזאת ההירכיה הפולינומיאלית.

שאלה מעניינת היא האם באמת כל מחלקה מכילה ממש את קודמתה או שבשלב כלשהו ההירכיה קורסת, כלומר האם החל ממקום מסויים כל המחלקות שוות. וזאת באמת שאלה פתוחה.

משפט. אם $P=NP$ אז $P=PH$.

כלומר ההיררכיה הפולינומיאלית קורסת לרמה ה־0.

$$\begin{tikzcd}
\vdots & & \vdots \\
\Sigma_3 \arrow[u] \arrow[urr] & & \Pi_3 \arrow[u] \arrow[ull] \\
\Sigma_2 \arrow[u] \arrow[urr] & & \Pi_2 \arrow[u] \arrow[ull] \\
NP \arrow[u] \arrow[urr] & & coNP \arrow[u] \arrow[ull] \\
& P \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

כרגיל חצים הם הכלה.

הוכחה. נראה שתחת הנחה זו $\Sigma_2 = P$ ובאופן דומה (למשל באינדוקציה) ניתן להכליל זאת ל- Σ_i.
נראה שכל שפה שאפשר להכריע ב- Σ_2 אפשר להכריע ב- P.
תהא $A \in \Sigma_2$ אזי קיימת מ"ט דטרמיניסטית פולינומיאלית M וקיים פולינום p כך ש:

$$\forall x \quad x \Longleftrightarrow \exists u \in \{0,1\}^{p(|x|)} \forall v \in \{0,1\}^{p(|x|)} M(x,u,v) = T$$

נגדיר שפה A':

$$A' = \{(x,u) | \forall v \in \{0,1\}^{p(|x|)} . M(x,v,u) = T\}$$

נשים לב ש- $A' \in coNP$ לפי הגדרתה (כי p פולינום ו- M מכונת טיורינג דטרמיניסטית פולינומיאלית). לכן מההנחה $A' \in P$ ולכן קיימת מכונת טיורינג דטרמיניסטית, פולינומיאלית M' שמכריעה את A'.
קיבלנו,

$$\forall x \quad x \Longleftrightarrow \exists u \in \{0,1\}^{p(|x|)} M'(x,u) = T$$

כלומר הצלחנו להוריד כמת. מהתיאור $A \in NP$ (כי M' דטרמיניסטית פולינומיאלית, p פולינום) ולכן לפי ההנחה $A \in P$. $\square$

קל למצוא שפה שלמה לכל שלב בהיררכיה, פשוט ניקח את המתאימה ל- SAT עם כמתים מתאימים. כעת, טבעי לשאול האם יש שפה ששלמה בהיררכיה הפולינומיאלית? כלומר שתהיה ב- PH ותהיה גם PH–קשה.

הגדרה. $TQBF$:
קלט: נסוחא בוליאנית עם כמתים $\forall / \exists x_1 \forall / \exists x_2 \ldots \forall / \exists x_n \varphi(x_1, \ldots, x_n)$
שאלה: האם הנוסחא היא אמת?

דוגמא.

$$\forall x \exists y (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \in TQBF$$

כי לכל x יש y ששונה ממנו.

הערה. לא ברור האם $TQBF \in PH$ כי לא ניתן למצוא i קבוע עבורו $TQBF \in \Sigma_i$.

טענה. אם קיימת שפה PH שלמה (תחת רדוקציות פולינומיאליות) אז ההירכיה הפולינומיאלית קורסת.

הסבר. נניח ש- A היא PH-שלמה בפרט $A \in PH$ אז קיים i עבורו $A \in \Sigma_i$. נשים לב שמאחר ש- A היא PH-קשה, כל שפה PH שייכת ל-Σ_i ולכן $PH = \Sigma_i$.

משפט. $TQBF$ היא $PSpace$ שלמה. כלומר $TQBF \in PSpace$ וכן $TQBF$ היא $PSpace$-קשה.
מה זה $PSpace$ קשה?

$$\forall A \in PSpace \qquad A \leq_{\mathrm{p}} TQBF$$

רדוקצית זמן פולינומיאלית.

טענה. $TQBF \in PSpace$.

הוכחה. הקלט הוא נוסחא בוליאנית עם כמתים. $\forall/\exists x_1 \forall/\exists x_2 \ldots \forall/\exists x_n \varphi$ עם n משתנים. נסמן את אורך הנוסחא ב- m.
נתאר פרוצדורה רקורסיבית שכריע האם מדובר בפסוק אמת. נציב $x_1 = T$ ונבדוק רקורסיבית האם הפסוק אמיתי ואז נציב $x_1 = F$ ונבדוק האם הפסוק אמיתי. לצורך הריצות האלה נשתמש באותו מקום על הסרט. אם הכמת הוא $\forall$ נקבל אם ורק אם שתי הקריאות קיבלו ואם הכמת הוא $\exists$ נקבל אם ורק אם אחת הקריאות קיבלה.
עומק הרקורסיה הוא n ובכל הפעלה רקורסיבית אורך הנוסחא $\geq m$ ולכן (בגלל השימוש באותו מקום) אנו משתמשים ב- $O(m \cdot n)$ מקום על הסרט וזהו מקום פולינומיאלי בגודל הקלט $\square$

לא נראה השיעור שהיא $PSpace$ קשה. במקום זה:

שאלה. מהי המחלקה P^{TQBF}?

הערה.

$$PH \subseteq PSpace \subseteq EXP$$

מסתבר ש- $P^{TQBF} = PSpace$.