סיבוכיות – תרגול 6

כל העולם הוא חישוב אחד גדול

29.03.11

ההירכיה הפולינומיאלית

ראינו כבר הגדרה של המחלקה $\Sigma_2(\exists\forall P)$.

תזכורת. Σ_2 היא מחלקת השפות $A \subseteq \{0,1\}^*$ עבורן קיימת מכונת טיורינג דטרמיניסטית פולינומיאלית M ופולינום p כך שלכל $x \in \{0,1\}^*$:

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

תרגיל. הוכיחו כי $\Sigma_2 = NP^{SAT}$.

הוכחה. תחילה נראה $\Sigma_2 \subseteq NP^{SAT}$. תהא $A \in \Sigma_2$. אזי קיימים מכונת טיורינג דטרמיניסטית פולינומיאלית M ופולינום p כל שלכל $x \in \{0,1\}^*$:

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

נגדיר

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

נשים לב ש- $A' \in coNP$ ולכן $\overline{A'} \in NP$. מכאן, יש רדוקציה פולינומיאלית f מ- $\overline{A'}$ ל- SAT (כי NP SAT קשה). נגדיר מכונת טיורינג אי-דטרמיניסטית M' שבהינתן קלט x תנחש $u \in \{0,1\}^{p(|x|)}$, תבנה את הנוסחא $f(\langle x,u\rangle)$ ותשאל את האורקל האם $f(\langle x,u\rangle) \in SAT$.
המכונה M' תחזיר תשובה הפוכה לתשובת האורקל.

נכונות: $x \in A \Leftrightarrow$ קיים $u \in \{0,1\}^{p(|x|)}$ עבורו $\langle x,u\rangle \in A' \Leftrightarrow$ קיים u עבורו $\langle x,u\rangle \notin \overline{A'}$ $\Leftrightarrow$ קיים u עבורו $f(\langle x,u\rangle) \notin SAT$ $\Leftrightarrow$ קיים תסריט ריצה של המכונה M' עבורו M' מקבלת את x.
זמן הריצה של M' פולינומיאלי כי אורך העד u פולינומיאלי וכן ניתן לממש את f בזמן פולינומיאלי.

כעת נראה $NP^{SAT} \subseteq \Sigma_2$. תהא $A \in NP^{SAT}$ אזי קיימת מכונת טיורינג M אי־דטרמיניסטית שרצה בזמן פולינומיאלי עם אורקל ל- SAT ומכריעה את A.
עבור קלט x נסמן ב- k את מספר הקריאו לאורקל של המכונה M בריצתה על x. נבחר u, v באופן הבא:
u יכיל:

- חלק z שיכיל את סדרת הניחושים האי־דטרמיניסטיים של המכונה M בריצתה על x.

- היינו רוצים לקחת סדרת תשובות האורקל $a_1,\ldots,a_k \in \{0,1\}$ בריצת M על x. הבעיה שאם הקלט לא בשפה אולי קיימת סדרת תשובות (לא נכונות כמובן) שבהתאם לתשובות המכונה תגיע למצב מקבל. כדי שזה כן יעבוד נוסיף משהו נוסף:
- רשימת השמות $u_1,\ldots,u_k$.

v יכיל: רשימת השמות $v_1,\ldots,v_k$
נגדיר מכונת טיורינג M' שבהינתן קלט x ו- u,v כנ"ל מסמלצת את M על x: במקום ניחושים אי־דטרמיניסטיים M' תשתמש ב- z ובמקום קיראות לאורקל נפעל לפי התשובות $a_1,\ldots,a_k$ כמו כן לכל i אם M $a_i=1$ תבדוק ש- u_i היא השמה מספקת עבור φ_i (כאשר φ_i היא הנוסחא עבורה האורקל נדרש להכריע האם ספיקה בפעם ה- i) ואם M' $a_i=0$ תבודק ש- v_i היא השמה שאינה מספקת את φ_i. אם אחד מאלה לא מתקיים M' תדחה. אחרת, M' תחזיר את תוצאת הריצה של M.

נכונות: $x\in A \Leftrightarrow$ קיימת סדרת ניחושים z עבורה M מקבלת את $x \Leftrightarrow$ קיימת סדרת ניחושים z וקיימות תשובות אורקל נכונות $a_1,\ldots,a_k$ עבורן M מקבלת את $x \Leftrightarrow$ קיימת סדרת ניחושים z ותשובות $a_1,\ldots,a_k$ של האורקל כך שלכל i כך ש- $a_o=1$ קיימת השמה מספקת u_i ל- φ_i ולכל i כך ש- $a_i=0$ כל השמה v_i אינה מספרקת את φ_i, כך ש-M מקבלת את $x \Leftrightarrow$ קיים u עבורו לכל v M' מקבלת את $\langle x,u,v\rangle$.

המכונה M' רצה בזמן פולינומיאלי משום שמסמלצת את M שזמן ריצתה פולינומיאלי וכן הבדיקה האם השמה מספקת נוסחא ניתנת למימוש בזמן פולינומיאלי.
האורך של v,u פולינומיאלי: סדרת הניחושים z היא באורך פולינומיאלי כי זמן הריצה של M הוא פולינומיאלי וכל בחירה אי־דטרמיניסטית מצריכה $O(1)$ תווים. מספר הקריאות לאורקל (k) גם הוא חסום ע"י זמן הריצה M ולכן רשימת התשובות a_i וגם ההשמות v_i,u_i היא באורך פולינומיאלי ב- $|x|$. □

האם NP^{SAT} סגורה למשלים? לא ידוע. שקול לשאלה האם $\Sigma_2=\Pi_2$.
האם P^{SAT} סגורה למשלים? כן. זאת מחלקה דטרמיניסטית לכן לכל מכונת טיורינג M שמכריעה שפה A ניתן להחליף ב- M את המצבים המקבל והדוחה ולקבל מכונת טיורינג שמכריעה את $\overline{A}$ ולכן $\overline{A}\in P^{SAT}$.