סיבוכיות - תירגול 4

אורקלים

P^O היא מחלקת השפות שניתן להכריע בזמן פולי' תוך שימוש באורקל O.

נגדיר: $P^P=\bigcup_{O\in P}P^O$, $P^{NP}=\bigcup_{O\in NP}P^O$, $P^{SAT}=P^{NP}$.

SAT שלמה ולכן כמו שימוש באורקל כלשהו ויותר.

<u>טענה:</u> $P^P=P$. לא תורם לכוח המחלקה.

<u>הסבר:</u> ברור ש- $P\subseteq P^P$. כי ניתן לא להשתמש באורקל, ונכריע אותה בזמן פולינומיאלי.

נראה ש: $P^P\subseteq P$. בהינתן שפה $L\in P^P$, קיימת מ"ט פולי' M שמכריעה את L תוך שימוש באורקל O עבורו קיים אלגוריתם שרץ בזמן $q(n)$.

נסמן את זמן ריצת M ב-$p(n)$ (p, q פולינומים). נראה ש $L\in P$!

נסמלץ את M וכל פניה לאורקל ← נפעיל את האלגוריתם שמכריע את O. כל קלט לאורקל באורך $\le p(n)$ (חסום ע"י זמן הריצה) והפעלת האלגוריתם של O תצריך $q(p(n))$ צעדים. בסה"כ זמן הריצה יהיה $\le p(n)\cdot q(p(n))$, וזהו זמן פולי' (פולינומים סגורים לכפל והרכבה).

<u>שאלה:</u> האם $EXP^{EXP}=EXP$?

$$EXP=\bigcup_{c\ge 1}DTIME(2^{n^c})$$

צד אחד, ברור. כי ניתן לא להשתמש באורקל.
האם ניתן לעשות סימולציה כמו קודם?

<u>תשובה:</u> כעת לא ניתן לבצע סימולציה של EXP^{EXP} בזמן אקספוננציאלי משום שהקלט לאורקל עשוי להיות באורך 2^n והפעלת האלגוריתם שמכריע את האורקל תצריך $\underbrace{2^{(2^n)}}_{\text{כפול אקספ'}}$ צעדים. (פונקציות אקספ' אינן סגורות להרכבה).

<u>כזכור, משפט היררכיית הזמן:</u> לכל f,g המקיימות $g(n)=\omega(f(n)\cdot\log f(n))$ מתקיים $DTIME(f(n))\subsetneq DTIME(g(n))$ ולכן $P\subsetneq EXP\subsetneq DTIME(2^{(2^n)})$.

<u>טענה:</u> $EXP^{EXP}\ne EXP$.

<u>הוכחה:</u> נראה ש- $DTIME(2^{(2^n)})\subseteq EXP^{EXP}$ וממשפט היררכיית הזמן נסיק $EXP^{EXP}\ne EXP$.

נגדיר: $EXP\ni EXPCOM=\{\langle M,x,1^n\rangle \mid$ M מחזירה 1 על x תוך 2^n צעדים$\}$

זה אקספ' לאורך הקלט כי הוא באורך n (1^n).

תהא L שפה ב-$DTIME(2^{(2^n)})$, אזי קיימת מכונת טיורינג M שמכריעה את L ורצה בזמן $c\cdot 2^{(2^n)}$. נראה ש- $L\in EXP^{EXPCOM}$: בהינתן קלט x, נשאל את האורקל האם הקלט $\langle M,x,1^{2^{n}}\rangle$ ($|x|=n$) שייך ל- EXPCOM ונחזיר את התשובה.

ניתן לבצע את זה בזמן אקספוננציאלי ב-|x|.

<u>נכונות:</u> $\forall x.\ x \in L \Leftrightarrow \langle M, x, 1^{2^{|x|+c}} \rangle \in EXPCOM$

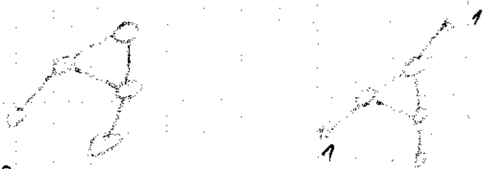
כי זמן הריצה של M הוא $2^{(2^n)}$ ... י יכול להיות אפס!

<u>סימונים:</u>

$\exists P = NP$. $\forall P = coNP$. $\exists\forall P = \Sigma_2^p$. $\forall\exists P = \Pi_2^p$

<u>המחלקה Π_2^p</u> היא מחלקת השפות L שעבורן קיימים מ"ט פולי' M ופולינום p כך ש- $\forall x \in \{0,1\}^{p(|x|)}.\ x \in L \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}.\ \exists v \in \{0,1\}^{p(|x|)}.\ M(x,u,v) = 1$

<u>דוגמה:</u> $A = \{G \mid$ כל 3-צביעה של הצלעות של G ניתנת להשלמה ל-3-צביעה חוקית של G $\}$



קיימת צביעה לא חוקית, כמו

שתי צביעות חוקיות כמשלו

$G \in A \Leftrightarrow$ <u>לכל</u> צביעה של הצלעות של G, <u>קיימת</u> צביעה של שאר צמתי G, כך שהצבעים חוקית (כל שני צמתים סמוכים צבועים שונה).

u יהיה קידוד של צביעת הצלעות של G, v קידוד של צביעת שאר צמתי G

$G \in A \Leftrightarrow \forall u.\ \exists v.\ \underbrace{M(G,u,v)=1}$

המכונה בודקת בזמן פולינומיאלי שהצביעה (u,v) חוקית עבור G.

לכן השפה נמצאת ב-Π_2^p.

<u>שאלה 4 תרגול ב:</u> נראה רדוקציה שמשמרת את מספר הפתרונות מ-SAT ל-3SAT.

<u>ניסיון 1:</u> מדוע הרדוקציה הרגילה לא משמרת: $(w_1 \vee w_2 \vee w_3 \vee w_4) \rightarrow (w_1 \vee w_2 \vee u) \wedge (w_3 \vee w_4 \vee \bar{u})$

רדוקציה זו לא משמרת מספר פתרונות (יש השמה של u ו-$\bar{u}$ עבור חלק מהמקרים).

<u>ניסיון ב:</u> $(\underbrace{w_1 \vee w_2}_{u} \vee w_3 \vee w_4) \rightarrow (u \vee w_3 \vee w_4) \wedge \underbrace{(u \leftrightarrow (w_1 \vee w_2))}$

כדי שיסתפק, חייבים לספק את $w_1 \vee w_2$, כי אחרת הפסוקית השניה לא תסתפק.

נכתוב כ-3 cnf:

$(u \rightarrow (w_1 \vee w_2)) \wedge ((w_1 \vee w_2) \rightarrow u) \equiv$

$\overset{(*)}{\equiv} (\bar{u} \vee w_1 \vee w_2) \wedge ((\bar{w}_1 \wedge \bar{w}_2) \vee u) \equiv (\bar{u} \vee w_1 \vee w_2) \wedge (\bar{w}_1 \vee u) \wedge (\bar{w}_2 \vee u)$

(*) $(A \rightarrow B) \equiv (\neg A \vee B)$

עבור יותר מ-4 ליטרלים, נפצל פסוק ב-1 ואז זה עדיין פולי' (עד n המשתנים ליטרלים)

הכוונה היא שזה $u \Leftrightarrow (w_1 \vee w_2)$

שווה (נכון למראית) "מספיק" זה כמשהו חשב