30.3.09 סיבוכיות - שיעור 5

(1)

סיבוכיות זמן
- P
- NP
- EXP, NEXP
- Σ_2^p, Π_2^p
- היררכיית הזמן
- אורקלים

<u>הגדרה</u> $EXP = \bigcup_{c\geq 1} DTIME(2^{n^c})$

$NEXP = \bigcup_{c\geq 1} NTIME(2^{n^c})$

<u>משפט:</u> אם $EXP \neq NEXP$ אז $P \neq NP$

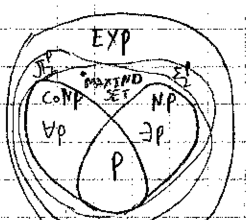
<u>הוכחה:</u> נניח ש $P=NP$ ונוכיח ש- $EXP=NEXP$.
מספיק להוכיח כי $NEXP \subseteq EXP$

תהא L שפה כלשהי ב- $NEXP$. לכן, קיים אלגוריתם אי דטרמיניסטי M שמכריע את L בזמן 2^{n^c} עבור איזשהו c.

נגדיר שפה חדשה: $L_{pad} := \{\langle x, 1^{2^{|x|^c}}\rangle : x\in L\}$

אנו טוענים ש- $L_{pad}\in NP$: נראה אלגוריתם אי דטרמיניסטי ל- L_{pad} שפועל בזמן פולינומיאלי: בהינתן קלט, הוא קודם בודק שהוא מהצורה $\langle x, 1^{2^{|x|^c}}\rangle$ עבור איזשהו x. אם כן, מפעיל את M על x ומחזיר את תשובתו של M. זמן הריצה של המכונה הוא $2^{|x|^c}$ וזה לינארי בגודל הקלט.

כיוון ש- $P=NP$, $L_{pad}\in P$. מכך נובע שיש אלגוריתם שרץ בזמן אקספוננציאלי ל- L. האלגוריתם: בהינתן קלט x, מכין את המחרוזת $\langle x, 1^{2^{|x|^c}}\rangle$ וקורא לאלגוריתם של L_{pad} ומחזיר את תשובתו. זמן הריצה הוא $poly(2^{|x|^c}) = 2^{O(|x|^c)}$ ולכן $L\in EXP$.



<u>מחלקות Π_2^p, Σ_2^p [ספר AB 5.1]</u>

<u>דוגמא</u> נגדיר שפה MIN-DNF: בהינתן קלט $\langle u,k\rangle$ כאשר u נוסחת DNF, k מספר, האם קיימת נוסחת DNF ψ בגודל $\leq k$ כך ש $u\equiv\psi$.

* ניתן להגדיר את Σ_2^p כ- $\exists\forall P$ (קיים, כך שלכל..., מתקיים P) ואת Π_2^p ניתן להגדיר כ- $\forall\exists P$ (לכל, קיים, כך ש-P). *\

<u>הגדרה:</u> Σ_2^p היא מחלקת השפות L שיש עבורן מכונת טיורינג פולינומיאלית ופולינום p כך ש:

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

<u>הערה:</u> קל לראות ש- $MIN\text{-}DNF \in \Sigma_2^p$ כי התנאי אומר: "קיימת ψ כך שלכל y $\underline{\varphi(y)=\psi(y)}$" תנאי פולינומי

בנוסף, MIN-DNF היא Σ_2^p-שלמה.

<u>הגדרה:</u> Π_2^p מוגדרת בצורה דומה רק $\forall\exists$ במקום $\exists\forall$

<u>הגדרה שקולה</u> $\Pi_2^p = \{\bar{L} : L\in\Sigma_2^p\}$ (תרגיל: הוכיחו ששקול)

u.multinet.co.il

<u>הגדרה:</u> MAXINDSET - בהינתן גרף G ומספר k, האם גודל הקבוצה הבלתי תלויה הגדולה ביותר ב-G היא <u>בדיוק</u> k?

ניתן לבטא את התנאי כ:

"קיימת קבוצה חברים S בגודל k כך שלכל קבוצת חברים T בגודל k+1 אין ב-S קשתות ויש ב-T קשתות."

או:

"לכל קבוצה T בגודל k+1 קיימת קבוצה S בגודל k כך שב-S אין קשתות וב-T יש קשתות."

<u>תרגיל:</u> הראו ש-MAXINDSET שייך ל-$\Pi_2^p \cap \Sigma_2^p$ (נובע ישירות ממה שאמרנו קודם).

<u>הערה:</u> בעצם הבעיה היא DP-שלמה.

<u>תרגיל:</u> הראו ש-NP ו-coNP מוכלים ב-Σ_2^p וב-Π_2^p.

<u>הערה:</u> אפשר להמשיך ולהגדיר Σ_3^p, Π_3^p וכך הלאה והאיחוד של כל אלה נקרא ההיררכיה הפולינומיאלית, מסומן PH.

<u>משפט:</u> $P = NP \Rightarrow \Sigma_2^p = P$ (ובעצם $PH = P$)

<u>הוכחה:</u> נניח ש-$P=NP$ ונראה ש-$\Sigma_2^p=P$. תהי L שפה כלשהי ב-Σ_2^p. לפי ההגדרה, קיים אלגוריתם M ופולינום p, כך ש-:

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

נגדיר שפה

$$L' := \{\langle x,u\rangle : u \in \{0,1\}^{p(|x|)},\ \forall v \in \{0,1\}^{p(|x|)}\ M(x,u,v)=1\}$$

מההגדרה נובע ש-$L' \in coNP$, כיוון ש-$P=NP$ גם $coNP=P$ ולכן $L'\in P$. לכן, קיים אלגוריתם פולי' M' שמכריע את L'. כלומר קיבלנו ש:

$$x\in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}.\ M'(x,u)=1$$

הפעם נשתמש ב-$P=NP$ על מנת לקבל ש-$L\in P$. ∎

<u>משפט</u> היררכיית הזמן [AB 3.1]

<u>משפט</u> לכל פונקציות f,g כך ש-$g(n)=\omega(f(n)\log f(n))$ (כלומר, $\lim_{n\to\infty}\frac{f(n)\log f(n)}{g(n)}=0$), (למשל $g(n)=n^4$, $f(n)=n^2$), מתקיים: $DTIME(f(n)) \subsetneq DTIME(g(n))$.

	M_0	M_1	M_{00}	M_{01}	...
0					
1					
00					
01					
11					
⋮					

<u>הערה:</u> ניתן לבנות את מכונת הטיורינג האוניברסלית, כך שזמן הריצה שלה על הזוג $\langle x,\alpha\rangle$ הוא $c\cdot T\log T$ כאשר T הוא זמן הריצה של M_α על x ו-c הוא קבוע שתלוי ב-α אבל לא ב-x.

<u>הערה:</u> נניח שלכל מכונת טיורינג יש אינסוף ייצוגים α (למשל, ניתן להוסיף רווחים בסוף).

<u>הוכחה:</u> נגדיר בעית הכרעה בדרך הבאה: בהינתן קלט α, האם כאשר נפעיל את מכונת הטיורינג האוניברסלית U למשך $g(|\alpha|)$ צעדים על מנת לסמלץ את M_α על קלט α, היא תעצור ותענה 0?

מההגדרה נובע שהבעיה ניתנת לחישוב בזמן $O(g(n))$

על מנת להראות שהבעיה לא ב-$DTIME(f(n))$, ניקח מכונה כלשהי M ונראה שהיא לא מצליחה לחשב את הבעיה בזמן $O(f(n))$.

נניח ש-α הוא קוד המתאר את M ונסתכל על קלט α לבעיה שלנו. אם המכונה M על קלט α עוצרת בתוך זמן T שמאפשר למכונה האוניברסלית לסמלץ אותה בזמן $g(|\alpha|)$ אז קיבלנו שהתשובה ש-M מוצאת על הקלט α היא מהגדרה לא נכונה ולכן המכונה M נכשלה.

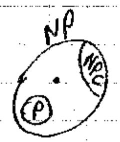
אחרת, קיבלנו שזמן הריצה T של M על הקלט α הוא כך ש $c \cdot T\log T > g(|\alpha|)$ (כאשר c הוא קבוע שתלוי במכונה M).

כיוון שיש אינסוף קלטים α שעליהם M רצה זמן T כך ש- $c T\log T > g(|\alpha|)$, מכך נובע שלא ייתכן ש-M רצה בזמן אסימפטוטי $O(f(n))$ (כי אם היתה כזו, זמן הריצה שלה היה לכל היותר $c \cdot f(n)$ עבור n גדול מספיק, בסתירה למה שראינו).

מהמשפט נסיק כי $DTIME(n) \subsetneq DTIME(n^2) \subsetneq \dots \subsetneq P \subseteq DTIME(n^{\log n}) \subsetneq \dots \subsetneq EXP \subsetneq DTIME(2^{2^n}) \dots\dots$

$\subseteq DTIME(n^{\log\log n})$

<u>אורקלים ומכונות אורקל</u>



(אם $P \neq NP$)

<u>הגדרה</u> תהא $O \subseteq \{0,1\}^*$ שפה כלשהי. אלגוריתם עם גישה לאורקל O זה אלגוריתם שיש לו פקודה מיוחדת שמאפשרת לפתור את O בצעד אחד (קריאה לאורקל).

(סמן אלגוריתם כזה בצורה M^O. בצורה דומה נגדיר אלגוריתמים אי דטרמיניסטים ונגדיר P^O וגם NP^O כצפוי במכונות אלו!)

<u>טענה</u> $\overline{SAT} \in P^{SAT}$.

<u>הוכחה:</u> נפעיל את האורקל על הקלט φ ונענה את ההפך.

<u>טענה</u> תהא $O \in P$ אז $P^O = P$.

<u>הוכחה:</u> $P \subseteq P^O$: ברור, אין צורך לקרוא ל-O.

$P^O \subseteq P$: ברור, ניתן לסמלץ בפולינום את הקריאות ל-O. ∎

נראה עכשיו עולם שבו $P = NP$.

<u>טענה</u> נגדיר: $EXPCOM = \{\langle \alpha, x, 1^n \rangle :$ M_α מוציא 1 על קלט x תוך 2^n צעדים$\}$

אז $P^{EXPCOM} = NP^{EXPCOM} = EXP$.

u.multinet.co.il

<u>הוכחה:</u> $EXP \overset{①}{\subseteq} P^{EXPCOM} \overset{②}{\subseteq} NP^{EXPCOM} \overset{③}{\subseteq} EXP$

① תהא $L \in EXP$ שפה כלשהי ותהא M_α אלגוריתם שפותר את L בזמן 2^{n^c} עבור איזשהו c.

נבנה אלגוריתם שמשתמש ב- EXPCOM וזה בזמן פולינומיאלי: על הקלט x, מחזיר את תשובת האורקל על: $\langle \alpha, x, 1^{n^c} \rangle$.

② לא נשים לב שיכול להיות מצב בו $P \subseteq NP$ אך כשמוסיפים אורקל זה לא מתקיים אז/

ברור כי כל מכונה דטרמיניסטית היא בפרט מכונה אי דטרמיניסטית, גם עם אורקל (אין במילים אחרות, אפשר תמיד להתעלם מהעץ).

③ בזמן אקספוננציאלי אפשר לעבור על כל הבחירות האי-דטרמיניסטיות האפשריות וגם לחשב את תשובת האורקל.

∎

זה מראה לנו שבעזרת טכניקות שנקראות relativizing, לא נוכל להוכיח ש- $P \neq NP$. אלו טכניקות הוכחה שלא מסתכלות בקוד של התוכנה אלא רק בקופסה שאפשר לסמלץ תוכנה נתונה בצורה יעילה.

בפרט, זה כולל הוכחות כמו ההוכחה שראינו להיררכיית הזמן (לומר לכסון) כי רק השתמשנו בקידוד של מכונות על ידי קוד + האפשרות לסמלץ אותו.

<u>תרגיל:</u> הראו שלכל f,g, $g(n)=\omega(f(n)\log f(n))$ ולכל O, $DTIME^O(f(n)) \subsetneq DTIME^O(g(n))$.

האם אין ניתן להראות ש- $P=NP$ בעזרת לכסון?

<u>משפט:</u> [BAKERGILL SOLOVAY 76] קיים אורקל A שעבורו $P^A \neq NP^A$.

<u>הוכחה:</u> לכל שפה A, נגדיר את השפה $U_A = \{1^n : \text{קיימת מחרוזת } x \in A \text{ באורך } n\}$

לכל A שנבחר מתקיים ש- $U_A \in NP^A$ כי הבדיקה נכונה להגיע לנו איפה נמצא את המחרוזת $x \in A$. נותר לבנות A כך ש- $U_A \notin P^A$.

U_A הנה מצב ↓

A:
0, 1
00, 01, 10, 11
000, 001, 010, 011, 100, 101, 110, 111