# סיבוכיות / תרגיל בית #4

אריאל סטולרמן

**(1)**

(a) $DTIME(2^n) \subsetneq NTIME(2^{2n})$ : **הטענה נכונה**

תחילה נראה כי $DTIME(2^n) \subsetneq DTIME(2^{2n})$ : נגדיר $f(n) = 2^n$ ו-$g(n) = 2^{2n}$. ברור כי $g(n) = \omega(f(n) \cdot \log f(n))$ שכן $\lim_{n\to\infty} \frac{f(n)\cdot \log f(n)}{g(n)} = \lim_{n\to\infty} \frac{2^n \cdot n}{2^n \cdot 2^n} = \lim_{n\to\infty} \frac{n}{2^n} = 0$. ממשפט היררכית הזמן נובע כי $DTIME(2^n) \subsetneq DTIME(2^{2n})$.

כמו כן, ברור כי $DTIME(2^{2n}) \subseteq NTIME(2^{2n})$, שכן לכל אלג׳ דטר׳ הרץ בזמן $O(2^{2n})$ הוא בפרט אלג׳ לא דטר׳ הרץ בזמן $O(2^{2n})$ (פשוט ללא פיצולים לא דטר׳). מכאן ש: $DTIME(2^n) \subsetneq NTIME(2^{2n})$, כנדרש.

(b) $P \neq NP \text{ or } NP \neq EXP$ : **הטענה נכונה**

נסתכל על השלילה הלוגית של הטענה: $P = NP \text{ and } NP = EXP$. משלילה זו נובע כי $P = EXP$, אך זו בסתירה למש פט היררכית הזמן, שכן ידוע למשל עבור $f(n) = n, g(n) = 2^n$ ש-$DTIME\big(f(n)\big) \subsetneq DTIME(g(n))$, כאשר $DTIME\big(f(n)\big) \subseteq P$ ו-$DTIME\big(g(n)\big) \subseteq EXP$ (כלומר קיימות שפות ב-$EXP$ שאינן ב-$P$). כיוון ששלילה זו לא נכונה, אזי הטענה המקורית נכונה.

(c) $\exists k > 0 \; s.t. \; NP \subseteq DTIME(n^k)$ : **שקול לשאלה פתוחה**

ידוע כי $P = \bigcup_{c\geq 1} DTIME(n^c)$, ולפיכך $\forall k > 0. DTIME(n^k) \subseteq P$. כמו כן ידוע כי $P \subseteq NP$ (טרוויאלי – כל שפה הניתנת להכרעה בזמן דטר׳ פולי׳ בפרט ניתנת להכרעה בזמן לא דטר׳ פולי׳). מכאן שאם הטענה היתה נכונה היה מתקיים $P = NP$, וזו שאלה פתוחה.

(d) $\forall L \in NP \bigcap coNP. NP^L = NP$ : **הטענה נכונה**

$NP \subseteq NP^L$: טרוויאלי; כל שפה הניתנת להכרעה בזמן פולי׳ לא דטר׳, ניתנת להכרעה בזמן פולי׳ לא דטר׳ עם אורקל $L$ – פשוט ע״י אותו אלג׳ ללא שימוש באורקל.

$NP^L \subseteq NP$: תהי $L \in NP \bigcap coNP$, ותהי $L' \in NP^L$. נראה כי $L' \in NP$. ולפיכך קיים אלג׳ פולי׳ לא דטר׳ המכריע את $L$. יהי $p$ פולינום כך שהאלג׳ המכריע את $L$ עושה זאת בזמן $p(n)$ לא דטר׳. $L' \in NP^L$ ולפיכך קיים פולינום $q$ ואלג׳ עם אורקל $L$ המכריע את $L'$ בזמן $q(n)$ לא דטר׳. ניתן לסמלץ את האלג׳ האחרון כך שבמקום לקרוא לאורקל, לקרוא לאלג׳ המכריע את $L$ בזמן $p(n)$ לא דטר׳. כל קלט של אלג׳ זה יהיה לכל היותר באורך $q(n)$, ולכן הרצת האלג׳ של $L$ עליו תהיה לכל היותר בזמן $q \circ p(n)$ לא דטר׳. סה״כ נקבל אלג׳ הרץ בזמן $p \cdot q \circ p(n)$ לא דטר׳ המכריע את $L'$, ולכן $L' \in NP$.

לבסוף, קיבלנו כי לכל $L \in NP \bigcap coNP$ מתקיים כי $NP^L = NP$, כנדרש.

**(2)**

(a) תהי $\Sigma_2^p SAT = \{\psi \mid \psi = \exists x_1, \dots, x_n \forall y_1, \dots, y_n. \varphi(x_1, \dots, x_n, y_1, \dots, y_n) \; is \; True; \varphi \in CNF\}$.

מהגדרת השפה קל לראות כי $\Sigma_2^p SAT \in \Sigma_2^p$, שכן ניתן לנסחאות ה-$CNF$ $\varphi$ מעל $x_1, \dots, x_n, y_1, \dots, y_n$ ($n$ מספר טבעי כלשהו) כך שקיימות הצבות ל-$x_1, \dots, x_n$ כך שלכל הצבה ל-$y_1, \dots, y_n$ הנוסחה $\varphi$ מסתפקת. ממשפט שנלמד בהרצאה ידוע כי $P = NP \Leftrightarrow \Sigma_2^p = P$, ולפיכך $\Sigma_2^p \in P$.

(b)

נראה תחילה כי $\Pi_2^p$ - $(2,3) - CE = \{< G, S > | S \subseteq V(G), every \; 2 - col \; of \; S \; is \; extendible \; to \; 3 - col \; of \; V\}$ היא שפה ב- $x \in (2,3) - col \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}. \exists v \in \{0,1\}^{p(|x|)}. M(x,u,v) = 1$ : $< G, S \geq x \in \{0,1\}^*$ מכונת טיורינג פולי׳ ופולינום $p$ כך שלכל

נניח תחילה כי $< G, S > \in (2,3) - CE$, אזי לכל 2-צביעה של $S$ קיימת הרחבה ל-3 צביעה של כל $G$. המ״ט תקבל כ-$u$ כל צביעה אפשרית של $S$, וכ-$v$ את הצביעה המשלימה לה, ותבדוק שהצביעה חוקית. ברור כי אורך כל הצביעה הוא פולי׳ בגודל $V(G)$ וכי בדיקת חוקיות הצביעה פולי׳ בגודל $G$. לפיכך המ״ט פולי׳ ונכונה.

נניח כעת כי $\forall u.\exists v.M(x,u,v)=1$ (כמתואר לעיל). מהגדרה, לכל 2-צביעה של $S$ המתקבלת מ-$u$ קיימת הרחבה ל-3-צביעה של כל $V(G)$ המתקבלת מ-$v$ כך שהצביעה $u,v$ של קודקודי $G$ חוקית. מהגדרת השפה נובע כי $x\in(2,3)-CE$. מהגדרה נובע כי $(2,3)-CE\in\Pi_2^p$, כנדרש.

נראה כעת כי $(2,2)-CE\in coNP$. מהגדרה, $<G,S>\in(2,2)-CE$ אם לכל 2-צביעה של $S$ קיימת הרחבה ל-2-צביעה של כל $V(G)$ כך שצביעה זו חוקית. מאותם שיקולים של החלק הראשון נובע כי $(2,2)-CE\in\Pi_2^p$, כלומר קיימת מ"ט פולי' $M$ ופולינום $p$ כך שלכל $x\in\{0,1\}^*$ מתקיים: $x\in(2,2)-CE\Leftrightarrow\forall u\in\{0,1\}^{p(|x|)}.\exists v\in\{0,1\}^{p(|x|)}.M(x,u,v)=1$. נגדיר את השפה הבאה:

$L=\{<G,S,v>|v\in\{0,1\}^{p(|x|)},\ \forall u\in\{0,1\}^{p(|x|)}.M(x,u,v)=1\}$. מהגדרה נובע כי שפה זו היא ב-$coNP$. ברור כי $x\in(2,2)-CE$ אמ"מ $<G,S,v>\in L$. בדיקת קיום $v$ כנדרש, דהיינו קיום השלמת צביעה ל-2-צביעה חוקית שקולה לבדיקת קיום 2-צביעה חוקית בכל $G$, ובדיקה זו הינה פולינומיאלית (קיימת 2-צביעה חוקית אמ"מ לא הגרף דו"צ, כלומר ללא מעגלים שליליים, וזאת ניתן לבדיקה ע"י $BFS$ בזמן פולי'). לפיכך ניתן לבדוק בזמן פולי' לא דטר' שלכל 2-צביעה חוקית של $S$ קיימת השלמה ל-2-צביעה חוקית של כל $G$. מהגדרה נובע כי $(2,2)-CE\in coNP$.

**(3)**

*(a)* להלן הוכחה כי $NTIME(n)\subseteq DTIME(n^{10})\Rightarrow P=NP$:

נניח כי $NTIME(n)\subseteq DTIME(n^{10})$, אזי כל אלג' הרץ בזמן לא דטר' $n$ ניתן לסמלץ ע"י אלג' דטר' הרץ בזמן $n^{10}$. תהי $L\in NP$, אזי קיים $k\geq 1$ ואלג' הרץ בזמן $n^k$ לא דטר' המכריע את $L$. נגדיר שפה חדשה $L_{pad}=\{<x,1^{|x|^k}>|x\in L\}$. נגדיר אלג' המכריע את $L_{pad}$: בהינתן קלט, בודק שהוא אכן מהצורה $<x,1^{|x|^k}>$, ואם לא מיד דוחה. אם כן, נריץ על $x$ את האלג' המכריע את $L$, ונחזיר את תשובתו. האלג' רץ בזמן לא דטר' $n^k$. כיוון שאורך הקלט הוא $n+n^k=O(n^k)$, ונסמן אורך הקלט ל-$L_{pad}$ כ-$m$, אזי האלג' המכריע את $L_{pad}$ רץ בזמן לא דטר' $m$. לפי הנחה, ניתן לסמלץ אלג' זה ע"י אלג' דטר' הרץ בזמן $m^{10}=n^{10k}$, כלומר אלג' פולי'. כיוון שברור ש-$<x,1^{|x|^k}>\in L_{pad}\Leftrightarrow x\in L$, אזי $L\in P$, ולכן $NP\subseteq P$. כיוון שידוע ש-$P\subseteq NP$, נקבל כי $P=NP$, כנדרש.

*(b)*

נניח כי לכל $L\in NP, L\subseteq\{1^*\}$ מתקיים כי $L\in P$. נראה $EXP=NEXP$:

$EXP\subseteq NEXP$: טרוויאלי. לכל שפה ב-$EXP$ קיים אלג' דטר' המכריע אותה בזמן אקספ', ולכן קיים לה גם אלג' לא דטר' המכריע אותה בזמן אקספ' – אותו אלג' בדיוק ללא ריצות לא דטר' (או לחילופין: התעלמות מהעד והרצת האלג' הדטר' המקורי).

$NEXP\subseteq EXP$: תהי $L\in NEXP$, אזי קיים אלג' לא דטר' המכריע את $L$ בזמן $2^{n^c}$ לכל קלט מאורך $n$ ועבור $c$ קבוע כלשהו. נניח תחילה כי $L$ שפה בינארית, כלומר קלטים לאלג' המכריע את $L$ הם בייצוג בינארי ($x\in\{0,1\}^*$). לכן לכל $x$ מתקיים כי אורך הקלט $n=\log x$, ולכן האלג' מכריע את $L$ בזמן לא דטר' $2^{\log(x)^c}=x^c$. נסתכל על השפה הבאה: $L_{pad}=\{1^x\mid x\in L\}$ – שפת הייצוגים האונאריים של כל $x\in L$. נבנה את האלג' הבא להכריע שפה זו: בהינתן קלט $1^k$, ממיר אותו לייצוג בינארי ו מריץ על התוצאה את האלג' המכריע של $L$. סה"כ לכל קלט באורך $m$ זמן הריצה יהיה לא דטר' $O(m^c)$, כלומר $L_{pad}\in NP$. כיוון ש-$L_{pad}$ היא שפה אונארית, מהנחה מתקיים כי $L_{pad}\in P$, כלומר קיים אלג' דטר' המכריע את $L_{pad}$ בזמן פולי' $O(m^c)$ כאשר $m$ אורך הקלט (האונארי) ו-$c$ קבוע כלשהו. במעבר חזרה לייצוג בינארי נקבל כי ניתן להכריע את $L$ בזמן דטר' $O(2^{|x|^c})$, ומכאן $L\in EXP$. נסתכל על המקרה בו $L\in NEXP$ שפה אונארית, לכן ל-$L$ אלג' לא דטר' המכריע אותה בזמן $2^{|x|^c}$ לכל קלט אונארי $x$ עבור $c$ קבוע כלשהו. נבנה את השפה הבאה: $L_{pad}=\{1^n\cdot 1^{2^n}\mid 1^n\in L\}$. נבנה אלג' המכריע שפה זו: בהינתן קלט, תחילה בודק שהוא מהצורה $1^n\cdot 1^{2^n}$, ואם כן מריץ את האלג' המכריע את $L$ על $1^n$, ומחזיר את תשובתו. ברור כי $1^n\cdot 1^{2^n}\in L_{pad}\Leftrightarrow 1^n\in L$. זמן הריצה של אלג' זה הוא $2^{|x|^c}$ לא דטר' ($x=1^n$), וכיוון שזהו אורך הקלט אזי $L_{pad}\in NP$. מהגדרתה, ברור כי $L_{pad}$ שפה אונארית, ולכן לפי הנחה $L_{pad}\in P$. מכאן, שקיים אלג' דטר' המכריע את $L_{pad}$ בזמן פולי' באורך הקלט, ולכן קיים אלג' המכריע את $L$ בזמן אקספוננציאלי באורך הקלט. מכאן ש-$L\in EXP$. בכל מקרה קבלנו כי $NEXP\subseteq EXP$. מכאן שמתקיים: $EXP=NEXP$, כנדרש. מכאן, אם $EXP\neq NEXP$, אז קיימת שפה (אונארית) ב-$NP$ שאינה ב-$P$, ולכן $NP\neq P$. לפי משפט לנדר, קיימת שפה ב-$NP\backslash P$ שאינה $NPC$, כנדרש.

**(4)**

**(a) טענה: $S_2^P$ סגורה תחת משלים**

תהי $L \in S_2^P$, אזי קיימת מ"ט $M$ הרצה בזמן פולי' ופולינום $p$ כך שלכל $x \in \{0,1\}^*$:

$$x \in L \Rightarrow \exists y \in \{0,1\}^{p(|x|)}. \forall z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 1$$

$$x \notin L \Rightarrow \exists z \in \{0,1\}^{p(|x|)}. \forall y \in \{0,1\}^{p(|x|)}. M(x,y,z) = 0$$

נגדיר את המכונה $M'$ באופן הבא: $M'(x,y,z) \coloneqq \overline{M(x,z,y)}$. ברור כי מכונה זו רצה בזמן פולי', שכן $M$ פולי' וסה"כ מחליפים סדר ארגומנטים ואת התוצאה הסופית.

נניח $x \in \bar{L}$, אזי $x \notin L$. לפיכך: $\exists z \in \{0,1\}^{p(|x|)}. \forall y \in \{0,1\}^{p(|x|)}. M(x,y,z) = 0$. נסמן $y' = z, z' = y$ ונקבל כי $\exists y'. \forall z'. M(x,z',y') = 0$, וזה הרי שקול ל-$\exists y'. \forall z'. M'(x,y',z') = 1$.

נניח $x \notin \bar{L}$, אזי $x \in L$. לפיכך: $\exists y \in \{0,1\}^{p(|x|)}. \forall z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 1$. נסמן $y' = z, z' = y$ ונקבל כי $\exists z'. \forall y'. M(x,z',y') = 1$, וזה הרי שקול ל-$\exists z'. \forall y'. M'(x,y',z') = 0$.

מכאן שקיימת מ"ט $M'$ הרצה בזמן פולי' ופולינום $p$ כך שלכל $x \in \{0,1\}^*$:

$$x \in \bar{L} \Rightarrow \exists y' \in \{0,1\}^{p(|x|)}. \forall z' \in \{0,1\}^{p(|x|)}. M'(x,y',z') = 1$$

$$x \notin \bar{L} \Rightarrow \exists z' \in \{0,1\}^{p(|x|)}. \forall y' \in \{0,1\}^{p(|x|)}. M'(x,y',z') = 0$$

ולכן $\bar{L} \in S_2^P$, כנדרש.

**(b)** $S_2^P \subseteq \Sigma_2^P \cap \Pi_2^P$:

$S_2^P \subseteq \Sigma_2^P$: תהי $L \in S_2^P$, אזי קיימת מ"ט $M$ הרצה בזמן פולי' ופולינום $p$ כך שלכל $x \in \{0,1\}^*$:

$$x \in L \Rightarrow \exists y \in \{0,1\}^{p(|x|)}. \forall z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 1$$

כמו כן מתקיים: $x \notin L \Rightarrow \exists z \in \{0,1\}^{p(|x|)}. \forall y \in \{0,1\}^{p(|x|)}. M(x,y,z) = 0$, והרי אם קיים $z$ כלשהו, נסמנו למשל $z_1$, המקיים <u>לכל</u> $y$: $M(x,y,z) = 0$, הרי ברור כי לכל $y$ קיים $z$ המקיים $M(x,y,z) = 0$ - פשוט נבחר את אותו $z_1$ (אולי היחיד) המקיים $M(x,y,z) = 0$. מכאן:

$\forall y \in \{0,1\}^{p(|x|)}. \exists z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 0 \neq 1$, וזו השלילה של האגף הימני בגרי רה הראשונה. מכאן, מתקיים יחס אמ"מ:

$x \in L \Leftrightarrow \exists y \in \{0,1\}^{p(|x|)}. \forall z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 1$, ומקיום תנאי זה נובע כי $L \in \Sigma_2^P$, כנדרש.

$S_2^P \subseteq \Pi_2^P$: משיקולים דומים ניתן להראות כי $L$ מקיימת גם את התנאי: $x \notin L \Leftrightarrow \forall y \in \{0,1\}^{p(|x|)}. \exists z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 0$ (במקרה זה נבחר כי 0 יהיה הפלט של $M$ כאשר $x \notin L$, ולא 1).

$$x \notin L \Rightarrow \exists z \in \{0,1\}^{p(|x|)}. \forall y \in \{0,1\}^{p(|x|)}. M(x,y,z) = 0 \underset{\text{כפי שהוכח לעיל}}{\Rightarrow} \forall y. \exists z. M(x,y,z) = 0$$

$$x \in L \Rightarrow \exists y \in \{0,1\}^{p(|x|)}. \forall z \in \{0,1\}^{p(|x|)}. M(x,y,z) = 1 \neq 0$$

כאשר האגף הימני האחרון הוא שלילה של האגף הימני הראשון, ונובע מתכונות $L$ כשפה ב-$S_2^P$. לפיכך קיבלנו את יחס האמ"מ ומתקיים כי $L \in \Pi_2^P$.

לסיכום, קיבלנו כי $L \in S_2^P \Rightarrow L \in \Sigma_2^P \wedge L \in \Pi_2^P \Rightarrow L \in \Sigma_2^P \cap \Pi_2^P$, כנדרש.