מודלים חישוביים
תרגול מס' 11

11 בינואר 2017

נושאי התרגול:

- המחלקות P ו־ NP

1 המחלקות P ו־ NP

הגדרה 1.1 המחלקה $\mathcal{P}$ היא מחלקת כל השפות הניתנות להכרעה בזמן פולינומי עם מ"ט דטרמיניסטית. כלומר: $\mathcal{P} = \bigcup_{c>0} \mathrm{DTIME}\left(n^c\right)$ כך ש־ $\mathrm{DTIME}\left(f\left(n\right)\right)$ היא מחלקת כל השפות הכריעות ע"י מ"ט דטרמיניסטית חד־סרטית העושה לכל היותר $O\left(f\left(n\right)\right)$ צעדים עד שמקבלת או דוחה כל קלט.

שימו לב ש־ $\mathcal{P}$ אינה תלויה במודל. יחד עם זאת, למשל, $\mathrm{DTIME}\left(n\right)$ כן (ראינו למשל כיצד ניתן לסמלץ מ"ט דו־סרטית הרצה ב־ $O\left(n\right)$ צעדים ע"י מ"ט חד־סרטית הרצה ב־ $O\left(n^2\right)$ צעדים). כעת, נזכר כי עבור מ"ט אי־דטרמינסטית M שתמיד עוצרת, $x \in L\left(M\right)$ אם קיים מסלול חישוב (או, "סדרת ניחושים") שמגיע למצב מקבל, ו־ $x \notin L\left(M\right)$ אם כל מסלול חישוב דוחה. ואז:

הגדרה 1.2 המחלקה $\mathcal{NP}$ היא מחלקת כל השפות הניתנות להכרעה בזמן פולינומי עם מ"ט אי־דטרמיניסטית. כלומר: $\mathcal{NP} = \bigcup_{c>0} \mathrm{NTIME}\left(n^c\right)$ כך ש־ $\mathrm{NTIME}\left(f\left(n\right)\right)$ היא מחלקת כל השפות הכריעות ע"י מ"ט אי־דטרמיניסטית חד־סרטית העושה לכל היותר $O\left(f\left(n\right)\right)$ צעדים עד שמקבלת או דוחה כל קלט (בכל מסלול חישוב אפשרי).

כדי להציג אפיון אלטרנטיבי למחלקה $\mathcal{NP}$, נגדיר תחילה מוודא (verifier) עבור שפה.

הגדרה 1.3 מ"ט דטרמיניסטית M המקבל כקלט זוג (x, c) מוודאת שפה L אם מתקיים ש:

- אם $x \in L$ אז <u>קיים</u> c כך ש־ $M\left(x, c\right) - 1$ מקבלת.
- אם $x \notin L$ אז <u>לכל</u> c, $M\left(x, c\right)$ לא מקבלת.

משפט 1.4 שפה $L \in \mathcal{NP}$ אם"ם ל־ L קיים מוודא פולינומי (כלומר, M רצה בזמן שהוא פולינומי ב־ $|x|$).

תרגיל 1

הוכיחו כי קיים מוודא ל־ H_{TM}.

פתרון

המוודא הוא מ"ט המקבלת קלט לשפה שצריך לוודא ו"עד" כלשהו. מהו עד אפשרי לעצירה על מילה ע"י מ"ט? למשל, מספר הצעדים שלוקח למכונה לעצור על המילה. נגדיר V שעל קלט $(\langle M, w\rangle, c)$ מפרשת את c כמספר טבעי ומריצה את M על w למשך c צעדים. אם M עצרה, V תקבל. אחרת, V תדחה. ואז:

- אם $\langle M, w\rangle \in H_{TM}$ אז קיים c' כך ש־ M עוצרת על w אחרי c' צעדים ואז $V\left(\langle M, w\rangle, c'\right) = 1$ (כלומר, V מקבלת את $(\langle M, w\rangle, c')$).
- אם $\langle M, w\rangle \notin H_{TM}$ אז לכל c, M לא תעצור על w לאחר c צעדים ו־ $V\left(\langle M, w\rangle, c\right) = 0$ (כלומר, V לא תקבל את $(\langle M, w\rangle, c)$ לכל c).

תרגיל 2

הוכיחו כי שפה $L \in \mathrm{RE}$ אם"ם יש ל־ L מוודא.

פתרון

כיוון ראשון באופן דומה לתרגיל 1. תהא $L \in \mathrm{RE}$. אזי, קיימת מ"ט M_L המקבלת את L. נבנה מ"ט דטרמיניסטית V כך שעל קלט (x, c) תסמלץ את M_L על x למשך $|c|$ צעדים ותקבל אם"ם M_L קיבלה. ואז,

- אם $x \in L$ אז קיים c' כך ש־ M_L מקבלת את x אחרי $|c'|$ צעדים ואז $V(x, c') = 1$.
- אם $x \notin L$ אז לכל c, M_L לא תקבל את x ולכל c, $V(x, c) = 0$.

כיוון שני יהא V מוודא לשפה L מעל Σ. נבנה מ"ט M_L המקבלת את L. M_L על קלט x:

1. יהא $c_1, c_2, \ldots$ הסדר הלקסיקוגרפי של כל המילים ב־ $\Sigma^\star$.
2. לכל i החל מ־ 1:
   (א) לכל j מ־ 1 עד i:
      i. סמלץ את $V(x, c_j)$ למשך i צעדים.
      ii. אם V מקבלת, M_L תקבל.

ואז,

- אם $x \in L$ אז מחוקיות המוודא קיים c' כך ש־ $V(x, c')$ מקבלת ולכן גם M_L תקבל את x (כי קיים j כך ש־ $c' = c_j$ ו־ i כך ש־ V עוצרת על (x, c_j) לאחר i צעדים).
- אם $x \notin L$ אז לכל c, $V(x, c)$ לא מקבלת (לא משנה לאחר כמה צעדים). לכן, M_L לעולם לא תקבל.

תרגיל 3

1. האם $\mathcal{P}$ סגורה למשלים?
2. האם $\mathcal{NP}$ סגורה למשלים?

פתרון

1. כן. תהא M מ"ט המכריעה את L בזמן פולינומי. נחליף בין q_a ל־ q_r ונקבל מ"ט פולינומית המכריעה את $\bar{L}$. הנכונות טריוויאלית.
2. זו שאלה פתוחה. מדוע ה"טריק" של הסעיף הקודם לא יעבוד? אם N מ"ט א"ד המקבלת את L, אזי אם $x \in L$ קיים מסלול מקבל ואם $x \notin L$ כל מסלול דוחה. אם נהפוך את המצב המקבל והדוחה, נקבל מ"ט N' כך שאם $x \in L$ קיים מסלול דוחה ואם $x \notin L$ כל מסלול מקבל. דהיינו, אם $x \in \bar{L}$ כל מסלול מקבל ואם $x \notin \bar{L}$ קיים מסלול דוחה. זו אינה מ"ט המקבלת את $\bar{L}$! אנו מגדירים:

$$\mathrm{co}\mathcal{NP} = \left\{ \bar{L} \subseteq \Sigma^\star \mid L \in \mathcal{NP} \right\}$$

והשאלה $\mathcal{NP} \stackrel{?}{=} \mathrm{co}\mathcal{NP}$ היא שאלה פתוחה.

תרגיל 4

נגדיר: $\mathrm{EXP} = \bigcup_{c>0} \mathrm{DTIME}\left(2^{n^c}\right)$. הוכיחו: $\mathcal{P} \subseteq \mathcal{NP} \subseteq \mathrm{EXP}$.

פתרון

הכיוון $\mathcal{P} \subseteq \mathcal{NP}$ תהא $L \in \mathcal{P}$. אזי, קיימת מ"ט דטרמיניסטית M המכריעה את L בזמן פולינומי. נתייחס ל־ M כמוודא ל־ L אשר פשוט מתעלמת מהעד, ואז לפי המשפט $L \in \mathcal{NP}$. במילים אחרות: פשוט "לא נשתמש" באי־דטרמיניזם.

הכיוון $\mathcal{NP} \subseteq \mathbf{EXP}$ תהא $L \in \mathcal{NP}$. אזי, קיים פולינום p כך שעל קלט x, קיים מוודא V עבור L הרץ לכל היותר $p(|x|)$ צעדים. נבנה מ"ט M כך שעל קלט x:

1. עבור כל c באורך לכל היותר $p(|x|)$:
   (א) הרץ את $V(x,c)$ למשך $p(|x|)$ צעדים.
   (ב) אם V קיבלה, M תקבל ותצא.
2. M תדחה.

שימו לב שלקחנו את אותו חסם על זמן הריצה ועל אורך המוודא. ודאו כי אתם מבינים מדוע ניתן להניח זאת. ואז,

- זמן הריצה של M הוא אקספוננציאלי: עבור קלט x באורך n יש $O\left(2^{p(n)}\right)$ עדים אפשריים, ולכל עד זמן הריצה הוא לכל היותר $p(n)$. לכן, סה"כ, $O\left(p(n) \cdot 2^{p(n)}\right)$.
- אם $x \in L$ אזי קיים עד c' באורך לכל היותר $p(|x|)$ כך ש־ $V(x,c')$ רץ בלכל היותר $p(|x|)$ צעדים ומקבל. אזי, M תגיע אליו ותקבל.
- אם $x \notin L$ אזי לכל c באורך לכל היותר $p(|x|)$, $V(x,c)$ לא תקבל ב־ $p(|x|)$ צעדים ולכן M תדחה.