

מודלים חישוביים

תרגול מס' 11

3 ביוני 2015

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: $\mathcal{P} = \bigcup_{c>0} \text{DTIME}(n^c)$ כך ש- $\text{DTIME}(f(n))$ היא מחלקת כל השפות הכריעות ע"י מ"ט דטרמיניסטית חד-סרטית העושה לכל היותר $O(f(n))$ צעדים עד שמקבלת או דוחה כל קלט.

שימו לב ש- \mathcal{P} אינה תלויה במודל. יחד עם זאת, למשל, $\text{DTIME}(n)$ כן (ראינו למשל כיצד ניתן לסמלך מ"ט דו-סרטית הרצה ב- $O(n)$ צעדים ע"י מ"ט חד-סרטית הרצה ב- $O(n^2)$ צעדים). כעת, נזכר כי עבור מ"ט אי-דטרמיניסטית M שתמיד עוצרת, $x \in L(M)$ אם קיים מסלול חישוב (או, "סדרת ניחושים") שמגיע למצב מקבל, ו- $x \notin L(M)$ 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: $\mathcal{NP} = \bigcup_{c>0} \text{NTIME}(n^c)$ כך ש- $\text{NTIME}(f(n))$ היא מחלקת כל השפות הכריעות ע"י מ"ט אי-דטרמיניסטית חד-סרטית העושה לכל היותר $O(f(n))$ 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 קיים c כך ש- $M(x, c)$ מקבלת.

• אם $x \notin L$ אז לכל c , $M(x, c)$ דוחה.

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 $V(\langle M, w \rangle, c') = 1$ (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- $V(\langle M, w \rangle, c) = 0$ (כלומר, V תדחה את $(\langle M, w \rangle, c)$ לכל c).

תרגיל 2

הוכיחו כי שפה $L \in RE$ אם"ם יש ל- L מוודא.

פתרון

כיוון ראשון באופן דומה לתרגיל 1. תהא $L \in RE$. 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, \dots הסדר הלכסיקוגרפי של כל המילים ב- Σ^* .

2. לכל i החל מ-1:

(א) לכל j מ-1 עד i :

- סמלץ את $V(x, c_j)$ למשך i צעדים.
- 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

הוכיחו את המשפט מתחילת התרגול: שפה $L \in \mathcal{NP}$ אם"ם ל- L קיים מוודא פולינומי.

פתרון

כיוון ראשון תהא $L \in \mathcal{NP}$. אזי, קיימת מ"ט א"ד N המכריעה את L בזמן פולינומי. נבנה מוודא פולינומי V , שעל קלט (x, c) : סמלץ את N על x , אך בכל פעם ש- N מבצעת ניחוש אי-דטרמיניסטי, V קוראת את הביט הבא ב- c ופועלת על פיו.

ברור כי זמן הריצה של V הוא פולינומי, שכן לכל c אנו מסמלצים ענף חישוב של N וכל ענף כזה מגיע למצב מקבל או דוחה תוך מספר פולינומי של צעדים. ואז,

- אם $x \in L$ אז קיים מסלול חישוב מקבל של N . נקח את c' בתור הקידוד של מסלול החישוב הזה, ואז $V(x, c') = 1$.
- אם $x \notin L$ אז בכל מסלול חישוב, N דוחה. לכן, לכל c , $V(x, c) = 0$.

שימו לב שמהבנייה הנ"ל אנו יכולים להסיק כי ניתן (וכך עושים) להניח כי אורך העד המוודא למכונת \mathcal{NP} הוא פולינומי, שכן אחרת לא יהיה לנו די זמן לקרוא את כולו.

כיוון שני יהא V מוודא פולינומי ל- L . אזי, קיים פולינום p כך ש- $|c| \leq p(|x|)$. נבנה מ"ט א"ד N . על קלט x : מנחשת c באורך לכל היותר $p(|x|)$, מריצה את $V(x, c)$ ועונה כמורה. ברור כי N רצה בזמן פולינומי, שכן V רץ בזמן פולינומי. כמו כן, אם $x \in L$ אז קיים c כך ש- $V(x, c) = 1$ ולכן ל- N קיים מסלול חישוב מקבל, ואם $x \notin L$ אז לכל c , $V(x, c) = 0$ ולכן ב- N כל המסלולים דוחים.

תרגיל 4

1. האם \mathcal{P} סגורה למשלמים?

2. האם \mathcal{NP} סגורה למשלמים?

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:

$$\text{coNP} = \{\bar{L} \subseteq \Sigma^* \mid L \in \text{NP}\}$$

והשאלה $\text{NP} = ? \text{coNP}$ היא שאלה פתוחה.

תרגיל 5

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

פתרון

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

הכיוון $\text{NP} \subseteq \text{EXP}$ תהא $L \in \text{NP}$, אזי קיים פולינום p כך שעל קלט x , קיים מודא 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 המודא. ודאו כי אתם מבינים מדוע ניתן להניח זאת, ואז,

- זמן הריצה של M הוא אקספוננציאלי: עבור קלט x באורך n יש $O(2^{p(n)})$ עדים אפשריים, ולכל עד זמן הריצה הוא לכל היותר $p(n)$. לכן, סה"כ, $O(p(n) \cdot 2^{p(n)})$.
- אם $x \in L$ אזי קיים עד c' באורך לכל היותר $p(|x|)$ כך ש- $V(x, c')$ רץ בכלל 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.

תרגיל 6

נוסחה בלוגיקה בוליאנית φ מעל המשתנים x_1, \dots, x_n היא בצורת CNF (Conjunctive normal form) אם היא מהצורה:

$$\varphi = (\ell_{1,1} \vee \dots \vee \ell_{1,i_1}) \wedge \dots \wedge (\ell_{m,1} \vee \dots \vee \ell_{m,i_m})$$

כך שכל ליטרל ℓ הוא x_k או $\neg x_k$ עבור $1 \leq k \leq n$ כלשהו. כלומר, φ הוא קוניונקציה ("וגם") של m פסוקיות (clauses) כך שכל פסוקית היא דיסיונקציה ("או") של משתנים ושיליתם. השמה בוליאנית היא פונקציה מקבוצת המשתנים ל- $\{0, 1\}$ והשמה v מספקת את φ אם "ה- evaluation של φ על v נתן 1. לדוגמא, עבור

$$\varphi = (x \vee y) \wedge (y \vee \neg z)$$

ההשמה $v(x) = 1, v(y) = 0, v(z) = 0$ היא מספקת ואילו ההשמה $v(x) = 0, v(y) = 0, v(z) = 1$ אינה מספקת. נגדיר את השפה:

$$\text{SAT} = \{\varphi \mid \varphi \text{ is a satisfiable CNF}\}$$

הוכיחו כי $\text{SAT} \in \text{NP}$.

פתרון

נשתמש בהגדרה של מוודא. השלימו לבד את ההוכחה תוך שימוש בהגדרה של מכונות אי-דטרמיניסטיות. יהא V מוודא כך שעל קלט $(\langle \varphi \rangle, v)$:

1. בדוק שאכן $\langle \varphi \rangle$ הוא קידוד של CNF חוקי. אם לא, דחה. יהא n מספר המשתנים ב- φ .
2. בדוק ש- v היא מחרוזת באורך n .
3. החלף כל משתנה ב- φ עם התו המתאים לו ב- v .
4. חשב את $\varphi(v)$.
5. אם $\varphi(v) = 1$ קבל. אחרת, דחה.

ואז,

- נסמן ב- m את מספר הפסוקיות ב- φ . קל לראות שניתן לבדוק שהקידוד חוקי ולחשב את $\varphi(v)$ בזמן $O(m \cdot n)$, שהוא פולינומי ב- $|\langle \varphi \rangle|$.
- אם $\varphi \in \text{SAT}$ אז קיימת השמה v' כך ש- $\varphi(v') = 1$, ואז $V(\langle \varphi \rangle, v') = 1$.
- אם $\varphi \notin \text{SAT}$ אז לכל השמה v , $\varphi(v) = 0$ ואז לכל v , $V(\langle \varphi \rangle, v) = 0$.