# מודלים חישוביים
# תרגול מס' 11

14 ביוני 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).

### תרגיל 1

האם $\mathcal{NP}$ סגורה למשלים?

### פתרון

זו שאלה פתוחה. מדוע ה"טריק" של להפוך בין $q_a$ ל־ $q_r$ 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 $\mathcal{NP} =^? \mathrm{co}\mathcal{NP}$ היא שאלה פתוחה.
כדי להציג אפיון אלטרנטיבי למחלקה $\mathcal{NP}$, נגדיר תחילה מוודא (verifier) עבור שפה.

**הגדרה 1.3** מוודא לשפה $L$ הוא מ"ט דטרמיניסטית $M$ המקבל כקלט זוג $(x, c)$ כך ש:

- אם $x \in L$ אז <u>קיים</u> $c$ כך ש־ $M\left(x, c\right)$ מקבלת.
- אם $x \notin L$ אז <u>לכל</u> $c$, $M\left(x, c\right)$ 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 2

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

### פתרון

**כיוון ראשון** 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 $\Sigma$. 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

הוכיחו: 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 $N$. $N$ על קלט $x$: מנחשת $c$ באורך לכל היותר $p(|x|)$, מריצה את $V(x,c)$ ועונה כמוהו.

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

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

**פתרון**

תהא $L \in \mathcal{NP}$. אזי, קיים מוודא $V$ ופולינום $p$ כך ש־ $V$ על קלט $x$ רץ 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.

## תרגיל 5

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

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

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

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

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

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

הוכיחו כי $\mathrm{SAT} \in \mathcal{NP}$.

**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־ $\varphi$.
2. בדוק ש־ $v$ היא מחרוזת באורך $n$.
3. החלף כל משתנה ב־ $\varphi$ 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־ $\varphi$. קל לראות שניתן לבדוק שהקידוד חוקי ולחשב את $\varphi(v)$ בזמן $O(m \cdot n)$, שהוא פולינומי ב־ $|\langle\varphi\rangle|$.
- אם $\varphi \in \mathrm{SAT}$ אז קיימת השמה $v'$ כך ש־ $\varphi(v') = 1$, ואז $V(\langle\varphi\rangle, v') = 1$.
- אם $\varphi \notin \mathrm{SAT}$ אז לכל השמה $v$, $\varphi(v) = 0$ ואז לכל $v$, $V(\langle\varphi\rangle, v) = 0$.