מודלים חישוביים
תרגול מס' 12

13 ביוני 2015

נושאי התרגול:

- המחלקות P, NP ו־ coNP – המשך.
- רדוקציות פולינומיות והמחלקה NPC.

1 המחלקות P, NP ו־ coNP

הגדרה 1.1 נזכיר: $\mathcal{P} = \bigcup_{c>0} \mathrm{DTIME}\left(n^c\right)$ כך ש־ $\mathrm{DTIME}\left(f\left(n\right)\right)$ היא מחלקת כל השפות הכריעות ע"י מ"ט דטרמיניסטית העושה לכל היותר $O\left(f\left(n\right)\right)$ צעדים עד שמקבלת או דוחה כל קלט. כמו כן, $\mathcal{NP} = \bigcup_{c>0} \mathrm{NTIME}\left(n^c\right)$ כך ש־ $\mathrm{NTIME}\left(f\left(n\right)\right)$ היא מחלקת כל השפות הכריעות ע"י מ"ט אי־דטרמיניסטית העושה לכל היותר $O\left(f\left(n\right)\right)$ צעדים עד שמקבלת או דוחה כל קלט (בכל מסלול חישוב אפשרי).

ראינו גם:

משפט 1.2 שפה $L \in \mathcal{NP}$ אם"ם ל־ L קיים מוודא פולינומי (כלומר, M רצה בזמן שהוא פולינומי ב־ $|x|$).

כעת, נגדיר:

הגדרה 1.3 המחלקה $\mathrm{co}\mathcal{NP}$: $\mathrm{co}\mathcal{NP} = \left\{L \subseteq \Sigma^\star \mid \bar{L} \in \mathcal{NP}\right\}$.

תרגיל 1

קליק בגרף לא־מכוון $G = (V, E)$ הוא תת־גרף שבו כל שני צמתים מחוברים בקשת. פורמלית: $A \subseteq V$ הוא קליק ב־ G אם לכל $v_1 \neq v_2$ ב־ V מתקיים ש־ $\{v_1, v_2\} \in E$. נגדיר את השפה:

$$\mathrm{CLIQUE} = \{(\langle G\rangle, k) \mid G \text{ is an undirected graph with a clique of size } k\}$$

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

פתרון

נשתמש בהגדרה של מכונות אי־דטרמיניסטיות. השלימו לבד את ההוכחה תוך שימוש בהגדרה של מוודא פולינומי. תהא M מ"ט אשר על קלט $\langle G\rangle$:

1. בודקת שאכן $\langle G\rangle$ הוא קידוד חוקי של גרף לא מכוון. אם לא, דחה. יהא n מספר הצמתים ב־ G.
2. נחש $A \subseteq V$ (דהיינו, לכל $v \in V$ נחש האם $v \in A$ או $v \notin A$). אם $|A| \neq k$, דחה.
3. לכל $i \neq j$ ב־ A:
   (א) בדוק האם $\{i, j\} \in E$.
   (ב) אם לא, M דוחה.
4. M מקבלת.

ואז,

- קל לראות שניתן לבדוק האם קבוצת צמתים משרה קליק בזמן $O\left(n^2\right)$, שהוא פולינומי ב־ $|\langle G\rangle|$.
- אם $(\langle G\rangle, k) \in \text{CLIQUE}$ אז קיים מסלול חישוב ב־ M שמנחש את קבוצת הצמתים המתאימה, ו־ M מקבלת.
- אם $(\langle G\rangle, k) \notin \text{CLIQUE}$ אז בכל מסלול חישוב, M דוחה.

תרגיל 2

הוכיחו כי $\overline{\text{3SAT}} = \{\langle\varphi\rangle \mid \varphi \text{ is not a satisfiable 3CNF formula}\} \in \text{co}\mathcal{NP}$.

פתרון

נוכיח כי $\text{3SAT} \in \mathcal{NP}$ ע"י מ"ט א"ד M הרצה בזמן פולינומי. M על קלט $\langle\varphi\rangle$:

1. בודקת ש־ $\langle\varphi\rangle$ היא קידוד של נוסחת 3CNF חוקית. אם לא, דוחה. יהא n מספר המשתנים ב־ φ.
2. מנחשת $v = v_1, \ldots, v_n \in \{0,1\}^n$.
3. מחשבת את $\varphi(v)$. אם $\varphi(v) = 1$ מקבלת ואחרת דוחה.

מתקיים ש:

- נסמן ב־ m את מספר הפסוקיות ב־ φ. קל לראות שניתן לבדוק שהקידוד חוקי, לנחש השמה 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־ $\varphi(v') = 1$. מכאן, קיים מסלול חישוב של M שינחש את v' ויקבל.
- אם $\varphi \notin \text{SAT}$ אז לכל השמה v, $\varphi(v) = 0$ אז לכל מסלול חישוב של M, לא ננחש השמה מספקת ולכן כל מסלול חישוב ידחה.

בעיות מפורסמות ב־ NP

פרט ל־ SAT, 3SAT ו־ CLIQUE, גם הבעיות האלו הן ב־ NP:

$$\begin{aligned}
\text{SubsetSum} &= \left\{\langle x_1, \ldots, x_k, t\rangle \mid \exists I \subseteq \{1,\ldots,k\} \,.\, \sum_{i\in I} x_i = t\right\} \\
\text{IS} &= \{\langle G, k\rangle \mid G \text{ is an undirected graph with an indepdent set of size } k\} \\
\text{KnapSack} &= \left\{\langle x_1, \ldots, x_k, y_1, \ldots, y_k, B, t\rangle \mid \exists I \subseteq \{1,\ldots,k\} \,.\, \left(\sum_{i\in I} x_i \le B\right) \wedge \left(\sum_{i\in I} y_i \ge t\right)\right\}
\end{aligned}$$

ונזכיר שקבוצה ב"ת (independent set) בגרף לא מכוון $G = (V, E)$ היא תת־קבוצה $A \subseteq V$ כך שלכל $u, v \in A$ מתקיים ש־ $\{u, v\} \notin E$.

2 רדוקציות פולינומיות והמחלקה NPC

הגדרה 2.1 שפה A ניתנת לרדוקציה פולינומית לשפה B (נסמן $A \le_p B$) אם קיימת $f : \Sigma^\star \to \Sigma^\star$ אשר חשיבה בזמן פולינמי ולכל x, $x \in A$ אם"ם $f(x) \in B$. הפונקציה f נקראת הרדוקציה הפולינומית.

שימו לב שההבדל בין ההגדרה הזו להגדרה של רדוקצית מיפוי היא שכעת אנו דורשים ש־ f תהיה לא רק חשיבה, אלא חשיבה באופן יעיל (בזמן פולינומי). ובאופן דומה למשפט עבור רדוקציות מיפוי:

משפט 2.2 אם $A \le_p B$ ו־ $B \in \mathcal{P}$ אז $A \in \mathcal{P}$. כנ"ל עבור $\mathcal{NP}$ ו־ $\text{co}\mathcal{NP}$.

משפט 2.3 אם $A \le_p B$ ו־ $A \notin \mathcal{P}$ אז $B \notin \mathcal{P}$. כנ"ל עבור $\mathcal{NP}$ ו־ $\text{co}\mathcal{NP}$.

כעת, נגדיר:

הגדרה 2.4 שפה $L \in \mathcal{NPC}$ (L היא $\mathcal{NP}$-שלמה) אם:

1. $L \in \mathcal{NP}$.
2. L היא $\mathcal{NP}$-קשה: לכל $A \in \mathcal{NP}$ מתקיים ש- $A \leq_p L$.

אם כך, המחלקה $\mathcal{NPC}$ היא מחלקת השפות ה"שלמות" ל- $\mathcal{NP}$. דהיינו, נמצאות ב- $\mathcal{NP}$ ו"קשות" לפחות כמו כל בעיה אחרת ב- $\mathcal{NP}$. כל השפות הנ"ל שהצגנו שהן ב- $\mathcal{NP}$ הן גם ב- $\mathcal{NPC}$. ודאו כי אתם יודעים להוכיח כי:

$$\text{SAT} \leq_p \text{3SAT} \leq_p \text{CLIQUE} \leq_p \text{IS}$$

המשפט הבא מראה כיצד ניתן להוסיף עוד בעיות למחלקה הזו:

משפט 2.5 אם $B \in \mathcal{NPC}$ ו- $B \leq_p C$ עבור $C \in \mathcal{NP}$ אז $C \in \mathcal{NPC}$.

תרגיל 3

הראו כי לכל $L \in \mathcal{NP}$, $L \leq_p A_{TM}$.

פתרון

תהא $L \in \mathcal{NP}$ עם מ"ט M המכריעה אותה. נראה $f(x) = \langle M', w \rangle$ כך ש- $x \in L$ אם"ם M' מקבלת את w. נבחר $M' = M$ ו- $w = x$, ואז:

- f ניתנת לחישוב בזמן פולינומי.
- אם $x \in L$ אזי M מקבלת את x, ו- $\langle M', w \rangle \in A_{TM}$.
- אם $x \notin L$ אזי M לא מקבלת את x, ו- $\langle M', w \rangle \notin A_{TM}$.

האם A_{TM} היא אם כך $\mathcal{NP}$-שלמה? לא! כי היא אינה ב- $\mathcal{NP}$ (הרי $\mathcal{NP} \subseteq \text{R}$).

תרגיל 4

הוכיחו: אם $\mathcal{NPC} \cap \text{co}\mathcal{NP} \neq \emptyset$ אז $\mathcal{NP} = \text{co}\mathcal{NP}$.

פתרון

תהא $L \in \mathcal{NPC} \cap \text{co}\mathcal{NP}$. נוכיח $\mathcal{NP} = \text{co}\mathcal{NP}$ בהכלה דו כיוונית.

- תהא $A \in \mathcal{NP}$. אזי, מכיוון ש- $L \in \mathcal{NPC}$ מתקיים ש- $A \leq_p L$. מכאן, ש- $\bar{A} \leq \bar{L}$ (ע"י אותה רדוקציה). מכך ש- $L \in \text{co}\mathcal{NP}$ נובע ש- $\bar{L} \in \mathcal{NP}$ ולכן גם $\bar{A} \in \mathcal{NP}$ ו- $A \in \text{co}\mathcal{NP}$.
- תהא $A \in \text{co}\mathcal{NP}$. אזי, $\bar{A} \in \mathcal{NP}$ ומהסעיף הקודם, $\bar{A} \in \text{co}\mathcal{NP}$ ולכן $A \in \mathcal{NP}$.

תרגיל 5

הוכיחו: אם $\mathcal{P} = \mathcal{NP}$ אז $\mathcal{NP} = \text{co}\mathcal{NP}$.

פתרון

נראה שתי דרכים.

דרך ראשונה

נראה כי $\text{SAT} \in \mathcal{NPC} \cap \text{co}\mathcal{NP}$ ואז מהשאלה הקודמת ינבע כי $\mathcal{NP} = \text{co}\mathcal{NP}$.

- $\text{SAT} \in \mathcal{NPC}$ – ידוע (משפט קוק־לוין).
- מכך ש־ $\text{SAT} \in \mathcal{NP}$ ומההנחה, נובע כי $\text{SAT} \in \mathcal{P}$ ומסגירות $\mathcal{P}$ למשלים, $\overline{\text{SAT}} \in \mathcal{P}$. מכך ש־ $\mathcal{P} \subseteq \mathcal{NP}$ נובע כי $\overline{\text{SAT}} \in \mathcal{NP}$ ולכן $\text{SAT} \in \text{co}\mathcal{NP}$.

דרך שנייה

ישירות תוך שימוש בהנחה:

$$L \in \mathcal{NP} \Leftrightarrow L \in \mathcal{P} \Leftrightarrow \bar{L} \in \mathcal{P} \Leftrightarrow \bar{L} \in \mathcal{NP} \Leftrightarrow L \in \text{co}\mathcal{NP}$$

תרגיל 6

נוסחה בלוגיקה בוליאנית φ מעל המשתנים $x_1, \ldots, x_n$ היא בצורת DNF (Disjunctive normal form) אם היא מהצורה:

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

כך שכל ליטרל ℓ הוא x_k או $\neg x_k$ עבור $1 \leq k \leq n$ כלשהו. בניגוד למצב ב־ SAT, הבעיה של להכריע האם פסוק DNF ספיק או לא ידועה להיות ב־ $\mathcal{P}$ (למה?). נגדיר:

$$\text{TDSAT} = \{\langle\varphi\rangle \mid \varphi\text{is a DNF tautology}\}$$

הוכיחו כי $\text{TDSAT} \in \text{co}-\mathcal{NP}$.

פתרון

נשים לב כי

$$\overline{\text{TDSAT}} = \{\langle\varphi\rangle \mid \varphi\text{is not a DNF formula or } \exists v.\varphi(v) = 0\}$$

נראה כי $\overline{\text{TDSAT}} \in \mathcal{NP}$ בעזרת עד פולינומי. עבור קלט $\langle\varphi\rangle, c$:

- אם $\langle\varphi\rangle$ אינו קידוד חוקי של נוסחה, קבל.
- אחרת, בדוק האם c היא השמה חוקית ומתקיים $\varphi(c) = 0$. אם כן, קבל. אחרת, דחה.

הפולינומיות ברורה. כעת, אם $\langle\varphi\rangle \in \overline{\text{TDSAT}}$ אזי או שהיא אינה חוקית או שקיימת השמה כך שעבורה φ מקבל False. מכאן, קיים c כזה כך שהמכונה תקבל. בכיוון השני, אם φ היא טאוטולוגיה ב־ DNF אז לא קיימת השמה c כך שהמכונה תקבל. לכן, $\text{TDSAT} \in \text{co}-\mathcal{NP}$.

תרגיל 7

עבור נוסחת CNF או DNF φ והשמה v נסמן ב־ $N(\varphi, v)$ את מספר הפסוקיות ב־ φ המסופקות ע"י v. נגדיר:

$$\text{C-CNF} = \{\langle\varphi, k\rangle \mid \varphi\text{is a CNF and } \exists v.N(\varphi, v) = k\}$$

ובאופן דומה נגדיר C-DNF. הוכיחו:

1. $\text{C-CNF} \leq_p \text{3SAT}$.
2. $\text{3SAT} \leq_p \text{C-CNF}$.
3. $\text{C-CNF} \leq_p \text{C-DNF}$.

פתרון

1. מכיוון ש־ $3\text{SAT} \in \mathcal{NPC}$ אנו צריכים להראות רק כי $\text{C-CNF} \in \mathcal{NP}$. השלימו את ההוכחה לבד.
2. נגדיר $f(\langle\langle\varphi\rangle\rangle) = \langle\varphi, |\varphi|\rangle$ כך ש־ $|\varphi|$ מציין את מספר הפסוקיות ב־ φ. ברור כי הרדוקציה פולינומית, וש־ φ ספיק אם"ם קיימת השמה שמספקת את כל הפסוקיות שלו.
3. נגדיר $f(\langle\varphi, k\rangle) = \langle\bar{\varphi}, |\varphi| - k\rangle$ כך ש־ $\bar{\varphi}$ מציין את ה־ DNF המתאים ל־ $\neg\varphi$ ע"י הפעלת כללי דה־מורגן. ברור כי הרדוקציה פולינומית, ומתקיים:

$$\langle\varphi, k\rangle \in \text{C-CNF} \Leftrightarrow \exists v.N(\varphi, v) = k \Leftrightarrow \exists v.N(\bar{\varphi}, v) = |\varphi| - k \Leftrightarrow \langle\bar{\varphi}, |\varphi| - k\rangle \in \text{D-CNF}$$

תרגיל 8

הוכיחו כי:

$$\text{IS} \wedge \text{CLIQUE} = \{\langle G, k\rangle \mid G \text{ has an IS and a clique of size } k\} \in \mathcal{NPC}$$

פתרון

נראה כי $\text{IS} \wedge \text{CLIQUE} \in \mathcal{NP}$ ושהיא $\mathcal{NP}$־קשה.

- קל לראות כי $\text{IS} \wedge \text{CLIQUE} \in \mathcal{NP}$ ע"י מוודא פולינומי: על קלט $\langle G, k\rangle, A$ הוא יוודא כי A מקודד שתי תתי קבוצות בגודל k של הצמתים של G, שהראשונה מהווה קבוצה ב"ת (כלומר, אין קשת בין אף זוג צמתים) ושהשנייה מהווה קליק (כלומר, בין כל זוג צמתים יש קשת). ברור כי ניתן לעשות זאת בזמן פולינומי, ושהקלט בשפה אם"ם קיים עד כזה.
- כעת, כדי להראות שהיא קשה, נראה $\text{CLIQUE} \leq_p \text{IS} \wedge \text{CLIQUE}$ (ואז, לפי המשפט הקודם, זה מספיק). הרדוקציה תהיה $f(\langle G, k\rangle) = \langle G', k\rangle$ כך ש־ G' הוא G בתוספת k צמתים מבודדים. ואז:
  - ברור כי f פולינומית (צריך בסה"כ להוסיף עוד k צמתים לגרף הנתון).
  - אם ל־ G יש קליק בגודל k אז ל־ G' יש קליק בגודל k (לא "הרסנו" אותו) וגם קבוצה ב"ת בגודל k ולכן $\langle G', k\rangle \in \text{IS} \wedge \text{CLIQUE}$.
  - אם ל־ G אין קליק בגודל k אז גם ל־ G' אין (הצמתים המבודדים לא יכולים להשתתף בקליק) ולכן $\langle G', k\rangle \notin \text{IS} \wedge \text{CLIQUE}$.