המחלקה להנדסת תוכנה

08/07/21
~~09:00-12:00~~
13:30-16:30

חישוביות וסיבוכיות

מועד ב'

ד"ר כרים אבו עפאש

תשפ"א סמסטר ב'

הנחיות חשובות:

- המבחן ללא חומר עזר וללא מחשבון.
- משך המבחן 3 שעות.
- המבחן מכיל 4 שאלות, יש לענות על כל השאלות.
- פתרו את המבחן תחילה במחברת טיוטה. לאחר מכן העתיקו את התשובות למקום המיועד בטופס התשובות בכתב קריא ומסודר. **בדיקת המבחן לא תביא בחשבון את דפי הטיוטה או תוספות בגב העמוד.**
- בתחילת המבחן, רשמו את מספר הנבחן בראש כל דף.
- מותר להשתמש במשפטים מהכיתה ומהתרגול, אך יש לציין את הניסוח המדויק של המשפט.
- במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודע" ותזכו ב- 20% מניקוד הסעיף.

השאלון מכיל 9 עמודים (כולל עמוד זה).

בהצלחה !

==========

שאלה 1 (20 נקודות)

נתונות שתי בעיות A ו- B מעל אותו א"ב Σ, ונתונים שני אלגוריתמים:

A_1 אלגוריתם המכריע את A בזמן פולינומיאלי

V_2 אלגוריתם אימות עבור B הרץ בזמן פולינומיאלי.

א) (15 נקודות)

בנו אלגוריתם אימות V עבור הבעיה $A \cup B$.

תארו במלים את האלגוריתם והוכיחו את נכונות הבניה.

הרעיון: V מקבל כקלט זוג (w,y) ורוצה לבדוק האם y היא עדות עבור ש- $w \in A \cup B$.
לצורך זה, V מריץ את A_1 על w. אם A_1 קיבל, אז V מקבל.
אחרת, V מריץ את V_2 על הזוג (w,y) ועונה כמוה.

האלגוריתם:
על קלט (w,y), V מבצע
1. מריץ את A_1 על w
• אם A_1 מקבל ⇐ V מקבל
• אם A_1 דוחה ⇐ V מריץ את V_2 על (w,y) ועונה כמוה.

נכונות:
(א) אם $w \in A \cup B$ ⇐ $w \in A$ או $w \in B$ ⇐
• אם $w \in A$ ⇐ A_1 מקבל את w ⇐ V מקבל את w.
• אם $w \notin A$ אבל $w \in B$ ⇐ קיימת עדות y כך ש- V_2 מקבל את הזוג (w,y) ⇐ קיימת עדות y כך ש- V יקבל את הזוג (w,y).

(ב) אם $w \notin A \cup B$ ⇐ $w \notin A$ וגם $w \notin B$ ⇐ A_1 דוחה את w וגם לכל עדות y, V_2 דוחה את הזוג (w,y) ⇐ לכל עדות y, V דוחה את הזוג (w,y).

ב) (5 נקודות)
האם האלגוריתם שבניתם רץ בזמן פולינומיאלי? הסבירו.

נסמן P_1 הפולינום של A_1
ונסמן P_2 הפולינום של V_2.
אז זמן הריצה של V חסום ע"י $O(P_1(|w|)+P_2(|w|))$
ולכן פולינומיאלי במודל $|w|$.

שאלה 2 (40 נקודות)

לכל אחת מהטענות הבאות, קבעו אם הטענה נכונה, לא נכונה או שקולה לבעיה פתוחה.
הסבירו בקצרה (לכל היותר 5 שורות) את קביעתכם. **אין ניקוד על תשובה נכונה ללא נימוק!**

א) (8 נקודות) אם $L_1 \le L_{acc}$ וגם $L_2 \le L_{acc}$, אזי $(L_1 \cup L_2) \le L_{acc}$.

נכון: ממשפט הרדוקציה, נובע ש- $L_1 \in RE$ וגם $L_2 \in RE$
ומכיוון ש- RE סגורה תחת איחוד, אז $L = L_1 \cup L_2 \in RE$

ניתן לבנות רדוקציה $L \le L_{acc}$.
תהי M מ"ט המקבלת את L.
פונקציית הרדוקציה: לכל $x \in \Sigma^*$: $f(x) = \langle M \rangle, \langle x \rangle$.
ברור ש- $x \in L \iff f(x) \in L_{acc}$.

ב) (8 נקודות) תהי A בעיה NP-קשה ותה B בעיה NP-שלמה. אזי מתקיים $A \le_P B$.

לא נכון:
הטענה לא נכונה לכל בעיה NP-קשה $A \notin NP$ (יש בעיות כאלה)
כי אם נניח בשלילה שקיימת רדוקציה $A \le_p B$, אז לפי משפט
הרדוקציה, מכיוון ש- $B \in NP$ (כי B היא NP-שלמה), מתקיים
ש- $A \in NP$ וזו סתירה לבחירה של A.

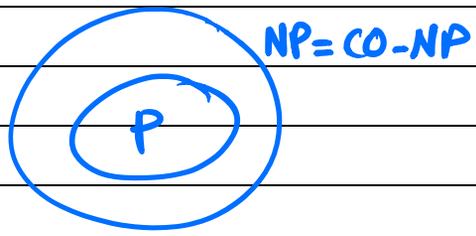
ג) (8 נקודות) אם $L \le \overline{L}$, אזי $L \in R$ או $L \notin RE$.

נכון: נניח בשלילה כי $L \le \overline{L}$ אבל $L \in RE \setminus R$.
אז קיימת רדוקציה $\overline{L} \le L$ ולפי משפט הרדוקציה, $\overline{L} \in RE$.
לכן קיבלנו ש- $L \in RE$ וגם $\overline{L} \in RE$.

לכן מהמשפט שהוכחנו בכיתה, נובע ש- $L \in R$, וזו סתירה.

ד) (8 נקודות) אם A היא בעיה NP-שלמה וגם $A \in CO\text{-}NP$, אזי $P = NP$.

לכן נכון / שקול לטענה פעמה.
אם A היא NP-שלמה וגם $A \in CO\text{-}NP$ אז זה מוכיח ש- $NP = CO\text{-}NP$
ומכן השאלה היא $P = NP$ נשארת פתוחה.



ה) (8 נקודות) קיים אלגוריתם המקבל כקלט נוסחה φ מצורת $3\text{-}CNF$ מעל המשתנים x_1, x_2, x_3, x_4, x_5 ומכריע בזמן פולינומיאלי האם φ ספיקה.

לכן: מכיוון ש- φ היא מעל המשתנים x_1, x_2, x_3, x_4, x_5, מספר ההשמות האפשריות הוא $2^5 = 32$ השמות.
אפשר לעבור על כל השמות אלו ולבדוק האם אחת מהן מספקת את φ, ולהחזיר תשובה בהתאם.
כמובן זמן הריצה לכל היותר $32 \cdot |\varphi| = O(|\varphi|)$, וזה פולינומיאלי באורך הקלט.

שאלה 3 (25 נקודות)

א) (6 נקודות)
הגדירו את המושגים *Clique* (קליקה), *VertexCover* (כיסוי בקודקודים), *IndependentSet* (קבוצה בלתי תלוייה).

קליקה: בהינתן גרף לא מכוון $G=(V,E)$, קליקה ב- G היא תת קבוצה $C\subseteq V$ כך שלכל שני קודקודים $u,v\in C$ מתקיים $(u,v)\in E$.

כיסוי בקודקודים: בהינתן גרף לא מכוון $G=(V,E)$, כיסוי בקודקודים ב- G הוא תת-קבוצה של קודקודים $C\subseteq V$ כך שלכל $(u,v)\in E$ מתקיים $u\in C$ או $v\in C$.

קבוצה בת"ת: בהינתן גרף לא מכוון $G=(V,E)$, קבוצה ב"ת ב- G היא תת-קבוצה של קודקודים $S\subseteq V$ כך שלכל שני קודקודים $u,v\in S$ מתקיים $(u,v)\notin E$.

ב) (4 נקודות)
הגדירו את הבעיות *Clique* ו- *VertexCover*.

Clique

קלט: גרף לא מכוון $G=(V,E)$ ומספר k.
פלט: האם G מכיל קליקה בגודל k?

$Clique=\{\langle G,k\rangle :$ G מכיל קליקה בגודל $k\}$

Vertex_Cover:

קלט: גרף לא מכוון $G=(V,E)$ ומספר k.
פלט: האם G מכיל כיסוי בקודקודים בגודל k?

$VC=\{\langle G,k\rangle :$ G מכיל כיסוי בקודקודים בגודל $k\}$

ג) (15 נקודות)

הוכיחו כי בעיית *Clique* היא *NP*-קשה ע"י רדוקציה פולינומיאלית מבעיית *VertexCover*.

פונקציית הרדוקציה:

בהינתן זוג $\langle G,k\rangle$ הקלט עבור VC, נגדיר זוג $\langle G',k'\rangle$ הקלט של Clique ונראה כי:

$\langle G,k\rangle \in VC \iff \langle G',k'\rangle \in Clique$.

נגדיר את $G'=(V',E')$ להיות הגרף המשלים של $G=(V,E)$, כלומר, $V'=V$ ו- $E'=\{(u,v) : (u,v)\notin E\}$.

ונגדיר $k'=|V|-k$. מזה נובע ש- $k=|V|-k'$.

נכונות הרדוקציה:

(1) ניתן לבנות את G' בזמן פולינומיאלי בגודל G.

(2) נראה כי $\langle G',k'\rangle \in Clique \iff \langle G,k\rangle \in VC$.

כיוון $\Leftarrow$:

נניח כי G מכיל כיסוי C בגודל k $\Leftarrow$ כל שני קודקודים ב- $V\setminus C$ לא מאוחרים בקלט ב- G $\Leftarrow$ כל שני קודקודים ב- $V\setminus C$ מאוחרים בקלט ב- G' $\Leftarrow$ $V\setminus C$ היא קליקה בגודל $k'=|V|-k$ ב- G' $\Leftarrow$ G' מכיל קליקה בגודל k'.

כיוון $\Rightarrow$:

נניח כי G' מכיל קליקה C בגודל k' $\Leftarrow$ כל שני קודקודים ב- C מאוחרים בקלט ב- G' $\Leftarrow$ כל שני קודקודים ב- C לא מאוחרים בקלט ב- G $\Leftarrow$ $V\setminus C$ היא כיסוי בקודקודים ב- G בגודל $k=|V|-k'$ $\Leftarrow$ G מכיל כיסוי בקודקודים בגודל k.

שאלה 4 (15 נקודות)

נתונה השפה הבאה: $L = \{ <M>,<w> \ : \ L(M) = \{w\} \}$.

כלומר L מכילה את כל הזוגות $<M>,<w>$ כך ש- M מקבלת אך ורק את w.

הוכיחו כי $L \notin R$ ע"י רדוקציה מ- L_{acc}.

הערה: יש עוד מקום עבור שאלה זו בעמוד הבא.

פונקציה הרדוקציה:

$$f(x) = \begin{cases} <M'>,<w> & : x = <M>,<w> \\ <M_\emptyset>,<\varepsilon> & : x \neq <M>,<w> \end{cases}$$

כאשר $M_\emptyset$ מ"ט הדוחה כל קלט.

M' היא מ"ט שפועלת באופן הבא:

על קלט y, מבצעת

- שומרת את y על סרט נוסף.
- מריצה את M על w
- אם M דוחה $\Leftarrow$ M' דוחה.
- אם M מקבלת $\Leftarrow$ מבדקת האם $y = w$
- אם כן $\Leftarrow$ מקבלת.
- אחרת $\Leftarrow$ דוחה.

אפשר במקום w להשתמש בכל מילה אחרת

אבחנה:

$$L(M') = \begin{cases} \{w\} & : w \in L(M) \\ \emptyset & : w \notin L(M) \end{cases}$$

נכונות הרדוקציה:

(1) f חשיבה כי ניתן לבנות מ"ט שמבצעת האם $x = <M>,<w>$. אם לא, תחזיר קידוד של $<M_\emptyset>,<\varepsilon>$ ואם כן, תחזיר קידוד של $<M'>,<w>$.

(2) נראה כי $x \in L_{acc} \iff f(x) \in L$

(כ) אם $x \in L_{acc} \Leftarrow x = <M>,<w>$ ו- $w \in L(M) \Leftarrow$

$f(x) = <M'>,<w>$ ולפי האבחנה, $L(M') = \{w\} \Leftarrow f(x) \in L$

(ב) אם $x \notin L_{acc}$ ⇐ שני מקרים

• $x \neq \langle M\rangle,\langle w\rangle$ ⇐ $f(x) = \langle M_\emptyset\rangle,\langle \varepsilon\rangle$ ולכן $L(M_\emptyset) = \emptyset \neq \{\varepsilon\}$

⇐ $f(x) \notin L$.

• $x = \langle M\rangle,\langle w\rangle$ ו. $w \notin L(M)$ ⇐ $f(x) = \langle M'\rangle,\langle w\rangle$ ולפי

האבחנה, $L(M') = \emptyset \neq \{w\}$ ⇐ $f(x) \notin L$.

לסיכום, הראינו רדוקציה $L_{acc} \leq L$, ומכיוון ש- $L_{acc} \notin R$,

ממשפט הרדוקציה, מתקיים ש- $L \notin R$!

בהצלחה!