תורת הסיבוכיות – תרגול 14
שאלות ממבחנים

שאלה 1 – Structural complexity

בכל אחד מהסעיפים הבאים נתונה רשימה של מחלקות סיבוכיות. לכל אחת מהרשימות (בנפרד) ציירו שני גרפים:

- **גרף ההכלות** – גרף מכוון אשר צמתיו הם המחלקות הנתונות, ויש בו קשת ממחלקה C_1 למחלקה C_2 אם ידוע בוודאות (ללא הנחות כלשהן) ש־ $\mathsf{C}_1 \subseteq \mathsf{C}_2$. אין צורך לצייר קשתות הנובעות מקשתות אחרות.
- **גרף אי־השוויונים** – גרף מכוון אשר צמתיו הם המחלקות הנתונות, ויש בו קשת ממחלקה C_1 למחלקה C_2 אם ידוע בוודאות שיש שפות ב־ $\mathsf{C}_1 \setminus \mathsf{C}_2$. אין צורך לצייר קשתות הנובעות מקשתות אחרות והכלות אותן סימנתם בגרף הקודם.

בשאלה זו אין צורך בהוכחות.

1. coRP , PSPACE , PH , $\mathsf{P}^{\#\mathsf{P}}$, NP , MA , BPP , AM.
2. coRL , $\mathsf{PL} \triangleq \mathsf{DSPACE}\left(\log^{O(1)} n\right)$, P , NL , $\mathrm{lu}-\mathsf{NC}^1$, DL , AC^1 , $\mathrm{lu}-\mathsf{AC}^0$.
   כאן $\mathrm{lu}-\mathsf{C}$ הוא קיצור של $\mathrm{logspace}-\mathrm{uniform}-\mathsf{C}$.

פתרון

1. להלן הגרפים.
   - גרף ההכלות:

$$\mathsf{coRP} \subseteq \mathsf{BPP} \subseteq \mathsf{MA} \subseteq \mathsf{AM} \subseteq \mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{PSPACE}$$
$$\mathsf{NP} \subseteq \mathsf{MA}$$

   הערות:
   – משפט Toda: $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$.
   - גרף אי־השוויונים: שום דבר לא ידוע.
2. להלן הגרפים.
   - גרף ההכלות:

$$\mathrm{lu}-\mathsf{AC}^0 \subseteq \mathrm{lu}-\mathsf{NC}^1 \subseteq \mathsf{DL} \subseteq \mathsf{coRL} \subseteq \mathsf{NL} \subseteq \mathsf{PL}$$
$$\mathsf{NL} \subseteq \mathsf{P}$$
$$\mathsf{NL} \subseteq \mathsf{AC}^1$$

   הערות:
   – ההכלה $\mathsf{NL} \subseteq \mathsf{PL}$ נובעת ממשפט Savitch.
   – ההכלה $\mathsf{coRL} \subseteq \mathsf{NL}$ נובעת ממשפט Immerman.
   – ההכלה $\mathsf{DL} \subseteq \mathrm{lu}-\mathsf{NC}^1$ נובעת מכך ש־ $\mathrm{FVAL} \in \mathsf{DL}$. (מה לגבי DL ו־ $\mathrm{lu}-\mathsf{AC}^1$?)

• גרף אי־השוויונים:

$$\mathsf{PL} \to \mathsf{NL}$$
$$\mathrm{lu}-\mathsf{NC}^1 \to \mathrm{lu}-\mathsf{AC}^0$$
$$\mathsf{AC}^1 \to \mathsf{P}\,,\,\mathsf{PL}$$

<u>הערות:</u>

– $\mathsf{NL} \subsetneq \mathsf{PL}$ נובע ממשפט ההיררכיה לזיכרון דטרמיניסטי.
– $\mathrm{PARITY} \in \mathrm{lu}-\mathsf{NC}^1 \setminus \mathrm{lu}-\mathsf{AC}^0$.
– יש ב־ AC^1 שפות שאינן כריעות.

שאלה 2 – מכונה לבדיקת אוב

מכונת טיורינג לבדיקת אוב עבור שפה L היא מכונת אוב פולינומית הסתברותית M כך שלכל אוב B ולכל קלט x מתקיים:

- אם $L = B$ אז M^B מקבלת את x בהסתברות 1.
- אם $B(x) \neq L(x)$ אז M^B דוחה את x בהסתברות לפחות $\frac{2}{3}$.

1. הוכיחו שלכל שפה $L \in \mathsf{P}$ קיימת מ"ט לבדיקת אוב.
2. הוכיחו שלכל שפה $L \in \mathsf{ZPP}$ קיימת מ"ט לבדיקת אוב.
3. הוכיחו שלשפה TQBF קיימת מ"ט לבדיקת אוב.

פתרון

1. בהינתן $L \in \mathsf{P}$, מכונה M לבדיקת אוב עבור L פועלת כך על קלט x: בודקת (בזמן פולינומי) אם $x \in L$; שואלת את האוב על x; ודוחה אם האוב ענה באופן שלא תואם את התשובה לשאלה $x \in L$. בבירור יש למכונה הזו הצלחה של 100%.

2. דומה לסעיף 1: הפעם המכונה בודקת באופן הסתברותי את שייכות x ל־ L. אם נתקלה בתשובה חד משמעית, המכונה מקבלת אם ורק אם האוב ענה באופן דומה. אם בדיקת השייכות נסתיימה ב־ "לא יודע", המכונה מקבלת אם האוב טוען ש־ x שייך ל־ L. בבירור אם x שייך ל־ L המכונה תקבל תמיד, ואחרת היא תדחה בהסתברות $\frac{2}{3}$ לפחות (ההסתברות להצלחה בבדיקה הראשונית).

3. זהו עיקר התרגיל.

אם כן, למכונה M יש אוב שהוא אולי אוב עבור TQBF ואולי לא. בהינתן x, המכונה תבדוק האם האוב טוען כי $x \in L = \mathrm{TQBF}$ או $x \in \overline{L}$; בכל מקרה בסופו של דבר מתקבלת טענה לגבי שייכות x לשפה מסויימת ב־ PSPACE. הרעיון הוא ש־ M מסוגלת לבדוק האם x שייך לשפה ב־ PSPACE באמצעות הפעלת מערכת ההוכחה האינטראקטיבית לשפות ב־ PSPACE שקיומה הוכח במשפט $\mathsf{IP} = \mathsf{PSPACE}$.

מאחר ו־ M פולינומית, היא לא יכולה להפעיל את מערכת ההוכחה כמות שהיא שכן אינה מסוגלת לסמלץ את המוכיח, אולם היא מסוגלת להשתמש באוב שלה לצורך סימולציה של המוכיח; זאת מכיוון שההוכחה של $\mathsf{IP} = \mathsf{PSPACE}$ אינה דורשת מהמוכיח יותר מאשר היכולת להכריע את TQBF.

אם B <u>אינו</u> אוב עבור TQBF, הנסיון להשתמש באוב כדי לסמלץ את מערכת ההוכחה עשוי להיכשל כמובן, אך דבר זה אינו בעייתי (שימו לב כי לא נדרש מאום על הסיטואציה בה $L \neq B$ אך $B(x) = L(x)$; נקודה עדינה זו הופכת לבעלת חשיבות בשלב זה). אם לעומת זאת B הוא אכן אוב עבור TQBF אז סימולציית מערכת ההוכחה תעבוד באופן מושלם ו־ M תקבל תמיד (משלמות מערכת ההוכחה וכי האוב ענה נכון על x מלכתחילה).

באופן פורמלי יותר, ניתן להגדיר שפה L של כל השלשות (x, π, r) של קלט x למערכת ההוכחה, תעתיק פרוטוקול π, ותשובה r של המוכיח, כך שהמוכיח החוקי על הקלט x ולאחר שכבר התקיים קטע הפרוקוטול π, עונה למוודא את התשובה r. מכיוון שהמוכיח פועל ב־ PSPACE, השפה L היא שפה ב־ PSPACE.

עדיין לא סיימנו, שכן M לא יכולה להסתפק <u>בזיהוי</u> ההודעה הנכונה הבאה בפרוטוקול אלא עליה להיות מסוגלת <u>למצוא</u> אותה. לשם כך נגדיר שפה L' של שלשות (x, π, r') כך ש־ r' היא <u>רישא</u> של ההודעה החוקית של המוכיח. גם L' היא ב־ PSPACE, שכן ניתן לעבור סדרתית על כל ההשלמות הפולינומיות של r' ולבדוק אותן (אנו בעצם משחזרים כאן את ההוכחה שאם $\mathsf{P} = \mathsf{NP}$ אז זיהוי יעיל גורר חיפוש יעיל; ההנחה $\mathsf{P} = \mathsf{NP}$ הייתה הכרחית שם כדי להכריע את השפה L', אבל כאן אנו מקבלים זאת בחינם בגלל כוחה הרב של PSPACE). מכיוון ש־ $L' \in \mathsf{PSPACE}$, יש לה רדוקציה ל־ TQBF, ולכן M יכולה לבדוק שייכות ל־ L' על ידי שאלות לאוב ובכך לבנות את תשובתו הבאה של המוכיח ובפועל לסמלץ אותו.

שאלה 3 – מעגלים אי־דטרמיניסטיים

מעגל אי־דטרמיניסטי C הוא מעגל בו המשתנים מתחלקים לשתי קבוצות: משתני קלט המסומנים ב־ $x_1, \ldots, x_n$, ומשתנים אי־דטרמיניסטיים המסומנים ב־ $y_1, \ldots, y_m$. ערך המעגל מוגדר באופן הבא: $C(x) = 1$ אם קיימת השמה $y \in \{0,1\}^m$ למשתנים האי־דטרמיניסטיים כך שערך המעגל תחת ההשמה (x, y) הוא 1, ואחרת $C(x) = 0$.

נסמן ב־ NPSC את מחלקת השפות אשר קיימת עבורן סדרת מעגלים אי־דטרמיניסטיים (לא אחידים) בגודל פולינומי.

המחלקה NP/poly מוגדרת באופן הבא: $L \in$ NP/poly אם קיימת מ"ט א"ד פולינומית M וסדרת עצות a_n באורך פולינומי ב־ n, כך שלכל x מתקיים $x \in L$ אם"ם M מקבלת את הקלט $(x, a_{|x|})$.

1. הוכיחו או הפריכו: NPSC $\subseteq$ PSPACE.
2. הוכיחו כי NPSC $=$ NP/poly.
3. הוכיחו כי AM $\subseteq$ NP/poly.

פתרון

1. הטענה אינה נכונה.

נשים לב ש־ P/poly $\subseteq$ NPSC, שכן קל לראות שמעגל דטרמיניסטי הוא מקרה פרטי של מעגל אי־דטרמיניסטי, אבל P/poly $\not\subseteq$ PSPACE שכן P/poly מכילה שפות שאינן כריעות.

2. נראה הכלה דו־צדדית.

- $\subseteq$: נניח ש־ $L \in$ NPSC. אזי, לפי הגדרה, קיימת עבור L סדרת מעגלים אי־דטרמיניסטיים בגודל פולינומי $\{C_n\}_{n \geq 0}$. יהי $p(n)$ חסם פולינומי על גודל C_n.

  הרעיון הוא להשתמש במעגלים כעצות. נבנה מ"ט א"ד M שעל קלט (x, a), מפרשת את a (רישא מאורך לכל היותר $p(n)$ של a) כקידוד של מעגל אי־דטרמיניסטי C; מפענחת את הקידוד, מנחשת y, ומחשבת את $C(x, y)$; ולבסוף מקבלת אם"ם $C(x, y) = 1$.

  M פולנומית שכן גודל C פולינומי, ולכן שערוך $C(x, y)$ דורש זמן פולינומי (CVAL $\in$ P). הנכונות נובעת מנכונות סדרת המעגלים (כאשר העצה היא $a_{|x|} = |\langle C_{|x|} \rangle|$). לכן, $L \in$ NP/poly.

- $\supseteq$: נניח ש־ $L \in$ NP/poly. אזי, קיימת עבור L מ"ט א"ד פולינמית M וסדרת עצות $\{a_n\}_{n \geq 0}$ כך ש־ $|a_n| \leq p(n)$ עבור פולינום כלשהו $p(n)$, ונניח שזהו גם חסם על זמן ריצת M.

  נעזר במשפט Ladner ונמיר את ריצת M על הקלט $((x, y), a)$, כאשר $|x| = n$ ו־ y מייצגת בחירות א"ד של M, למעגל $C_n(x, y, a)$ עם כניסות $x_1, \ldots, x_n, y_1, \ldots, y_{p(n)}, a_1, \ldots, a_{p(n)}$, ולבסוף נחווט $a_n \leftarrow a$. מתקבלת משפחת מעגלים $\{C_n(x, y, a_n)\}_{n \geq 0}$ כך שגודל המעגל ה־ n־י הוא פולינומי ביחס ל־ $n + 2p(n)$, ולכן גם ביחס ל־ n. הנכונות נובעת מנכונות הבנייה של Ladner ומנכונות סדרת העצות. לכן, $L \in$ NPSC.

3. בהסתמך על סעיף 2 נראה ש־ AM $\subseteq$ NPSC.

רעיון: ההוכחה היא וריאציה על ההוכחה ש־ BPP $\subseteq$ P/poly. נשתמש בהוכחה של מרלין הגון בשביל המשתנים האי־דטרמיניסטיים עבור המעגל האי־דטרמיניסטי שנבנה, ונחפש מחרוזת אקראית שטובה לכל הקלטים שאותה נחווט למעגל.

תהא אם כן שפה $L \in$ AM. אזי, קיים עבור L פרוטוקול ארתור־מרלין (A, M) בעל 2 סיבובים, כך שמתקיים:

$$x \in L \implies \exists M : \mathbf{Pr}[A \leftrightarrow M \text{ accepts } x] \geq \frac{3}{4} \quad \left(\iff \exists M : \mathbf{Pr}[A \leftrightarrow M \text{ errs on } x] \leq \frac{1}{4} \right)$$
$$x \notin L \implies \forall M' : \mathbf{Pr}[A \leftrightarrow M' \text{ accepts } x] \leq \frac{1}{4} \quad \left(\iff \forall M' : \mathbf{Pr}[A \leftrightarrow M' \text{ errs on } x] \leq \frac{1}{4} \right)$$

כאן, A היא מכונה הסתברותית פולינומית המייצגת את ארתור, ו־ M מייצגת את מרלין.

כזכור, ניתן להגביר הסתברויות של מערכת הוכחה תוך שמירה על מספר הסיבובים (באמצעות הגברה במקביל), ולכן נוכל להניח שמתקיים:

$$\begin{aligned} x \in L &\implies \exists M : \mathbf{Pr}[A \leftrightarrow M \text{ errs on } x] \leq 2^{-2n} \\ x \notin L &\implies \forall M' : \mathbf{Pr}[A \leftrightarrow M' \text{ errs on } x] \leq 2^{-2n} \end{aligned}$$

נסמן ב־ $p(n)$ חסם פולינומי הן על אורכי מחרוזות האקראיות והן על זמן ריצת A.

ניזכר כיצד מתנהל פרוטוקול ארתור־מרלין עם 2 סיבובים, בהינתן קלט x:

- A מגריל מחרוזת אקראית $r \in \{0,1\}^{p(n)}$ ושולח ל־ M'. (שימו לב שכל האקראיות של A נמצאת ב־ r)
- M' מחזיר תשובה $y = y(x,r)$ מאורך לכל היותר $p(n)$.
- A מבצע חישוב סופי שתלוי בקלט x, באקראיות r, ובמענה המוכיח y, שלאחריו מחליט אם לקבל או לדחות.

אם כן, נוכל (באמצעות משפט Ladner למשל) להמיר את החישוב ש־ A מבצע למעגל בוליאני C (מגודל פולינומי) עם כניסות עבור x, r, ו־ y.

נקבע עתה אורך קלט n, ונתבונן בקלט מסוים $x \in \{0,1\}^n$. נרצה להגדיר כעת קבוצה BAD_x של מחרוזות "רעות" בדומה לנעשה בהוכחה ש־ $\mathsf{BPP} \subseteq \mathsf{P/poly}$. אולם בגלל החוסר סימטריה שבאי־דטרמיניזם אנו נאלץ להפריד למקרים לפי האם x שייך לשפה או לא.

- נניח ש־ $x \in L$. לכל מחרוזת אקראיות r, נסמן ב־ $y_M(x,r)$ את מענה מרלין ההגון, ונתבונן במעגל C כאשר מציבים ב־ y מענה זה. במקרה זה, נגדיר:

$$BAD_x := \left\{ r \in \{0,1\}^n \;\middle|\; C(x, r, y_M(x,r)) = 0 \right\}$$

- נניח ש־ $x \notin L$. במקרה זה, נגדיר:

$$BAD_x := \left\{ r \in \{0,1\}^n \;\middle|\; \exists y \colon C(x,r,y) = 1 \right\}$$

לפי הנחה, מתקיים (בשני המקרים):

$$\Pr_r \left[r \in BAD_x \right] = \frac{|BAD_x|}{2^{p(n)}} \leq \frac{1}{2^{2n}}$$

לכן,

$$\Pr_r \left[\exists x \in \{0,1\}^n : r \in BAD_x \right] \underset{\text{union bound}}{\leq} \sum_{x \in \{0,1\}^n} \Pr_r \left[r \in BAD_x \right] \leq 2^n \cdot \frac{1}{2^{2n}} = \frac{1}{2^n} \ll 1$$

מכך נסיק שקיימת מחרוזת אקראיות r^* כך שלכל $x \in \{0,1\}^n$ מתקיים $\exists y \colon C(x, r^*, y) = 1 \iff x \in L$.

לכן, $L \in \mathsf{NPSC}$ לפי הגדרה. הראינו ש־ $\mathsf{AM} \subseteq \mathsf{NPSC} = \mathsf{NP/poly}$.