תורת הסיבוכיות (236313)
אביב תשע"ב
מועד א'
4.7.2014

מרצה: פרופ' אייל קושלביץ

מתרגל: יוחאי קפלן

הנחיות:

- המבחן הוא עם חומר סגור.
- חל איסור מפורש על החזקת אמצעי תקשורת נייד, דוגמת טלפון סלולרי ברשות הנבחן בעת הבחינה.
- נמקו את כל תשובותיכם.
- בכל סעיף ניתן לקבל 20% מהניקוד אם במקום תשובה כותבים "לא יודע/ת".
- מותר להשתמש בכל טענה שהוכחה בהרצאה או בתרגול, בתנאי שמצטטים אותה באופן מדויק.
- השתדלו לא להתעכב יתר על המידה על סעיף מסויים, כדי לצבור מקסימום נקודות בזמן העומד לרשותכם.
- בסוף המבחן יש מספר תזכורות למושגים רלוונטים.

בהצלחה!

שאלה 1 (שאלת ש"ב, 10 נקודות)

נגריל אוב A באופן הבא: לכל $x \in \Sigma^*$, $x \in A$ בהסתברות $\frac{1}{2}$ באופן בלתי תלוי במילים האחרות.

הראו כי לכל $\varepsilon > 0$, בהסתברות $1 - \varepsilon$ (על פני כל הגרלות ה־A האפשריות) מתקיים $\mathrm{BPP} \subseteq \mathrm{P}^A$.

שאלה 2 (שאלת ש"ב, 20 נקודות)

שאלה זו עוסקת במערכת הוכחה (או בוררות) אינטראקטיבית בה שני מוכיחים "וכחנים" P_{yes} ו־P_{no} מנסים להוכיח למוודא (בורר) V טענות סותרות. המוכיח P_{yes} מנסה תמיד להוכיח שהקלט x שייך לשפה L ו־P_{no} מנסה להוכיח ש־x אינו בשפה.

פורמלית המוכיחים והמוודא כולם **דטרמיניסטיים**; המוכיחים אינם מוגבלים חישובית והמוודא מוגבל לחישוב דטרמיניסטי פולינומי ב־$|x|$ בזמן. **פרוטוקול בוררות** על קלט x מתנהל בסיבובים, כאשר בכל סיבוב המוכיחים שולחים שניהם **סימולטנית** הודעות למוודא. כל הודעה כזו עשויה להיות תלויה ב־x ובכל ההודעות שנשלחו בסיבובים **קודמים** (כולל אלו שנשלחו על ידי המוכיח השני). לאחר סיבוב ההודעות האחרון, המוודא מחליט האם לקבל או לדחות את x באמצעות חישוב פולינומי ב־$|x|$, התלוי בקלט x ובכל ההודעות שנשלחו במהלך ביצוע הפרוטוקול.

נאמר שפרוטוקול $\Pi = (V, P_{yes}, P_{no})$ כנ"ל הוא **פרוטוקול בוררות עבור השפה** L אם לכל קלט x מתקיים:

- אם $x \in L$ אז לכל מוכיח P^*_{no} המוודא V באינטראקציה עם (P_{yes}, P^*_{no}) מקבל את x.
- אם $x \notin L$ אז לכל מוכיח P^*_{yes} המוודא V באינטראקציה עם $\left(P^*_{yes}, P_{no}\right)$ דוחה את x.

(אינטואיטיבית: כדי להבטיח שהמוודא יפסוק נכון, מספיק שהמוכיח המצדד בתשובה הנכונה יפעל לפי הפרוטוקול Π).

נסמן ב־$\mathrm{RG}[c]$ את מחלקת השפות להן קיים פרוטוקול בוררות בן c סיבובים וב־RG את מחלקת השפות להן קיים פרוטוקול בוררות בו מספר הסיבובים פולינומי ב־$|x|$.

הוכיחו את הטענות הבאות:

1. לכל c, המחלקה $\mathrm{RG}[c]$ סגורה למשלים (5 נקודות).
2. $\Sigma_2^p \subseteq \mathrm{RG}[2]$ (5 נקודות).
3. אם קיימת מכונת טיורינג המכריעה את L בזכרון פולינומי ובזמן $t(n)$ אז $L \in \mathrm{RG}[O(\log t(n))]$ (5 נקודות).
4. $\mathrm{RG} = \mathrm{PSPACE}$ (5 נקודות).

שאלה 3 (20 נקודות)

שאלה זאת עוסקת בתכונות של שפות אונאריות.

תהי U מחלקת השפות האונאריות.

1. הוכח כי $P^U = P/poly$ (10 נקודות)
2. הוכח כי לכל $f, g \geq \log n$ פונקציות זכרון כך ש־$g = o(f)$ קיימת שפה אונארית $L \in DSPACE(f(n)) \setminus DSPACE(g(n))$ (10 נקודות).

שאלה 4 (10 נקודות)

הראה כי אם $PP = PH$ ההיררכיה הפולינומית קורסת (בשאלה זאת ניתן להשתמש במשפט Toda: $PH \subseteq P^{PP}$)

שאלה 5 (40 נקודות)

תהא $h : \mathbb{N} \to \mathbb{N}$. נגדיר את המחלקה $\mathrm{NP}/h(n)$ להיות אוסף כל השפות הניתנות לזיהוי על ידי מכונת טיורינג אי־דטרמיניסטית פולינומית בעלת "עצה" באורך $h(n)$ התלויה רק באורך הקלט n (כלומר, לקלטים באותו אורך מתאימה אותה עצה).

פורמלית, $L \in \mathrm{NP}/h(n)$ אם קיימת מכונת טיורינג אי־דטרמיניסטית פולינומית M וסדרה $\{a_n\}_{n\in\mathbb{N}}$ כך ש־$|a_n| \le h(n)$ וכך ש־M מקבלת את $w\$a_{|w|}$ אם ורק אם $w \in L$.

נסמן $\mathrm{NP}/poly = \bigcup_{c\in\mathbb{N}} \mathrm{NP}/n^c$

1. תהי $M_0, M_1, M_2 \ldots$ מניה של כל מכונות הטיורינג.
נגדיר את השפה $L = \left\{\varphi | \varphi \in SAT \wedge M_{|\varphi|} \in L_\epsilon\right\}$.
הוכח: $L \in \mathrm{NP}/poly$ (5 נקודות).

2. $f : \Sigma^* \to \Sigma^*$ היא רדוקציה פולינומית משמרת אורך מ־L_1 ל־L_2 אם היא רדוקציה פולינומית ובנוסף, לכל x, y $|f(x)| = |f(y)| \implies |x| = |y|$. נסמן $L_1 \le_{|p|} L_2$.
הוכח/הפרך: אם $L_1 \le_p L_2$ אז $L_1 \le_{|p|} L_2$ (5 נקודות).

3. הוכח/הפרך: אם $L_1 \le_{|p|} L_2$ ו־$L_2 \in \mathrm{NP}/poly$ אז $L_1 \in \mathrm{NP}/poly$ (5 נקודות).

4. נגדיר את המכונה M שעל קלט φ, נוסחת CNF, ועצה a, מציבה את a ל־$|a|$ המשתנים הראשונים ב־φ ומקבלת נוסחא φ_a. מנחשת השמה ל־φ_a ומקבלת אם ההשמה מספקת.
עבור סדרת עצות $A = \{a_i\}_{i\in\mathbb{N}}$ נסמן את $L_A(M)$ כשפתה של M עם סדרת העצות A.
הוכח: לכל $L \in \mathrm{NP}/poly$ קיימת סדרת עצות A כך ש־$L \le_{|p|} L_A(M)$ (5 נקודות).

5. הוכח: $\mathrm{P} = \mathrm{NP}$ גורר $\mathrm{P}/poly = \mathrm{NP}/poly$ (5 נקודות).

6. הוכח: $\mathrm{AM}[2] \subseteq \mathrm{NP}/poly$ (5 נקודות).

7. נגדיר $(\mathrm{P}/poly)^B$ להיות מחלקת השפות המתקבלת ע"י מכונות דטרמיניסטיות פולינומית עם עצה פולינומית ואוב לשפה B.
הוכח כי $(\mathrm{P}/poly)^{\mathrm{NP}/poly} = (\mathrm{P}/poly)^{\mathrm{NP}}$ (5 נקודות).

8. תזכורת: עבור מחלקת שפות C נגדיר את $\exists_p C$ להיות כל השפות L כך שקיים יחס חסום פולינומית $R_L \in C$ המקיים $x \in L \iff \exists_p y : (x, y) \in R_L$. בצורה דומה נגדיר את $\forall_p C$.
הוכח: אם $\mathrm{PSPACE} \subseteq \mathrm{NP}/poly$ אז $\mathrm{PSPACE} = \exists_p \forall_p \mathrm{P}^{\mathrm{NP}}$ (5 נקודות).

תזכורות

- $\mathrm{AM}[2]$ היא מחלקת השפות שיש עבורן של פרוטוקולים אינטראקטיבים באורך שני סיבובים. המוודא הוא מ"ט הסתברותית פולינומית, שבסיבוב הראשון מגרילה ביטים ושולחת אותם למוכיח, ששולח תשובה. המוודא מבצע חישוב על תשובה זאת ומקבל/דוחה. המוודא צודק בהסתברות לפחות $2/3$.
- $\mathrm{P}/poly$ היא מחלקת השפות המתקבלות ע"י משפחת מעגלים בגודל פולינומי, או מחלקת השפות המתקבלות ע"י מכונת טיורינג פולינומית בעלת עצה באורך פולינומי התלויה רק באורך הקלט.
- $L_\epsilon = \{\langle M\rangle | \epsilon \in L(M)\}$