תורת הסיבוכיות (236313)
אביב תשע"ב
מועד ב'
23.9.2012

מרצה: פרופ' אייל קושלביץ

מתרגל: גדי אלכסנדרוביץ'

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.

בהצלחה!

שאלה 1 (25 נקודות)

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

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

1. נסמן $\mathrm{P/poly} = \bigcup_{c\geq 1} \mathrm{P}/n^c$. הוכיחו כי $L \in \mathrm{P/poly}$ אם ורק אם קיימת משפחת מעגלים פולינומית המזהה את L (10 נקודות).
2. הוכיחו כי אם $\mathrm{EXPTIME} \subseteq \mathrm{P}/1$ אז $\mathrm{P{=}NP}$ (5 נקודות).
3. הוכיחו כי אם $\mathrm{PSPACE} \subseteq \mathrm{P/poly}$ אז $\mathrm{PSPACE} = \Sigma_2^p$ (10 נקודות).

שאלה 2 (25 נקודות)

מכונת טיורינג עם אוב M תיקרא **איתנה** (Robust) אם לכל שתי שפות אוב A, B, מתקיים $L(M^A) = L(M^B)$ (השפה ש-M מקבלת אינה תלויה באוב). אם M איתנה, נסמן $L(M) = L(M^\emptyset)$ (כלומר, $L(M)$ היא השפה שאותה M מקבלת עם אוב **כלשהו**).

בהינתן מכונת טיורינג איתנה עם אוב M נאמר כי שפה A **עוזרת** ל-M אם M^A מכריעה את $L(M)$ בזמן פולינומי (אין דרישה שעבור אוב אחר M לא מכריעה את $L(M)$ בזמן פולינומי).

נסמן ב-$\mathrm{P}_{help}(A)$ את קבוצת כל השפות שניתנות להכרעה בידי מכונת טיורינג איתנה ש-A עוזרת לה.

עבור מחלקת שפות C נגדיר $\mathrm{P}_{help}(\mathrm{C}) = \bigcup_{A\in\mathrm{C}} \mathrm{P}_{help}(A)$. כמו כן נסמן $\mathrm{P}_{help} \triangleq \mathrm{P}_{help}\left(2^{\Sigma^*}\right)$.

1. תנו דוגמה למכונת טיורינג איתנה עם אוב M כך ש-$L(M) = \mathrm{SAT}$ ודוגמה לשתי שפות אוב A, B כך שעל כל קלט $x \in \mathrm{SAT}$, M^A רצה בזמן $O(p(n))$ עבור פולינום p כלשהו ו-M^B רצה בזמן $\Omega\left(2^{q(n)}\right)$ עבור פולינום $q(n)$ כלשהו (5 נקודות).
2. הוכיחו כי $\mathrm{P}_{help} = \mathrm{NP} \cap \mathrm{coNP}$ (10 נקודות).
3. הוכיחו כי $\mathrm{P}_{help}(\mathrm{BPP}) \subseteq \mathrm{ZPP}$ (10 נקודות).

שאלה 3 (25 נקודות)

בשאלה זו נציג הגדרה אלטרנטיבית של NL. סרט **לקריאה חד פעמית** במכונת טיורינג הוא סרט שהראש הקורא בו יכול לנוע רק ימינה או להישאר במקום.

נגדיר מחלקה VNL (Verifier-NL) בתור מחלקת השפות L כך שקיימת מכונת טיורינג **דטרמיניסטית** M עם סרט קלט לקריאה בלבד, סרט "עד" לקריאה חד פעמית וסרט עבודה, וקיים פולינום $p : \mathbb{N} \to \mathbb{N}$ כך שלכל $w \in \{0,1\}^*$ מתקיים

$$w \in L \iff \exists u \in \{0,1\}^{p(|w|)} \left(M(w,u) = \mathrm{acc}\right)$$

כאשר $M(w,u)$ מתאר את פלט המכונה בריצה שבתחילתה w כתוב בסרט הקלט ו-u כתוב בסרט העד, וכמו כן M פועלת בסיבוכיות זכרון $O(\log|w|)$.

1. הוכיחו כי $\mathrm{VNL} = \mathrm{NL}$ (10 נקודות).
2. נניח שנסיר את הדרישה שסרט העד יהיה לקריאה חד פעמית (אך נותיר אותו כסרט לקריאה בלבד). לאיזו מחלקה מוכרת שווה VNL כעת? (5 נקודות).
3. נניח שנתיר ל-M לעבוד בסיבוכיות זכרון פולינומית ול-u להיות מגודל אקספוננציאלי ($O(2^n)$), אך סרט העד נותר סרט לקריאה חד פעמית. לאיזו מחלקה מוכרת שווה VNL כעת? (10 נקודות).

שאלה 4 (15 נקודות)

תזכורת: קיימת רדוקציה פולינומית הסתברותית $L_1 \leq_r L_2$ אם קיימת מכונת טיורינג פולינומית הסתברותית M כך שלכל קלט x מתקיים $\Pr\left[x \in L_1 \iff M(x) \in L_2\right] \geq \frac{2}{3}$.

נגדיר: $\mathrm{BP} \cdot \mathrm{NP} = \{L | L \leq_r 3\mathrm{SAT}\}$.

הוכיחו כי $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$ (תזכורת: AM היא מחלקת השפות שקיים עבורן פרוטוקול ארתור־מרלין שבו ארתור שולח למרלין הודעה, מרלין עונה וארתור דוחה או מקבל בהתאם לתשובה).

שאלה 5 (10 נקודות)

נגדיר פונקציה:

$$f(C) \quad = \quad \frac{\left|a \in \{0,1\}^n \ | \ C(a) = 1\right|}{2^n}$$

דהיינו, f על מעגל C עם n קלטים מחזירה את אחוז ההשמות המקבלות ל־C.

הוכיחו כי אם f ניתנת לקירוב $\frac{1}{42}$־חיבורי (כלומר, קיים אלגוריתם יעיל A כך ש־$\left|A(C) - f(C)\right| \leq \frac{1}{42}$ לכל C) אז $\mathrm{P} = \mathrm{BPP}$.