תורת הסיבוכיות (236313)
אביב תשע"ו
9.6.2016

מרצה: פרופ' אייל קושלביץ
מתרגל: יובל דגן

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 (15 נק')

בהרצאה הגדרנו כפל של שתי מטריצות בוליאניות, A, B מסדר $n \times n$, על ידי: $(AB)_{ij} = \bigvee_{k=1}^{n} (A_{ik} \wedge B_{kj})$. נגדיר את הפונקציה f, שבתור קלט מקבלת n מטריצות בוליאניות מסדר $n \times n$ ומחשבת את הכפל הבוליאני שלהן. כלומר, $f(A_1, A_2, \ldots, A_n) = A_1 A_2 \cdots A_n$. שימו לב ש־ f יכולה לקבל קלטים לכל n.

1. (10 נק') הראו כי f ניתנת לחישוב בזיכרון $O(\log^2 n)$.
2. (5 נק') הראו כי אם f ניתנת לחישוב בזיכרון של $O(\log n)$ אז $\mathrm{DL} = \mathrm{NL}$.

שאלה 2 (10 נק')

הוכיחו/הפריכו: $\mathrm{P} = \mathrm{DSPACE}(n)$.

שאלה 3 (45 נק')

בעיית הבטחה π מוגדרת ע"י שתי קבוצות זרות של מילים (π_{YES}, π_{NO}), כאשר π_{YES} היא קבוצת ה"מילים שיש לקבל", ו־ π_{NO} היא קבוצת ה"מילים שיש לדחות". נשים לב כי ייתכן שיש מילים שאינן ב־ π_{YES} ולא ב־ π_{NO}. באופן כללי, נאמר שמ"ט M מקבלת את π, אם M מקבלת את כל המילים שב־ π_{YES} ודוחה את כל המילים שב־ π_{NO}, כאשר אין דרישות עבור מילים אחרות.

נגדיר מספר מחלקות של בעיות הבטחה. למשל, pr-BPP, מחלקת בעיות ההבטחה של BPP, היא מחלקת הבעיות $\pi = (\pi_{YES}, \pi_{NO})$, עבורן קיימת מ"ט הסתברותית פולינומית M שמקיימת:

- לכל $x \in \pi_{YES}$ מתקיים: $\Pr[M(x) = acc] \geq \frac{2}{3}$
- לכל $x \in \pi_{NO}$ מתקיים: $\Pr[M(x) = rej] \geq \frac{2}{3}$.

כך ניתן גם להגדיר את pr-RP, pr-coRP, את pr-NP בעזרת מכונות א"ד, ואת pr-coNP בעזרת מכונות קו־אי־דטרמיניסטיות.

כעת, נגדיר את המושג של בעיית הבטחה בתור אוב. תהי $\pi = (\pi_{YES}, \pi_{NO})$ בעיית הבטחה, M מכונת טיורינג ו־ L שפה. נאמר ש $L(M^{\pi}) = L$ אם לכל אוב A שמקיים $\pi_{YES} \subseteq A$ ו־ $\pi_{NO} \subseteq \bar{A}$ מתקיים כי $L = L(M^{A})$. כלומר, המכונה M צריכה לקבל את L בלא תלות בתשובות שמחזיר האוב למילים שאינן ב־ $\pi_{YES} \cup \pi_{NO}$.

כך, ניתן להגדיר למשל את $\mathrm{P}^{\text{pr-NP}}$, $\mathrm{RP}^{\text{pr-RP}}$ וכו'...

1. (5 נק') נגדיר את בעיית ההבטחה $xSAT = (\pi_{YES}, \pi_{NO})$ על ידי

$$\pi_{YES} = \{(\phi_1, \phi_2) \colon \phi_1 \in SAT, \phi_2 \notin SAT\}$$

$$\pi_{NO} = \{(\phi_1, \phi_2) \colon \phi_1 \notin SAT, \phi_2 \in SAT\}$$

הוכיחו כי $\mathrm{xSAT} \in \text{pr-NP} \cap \text{pr-coNP}$.

2. (10 נק') מהי המחלקה $P^{NP \cap coNP}$? הוכיחו.
3. (10 נק') הוכיחו כי $SAT \in P^{\text{pr-NP} \cap \text{pr-coNP}}$.
4. (10 נק') הראו שקיימת בעיה שלמה ב־ pr-RP והוכיחו. כלומר, שקיימת $\pi = (\pi_{YES}, \pi_{NO}) \in \text{pr-RP}$, כך שלכל $\pi' = (\pi'_{YES}, \pi'_{NO}) \in \text{pr-RP}$ קיימת רדוקציה פולינומית f מ־ π' ל־ π שמקיימת:
   - לכל $x \in \pi'_{YES}$ מתקיים: $f(x) \in \pi_{YES}$.
   - לכל $x \in \pi'_{NO}$ מתקיים: $f(x) \in \pi_{NO}$.

5. (10 נק') הוכיחו כי $\mathrm{BPP} \subseteq \mathrm{RP}^{\text{pr-coRP}}$.
רמז: בהוכחה ש־ $BPP \subseteq \Sigma_2^p$, הראינו שלכל $L \in BPP$ קיימת מכונת טיורינג דטרמיניסטית ופולינומית M, כך שלכל x:

$$x \in L \Leftrightarrow \exists s_1, \ldots, s_\ell \forall t,\ \bigvee_{i=1}^{\ell} (M(x, s_i \oplus t) = ACC)$$

בנוסף, מההוכחה נבעו שתי הטענות הבאות:

- אם $x \in L$ אז לפחות לחצי מהבחירות של $(s_1, \ldots, s_\ell)$ מתקיים כי

$$\forall t,\ \bigvee_{i=1}^{\ell} (M(x, s_i \oplus t) = ACC)$$

- אם $x \notin L$ אז לכל בחירה של $s_1, \ldots s_\ell$ מתקיים שלכל היותר לחצי מהבחירות של t מתקיים כי

$$\bigvee_{i=1}^{\ell} (M(x, s_i \oplus t) = ACC)$$

אין צורך לחזור על ההוכחה או להוכיח את הטענות.

שאלה 4 (10 נק')

תהי L פונקציה הניתנת לחישוב בזמן $O(T(n))$ במכונת טיורינג דטרמיניסטית חד סרטית, עבור פונקציה $T(n)$ כלשהי. בהרצאה ראינו ש־ L ניתנת לייצוג על ידי משפחת מעגלים בגודל $O(T(n)^2)$. בשאלה זו, עליכם להוכיח כי קיימת ל־ L משפחת מעגלים לא יוניפורמית בגודל $O\left(T(n)\log(T(n))\right)$.

היעזרו בטענה הבאה: קיימת ל־ L מכונת טיורינג דטרמיניסטית חד־סרטית M, המקיימת:

- M רצה בזמן $O(T(n)\log(T(n)))$.
- אם x, y קלטים באותו גודל n, אז M רצה זמן זהה עליהם. בנוסף, אם נסמן ב־ $h_1, h_2, h_3, \ldots, h_k$ את סדרת המיקומים של הראש הקורא של M במהלך החישוב על הקלט x, ונסמן ב־ $g_1, g_2, \ldots, g_k$ את סדרת המיקומים במהלך החישוב על הקלט y, אז $h_i = g_i$ לכל i.

(מכונה כזו נקראת Oblivious TM).

שאלה 5 (20 נק')

בשאלה זו נשתמש בהגדרה של AM עם נאותות מושלמת, כפי שהוגדר בהרצאה.

1. (5 נק') הוכיחו כי $\mathrm{AM}[2] \subseteq \Pi_2^p$.
2. (15 נק') הוכיחו כי אם GNI היא coNP שלמה, אז ההיררכיה הפולינומית קורסת.
הדרכה: הוכיחו כי תחת ההנחה הנ"ל, $\Sigma_2 \subseteq \Pi_2$, והשתמשו בכך שידוע ש־ $\mathrm{AM}[k] = \mathrm{AM}[2]$ לכל $k \in \mathbb{N}$.