תורת הסיבוכיות (236313)
אביב תשע"ב
מועד ב'
19.9.2014

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.

בהצלחה!

שאלה 1 (שאלת ש"ב, 10 נקודות)

נגדיר את המחלקה RL' על ידי השמטת הדרישה של ריצה בזמן פולינומי מהגדרת RL. הוכיחו כי $\mathrm{NL}=\mathrm{RL}'$.

שאלה 2 (שאלת ש"ב, 20 נקודות)

ידוע כי $\mathrm{PARITY} \notin \mathrm{AC}^0$. מטרת שאלה זו להוכיח כי גם $\text{s-t-CON} \notin \mathrm{AC}^0$.

לכל הצבה למשתנים $x_1,\ldots,x_n$ נתאים גרף לא מכוון G_1 בעל $n+2$ צמתים שנסמנם $s,v_1,\ldots,v_n,t$. בגרף G_1 יש קשת בין s ל־v_i אם i הוא הראשון עבורו $x_i=1$; יש קשת בין v_j ל־t אם j הוא האחרון עבורו $x_j=1$; ויש קשת בין v_i ל־v_j אם $i<j$, $x_i=x_j=1$ וכל המשתנים x_l כך ש־$i<l<j$ מקיימים $x_l=0$.

1. תארו מעגל AC^0 המחשב את מטריצת השכנויות של G_1 (מטריצה מסדר $(n+2)\times(n+2)$ של 0־ים ו־1־ים) מתוך המשתנים $x_1,\overline{x_1},\ldots,x_n,\overline{x_n}$ (5 נקודות).
2. תארו מעגל AC^0 המחשב את מטריצת השכנויות של גרף G_2 שבו יש אותם הצמתים כמו ב־G_1 וקשת בין u ל־w אם ורק אם יש מסלול באורך בדיוק 2 בין u ל־w ב־G_1 (10 נקודות).
3. בעזרת G_2 הראו כי $\mathrm{PARITY} \le_{\mathrm{AC}^0} \text{s-t-CON}$ (5 נקודות).

שאלה 3 (20 נקודות)

תזכורת: עבור מחלקת שפות C נגדיר את $\exists_p C$ להיות כל השפות L כך שקיים יחס חסום פולינומית $R_L \in C$ המקיים $x \in L \iff \exists_p y : (x,y) \in R_L$.

נגדיר את **ההירכיה הפולינומית של** C בצורה הרקורסיבית הבאה:

$PH_0(C)=C$ ו־

$PH_i(C)=\exists_p PH_{i-1}(C)$.

נסמן $PH(C)=\bigcup_{i\in\mathbb{N}} PH_i(C)$. (שימו לב כי $PH=PH(\mathrm{P})$)

1. הוכח/הפרך: $\forall C : PH_1(C)=NP^C$ (5 נקודות).
2. הוכח שההירכיה הפולינומית של PSPACE קורסת לרמה 0 (5 נקודות).
3. הוכח שההירכיה הפולינומית של E קורסת לרמה 1, אך לא לרמה 0, תזכורת $E=\bigcup_{c\in\mathbb{N}} DTIME(2^{cn})$ (10 נקודות).

שאלה 4 (50 נקודות)

למחלקות סבוכיות בסגנון BPP לא ידועות שפות שלמות או גרסאות מתאימות של משפטי היררכיה. בשאלה זאת נבחן וריאציה על המושג של שפה, שמאפשרת להתגבר על בעיות אלו.

בעיית הבטחה π מוגדרת ע"י שתי קבוצות זרות של מילים (π_{YES},π_{NO}). בעיית הבטחה ניתן לפיתרון בזמן פולינומי אם קיימת מ"ט דטרמיניסטית פולינומית שמקבלת את כל המילים ב־π_{YES} ודוחה את כל המילים ב־π_{NO}. נגדיר את $promise\text{-}P$ (נסמנה $p\text{-}P$) להיות מחלקת בעיות ההבטחה הניתנות לפיתרון בזמן פולינומי.

נגדיר את $promise\text{-}BPP$ (נסמנה $p\text{-}BPP$) להיות מחלקת בעיות ההבטחה כך שקיימת מ"ט הסתברותית פולינומית M שמקיימת:

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

1. נגדיר את $\{M$ מ"ט הסתברותית שרצה זמן $\geq k$ ומקבלת את x בהסתברות לפחות $\frac{2}{3}|\left(M,x,1^k\right)\}= L$.
הוכח ש־L היא BPP־קשה ביחס לרוקציות פולינומיות (6 נקודות).

2. סטודנט מתחכם טוען ש־$L\in BPP$ ע"י האלגוריתם הבא:
על קלט $\left(M,x,1^k\right)$ הרץ את M על x למשך k צעדים וענה כמוה.
הסבר מדוע האלגוריתם לא נכון (6 נקודות).

3. הגדר רדוקציה בין בעיות הבטחה כך שאם $\pi_1 \leq \pi_2$ אז:

(א) אם $\pi_2\in p\text{-}P$ אז $\pi_1\in p\text{-}P$

(ב) אם $\pi_2\in p\text{-}BPP$ אז $\pi_1\in p\text{-}BPP$

הוכח את תשובתך (6 נקודות).

4. הצע בעיה שלמה ב־$p\text{-}BPP$. הוכיח את שלמותה (6 נקודות).

5. הנח כי $p\text{-}P=p\text{-}BPP$, הוכח כי $p\text{-}NP=p\text{-}MA$ (6 נקודות).
($p\text{-}NP$ היא מחלקת בעיות ההבטחה כך שקיימת מ"ט א"ד פולינומית שיש לה מסלול מקבל לכל $x\in\pi_{YES}$ ואין מסלול מקבל לכל $x\in\pi_{NO}$. $p\text{-}MA$ היא מחלקת בעיות ההבטחה כך שקיים פרוטוקול MA שבסופו המוודא מקבל כל $x\in\pi_{YES}$ בהסתברות גדולה מ־$\frac{2}{3}$ ודוחה כל $x\in\pi_{NO}$ בהסתברות גדולה מ־$\frac{2}{3}$)

6. תהי $\pi=\left(\pi_{YES},\pi_{NO}\right)$ בעיית הבטחה. נאמר ששפה L היא **קונסיסטנטית** עם π אם $\pi_{YES}\subseteq L$ ו־ $\pi_{NO}\subseteq \bar{L}$ נסמן ב־$C\left(\pi\right)$ את מחלקת השפות הקונסיסטנטיות עם π. נאמר ש־$L\in P^{\pi}$ אם קיימת מ"ט דטרמיניסטית פולינומית M כך ש־$\forall L'\in C\left(\pi\right):L=L\left(M^{L'}\right)$. נגדיר $\mathrm{P}^{p\text{-}BPP}=\bigcup_{\pi\in p\text{-}BPP}\mathrm{P}^{\pi}$. בצורה דומה נגדיר את NP^{π} ו־$\mathrm{NP}^{p\text{-}BPP}$.
לאיזה מחלקה מוכרת שווה $\mathrm{P}^{p\text{-}BPP}$ (5 נקודות)?

7. לאיזה מחלקה מוכרת שווה $\mathrm{NP}^{p\text{-}BPP}$ (5 נקודות)?

8. נגדיר $p-BP\left(t\left(n\right)\right)$ להיות מחלקת בעיות ההבטחה הניתנות לפיתרון הסתברותי בזמן $O\left(t\left(n\right)\right)$.
תהי $M_1,M_2\ldots$ מניה של מכונות הטורינג ההסתברותיות כך שניתן בהינתן 1^n לחשב את קידוד M_n ב $O\left(n^2\right)$ זמן.
נגדיר את הפונקציה $f\left(1\right)=2, f\left(i+1\right)=2^{\left(f\left(i\right)^4\right)}$.
נגדיר את המכונה U להיות מכונה שעל קלט 1^n (היא דוחה קלט מצורה אחרת) מבצעת:

(א) אם $f\left(i\right)<n<f\left(i+1\right)$ אז סמלץ מסלול (באופן אקראי) של המכונה ההסתברותית M_i על הקלט 1^{n+1} למשך n^3 צעדים וענה כמוהה. אם היא לא עוצרת במהלכם, קבל.

(ב) אם $n=f\left(i+1\right)$ אז סמלץ את כל מסלולי החישוב של M_i על $1^{f\left(i\right)+1}$ למשך $\left(f\left(i\right)+1\right)^3$ צעדים, קבל אם M דוחה בהסתברות לפחות $\frac{2}{3}$ אחרת דחה.

הוכח כי בעיית ההבטחה של U נמצאת ב־$p-BP\left(n^5\right)$ (5 נקודות).

9. הוכח $p\text{-}BP\left(n^2\right)\subsetneq p\text{-}BP\left(n^5\right)$ (5 נקודות).
ניתן להשתמש בעובדה שקיימת מניה של מכונות הטורינג ההסתברותיות שמקיימת את הדרישות מהסעיף הקודם ושבה כל מכונה מופיעה אינסוף פעמים.