הטכניון – מכון טכנולוגי לישראל
הפקולטה למדעי המחשב

30.6.2003

פרופ' איל קושלביץ
מיכל אהרון

בחינה סופית

תורת הסיבוכיות

אביב תשס"ג – מועד א'.

הנחיות:

1. הבחינה עם חומר סגור.
2. נמקו את כל תשובותיכם.
3. התחילו כל תשובה בדף חדש.
4. בפתרון כל סעיף מותר להסתמך על טענות המופיעות בסעיפים קודמים.
5. מומלץ לא "להתקע" זמן רב מדי על אף סעיף.
6. משך הבחינה – 3 שעות.

בהצלחה !

שאלה 1: (36 נקודות)

<u>הגדרה:</u>

$UP = \{L \mid$ קיימת מ"ט א"ד פולי' המקבלת את L, ובה לכל קלט x יש לכל היותר מסלול מקבל אחד$\}$.

בשאלה זו נדון בסיבוכיות בעיית הפרוק (factoring). נזכיר כי בעית ההכרעה המתאימה (בהינתן מספר, האם הוא ראשוני או פריק) הוכחה לאחרונה כשייכת ל- P.

נזכיר כי לכל מספר טבעי $m \geq 2$ יש פרוק יחיד למספרים ראשוניים: $m = p_1 \cdot p_2 \cdot \ldots \cdot p_k$,

כך שלכל i: $p_i \leq p_{i+1}$, p_i ראשוני.

בעיית הפרוק הינה: על קלט m חשב את הפרוק. כלומר: $F(m) = p_1, p_2, \ldots, p_k$.

נגדיר שפה: $L = \{(m,r) \mid$ קיים $1<s<r$ המחלק את $m\}$.

<u>הוכח:</u>

א. (2 נק') $L \leq^T F$ (כלומר: קיימת רדוקצית טיורינג פולינומית מ- L ל- F).

ב. (10 נק') $F \leq^T L$.

ג. (12 נק') $L \in UP \cap co\text{-}UP$.

ד. (12 נק') נתבונן באלגוריתם הבא A על קלט m שמטרתו חישוב F(m).

> עבור $i = 1,2,3,\ldots$,
>
> עבור $j = 1,2,\ldots,i$,
>
> הרץ את מ"ט M_j (המכונה ה- j'ית בסדר לקסיקוגרפי) למשך i צעדים.
>
> אם M_j עוצרת, נסמן את הפלט שלה $(p_1,\ldots,p_k)$, ונבדוק האם זהו פרוק של m.
>
> אם כן – עצור, אחרת – המשך.

<u>הוכח:</u> A אלג' פולינומיאלי לפרוק **אם ורק אם** קיים אלג' פולינומיאלי לפרוק.

שאלה 2: (20 נקודות)

<u>הגדרה</u>: שפה L ניתנת לרדוקציה עצמית אם קיימת מ"ט פולינומית M^L המקבלת את L, כך שלכל קלט x, המכונה M^L שואלת את האוב רק שאלות y כך ש: $|y| < |x|$.

נגדיר: $SR = \{ L \mid$ L ניתנת לרדוקציה עצמית $\}$.

נאמר ששפה L היא SR-שלמה אם:

א. $L \in SR$.

ב. $\forall L' \in SR \quad L' \leq_p L$.

<u>הוכח</u>: TQBF היא SR-שלמה.

שאלה 3: (20 נקודות)

IPL1 היא מחלקת השפות שיש עבורן הוכחה אינטראקטיבית כפי שהוגדרה בהרצאה (שלמות מלאה, נאותות בהסת' 2/3), עם המגבלות הבאות:

- ההוכחה הינה בסיבוב אחד (המוכיח שולח הודעה π והמוודא מחליט ע"י פרוצדורה פולינומית הסתברותית אם לקבל או לדחות את x).
- המוודא עובד בסיבוכיות מקום לוגריתמית (לשם הבהירות, נניח כי למוודא סרט קלט לקריאה בלבד, סרט הוכחה לקריאה בלבד, וסרט עבודה, שבו הוא משתמש במקום לוגריתמי).

<u>הוכח</u>: א. (10 נק') $IPL1 \subseteq NP$.

ב. (10 נק') $NP \subseteq IPL1$.

שאלה 4: (24 נקודות)

נגדיר: $\alpha(n) = \min_s \{$ כל פונקציה $f:\{0,1\}^n \rightarrow \{0,1\}$ ניתנת לחישוב ע"י מעגל בגודל $\leq s$ $\}$ (בהרצאה ראינו כי $\alpha(n) = O(n \cdot 2^n)$).

א. (12 נק') (משפט היררכיה למעגלים)

לכל $0 \leq g(n) < \alpha(n)$ קיימת פונקציה $f:\{0,1\}^n \rightarrow \{0,1\}$ שלא ניתן לחשב אותה בסיבוכיות $g(n)$, אבל ניתן לחשב אותה בסיבוכיות $g(n)+O(n)$.

הדרכה: התבונן בזוגות של פונקציות הנבדלות זו מזו בערכן על השמה בודדת.

ב. (12 נק') לכל $c>0$, קיימת ב- PH שפה עם סיבוכיות מעגלים של לפחות n^c.

הדרכה: השתמש בתוצאת הסעיף הקודם.