TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE
HAIFA 32000, ISRAEL

הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב
חיפה 32000

ט"ו באלול תשס"ו 8 בספטמבר 2006

תורת הסיבוכיות (236313)

מבחן סיום מועד א'

סמסטר אביב תשס"ו

מרצה: פרופ' איל קושלביץ.

מתרגל: רועי אנגלברג.

הנחיות:

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

ב ה צ ל ח ה!

שאלה 1 (40 נק')

בהנתן שפה L, נגדיר את הפונקציה $f_L(x)$ להיות מספר המילים הקטנות/שוות לקסיקוגרפית ל- x השייכות לשפה L. כלומר: $f_L(x)=|\{ y \mid y\in L \text{ and } y\le x \}|$, כאשר היחס $\le$ מוגדר לפי הסדר הלקסיקוגרפי.

א. (7 נק') הוכיחו כי לכל $L\in PSPACE$ מתקיים ש- $f_L\in FPSPACE$ (תזכורת: המחלקה FPSPACE הינה מחלקת הפונקציות הניתנות לחישוב בזכרון פולינומי).

המחלקה UP מוגדרת כאוסף השפות להן קיימת מ"ט **א"ד** M העובדת בזמן פולינומי המקבלת אותן ולכל קלט יש ל- M מסלול מקבל **אחד לכל היותר**.

ב. (8 נק') הוכיחו כי לכל $L\in UP$ מתקיים ש- $f_L\in \#P$.

ג. (10 נק') הוכיחו כי **אם** $P=P^{\#P}$ **אזי** לכל $L\in P$ מתקיים ש- $f_L\in FP$.

ד. (15 נק') הוכיחו כי **אם** לכל $L\in P$ מתקיים ש- $f_L\in FP$ **אזי** $P=P^{\#P}$.

שאלה 2 (25 נק')

תהי strong-CON = { G | G is a strongly-connected directed graph }.

א. (10 נק') הוכיחו כי strong-CON$\in$NL.

ב. (15 נק') הוכיחו כי strong-CON היא NL-שלמה.

שאלה מס' 3 (35 נק')

נגדיר *מערכת הוכחה מרובת מוכיחים עבור שפה L* באופן דומה להגדרת מערכת הוכחה אינטראקטיבית עבור שפה L (עם מוכיח יחיד) כפי שהוצגה בהרצאה:

המערכת מורכבת מתיאור של מ"ט פולי' הסתברותית V (להלן המוודא) ותיאור של k (מס' קבוע כלשהו) של מ"ט לא מוגבלות חישובית אך **דטרמיניסטיות** $P_1,\ldots,P_k$ (להלן המוכיחים). לכל מוכיח P_i יש ערוץ תקשורת **נפרד** עם המוודא V, אך אין למוכיחים אפשרות לתקשר ביניהם (במהלך ריצת הפרוטוקול). במצב ההתחלתי הקלט x נתון למוודא ולכל המוכיחים. בכל סיבוב, המוודא יכול לשלוח הודעה (להלן שאלה) לכל מוכיח P_i בנפרד. כאשר הוא עושה כן, רק המוכיח המתאים מקבל את השאלה והוא עונה

עליה ביט (להלן תשובה) אותו מקבל רק המוודא (בסיבוב אחד המוודא יכול לשאול במקביל כמה מוכיחים). המערכת מקיימת את שתי הדרישות הבאות:

1. שלמות מלאה – לכל $x \in L$, בפרוטוקול בין המוודא למוכיחים המוודא מקבל את x בהסתברות 1.
2. נאותות (חלשה) – לכל $x \notin L$ ולכל k מוכיחים $P'_1,\ldots,P'_k$, בפרוטוקול בין המוודא למוכיחים המוודא מקבל את x בהסתברות קטנה מ- $1-\frac{3}{4p(|x|)}$ עבור $p(n)$ פולינום כלשהו.

נסמן את מחלקת השפות להן קיימת מערכת הוכחה מרובת-מוכיחים עם k מוכיחים ב- $O(t(n))$ סיבובים שבה המוודא משתמש ב- $O(r(n))$ ביטי אקראיות, ע"י $MIP[k,r(n),t(n)]$.

א. (15 נק') הוכיחו כי לכל שפה $L \in MIP[k,r(n),t(n)]$, קיים מוודא PCP שמשתמש ב- $O(r(n))$ ביטי אקראיות, קורא $O(k \cdot t(n))$ ביטי הוכחה ומקיים:
   1. שלמות מלאה;
   2. נאותות בהסתברות קטנה מ- $1-\frac{3}{4p(\cdot)}$ עבור $p(\cdot)$ פולינום כלשהו (בדומה לנאותות החלשה כפי שהוגדרה לעיל).

מטרת שני הסעיפים הבאים להוכיח כי $PCP(poly(n),poly(n)) \subseteq MIP[2,poly(n),poly(n)]$ (ובכך להוכיח למעשה את שקילותם). בפרט, בהנתן מוודא PCP עבור L נרצה לתאר מערכת הוכחה מרובת מוכיחים עבור L. לשם כך מוצעת מערכת הוכחה בה המוודא מתנהג באופן זהה למוודא PCP הנתון ובה מוכיח יחיד ש"מחליף" את סרט ההוכחה.

ב. (5 נק') ציינו בקצרה מהי הבעייתיות במערכת המוצעת.

ג. (15 נק') הוסיפו למערכת המוצעת מוכיח נוסף ושאלה **אחת** של המוודא אליו כך שיתקיימו דרישות השלמות המלאה והנאותות (החלשה). הוכיחו שהדרישות אכן מתקיימות! הסיקו כי $PCP(poly(n),poly(n)) \subseteq MIP[2,poly(n),poly(n)]$.

בהצלחה!