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

הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב
חיפה 32000

ז' בסיון, התשס"ח 10 ביוני 2008

תורת הסיבוכיות (236313)

מבחן סיום מועד ב'

סמסטר חורף התשס"ח

מרצה: פרופ' איל קושלביץ.

מתרגל: אילן גרונאו.

הנחיות:

1. **הבחינה עם חומר סגור.**
2. **בבחינה 3 שאלות. יש לענות על כולן.**
3. **נמקו את כל תשובותיכם. ניתן להסתמך על כל טענה שהוכחה בהרצאה או בתרגול בתנאי שמצטטים אותה במדויק.**
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 (20 נק')

בשאלה זו נתייחס למחלקה BPL המוגדרת כדלהלן:

$L \in \mathrm{BPL}$ אם קיימת מ"ט מטילת מטבעות M העובדת בזיכרון לוגריתמי ובזמן פולינומי כך ש:

- $x \in L \;\Rightarrow\; \Pr\left[M(x)=1\right] \geq \frac{2}{3}$.
- $x \notin L \;\Rightarrow\; \Pr\left[M(x)=1\right] \leq \frac{1}{3}$.

א. (10 נק') הוכיחו כי $\mathrm{BPL} \subseteq \mathrm{P}$.

ב. (10 נק') הוכיחו כי $\mathrm{BPL} \subseteq \mathrm{DSPACE}(\log^2(n))$

שימו לב: יתכן ובסעיף זה תתארו אלגוריתם המשתמש במספרים ממשיים. ייצוג מספרים כאלה בזיכרון מוגבל עשוי להכניס שגיאה לחישוב. במידה וזה המצב, עשוי להיות נוח יותר לנתח את האלגוריתם בהתעלם מהשגיאה הנ"ל ורק אחר-כך לנתח אותה.

שאלה 2 (45 נק')

תזכורת: פרוטוקול MA מוגדר באופן הבא:

1. המוכיח (Merlin) והמוודא (Arthur) מקבלים שניהם את הקלט x.
2. המוכיח שולח הודעה y למוודא.
3. המוודא מחליט על סמך x,y באופן הסתברותי ובזמן פולינומי (ב-$|x|$) אם לקבל או לדחות את x.

המחלקה MA היא מחלקת השפות הניתנות לחישוב ע"י פרוטוקול כנ"ל, כאשר פרוטוקול MA מחשב שפה L אם מתקיימים תנאי השלמות והנאותות הבאים:

- Completeness: $x \in L \Rightarrow \quad \Pr\left[\mathrm{MA}(x) = accept\right] \geq 3/4$.
- Soundness: $x \notin L \Rightarrow \forall \mathrm{M'}: \Pr\left[\mathrm{M'A}(x) = accept\right] \leq 1/4$.

א. (15 נק') הוכיחו כי $\mathrm{MA} \subseteq \Sigma_2^{\mathrm{P}}$.

ב. (5 נק') פרופסור X טוען שהמחלקה MA סגורה למשלים מהטיעון הבא: "נהפוך את מצבי הקבלה והדחייה בפרוטוקול MA עבור שפה כלשהי $L \in \mathrm{MA}$, ונקבל פרוטוקול MA עבור $\overline{L}$".

- הסבירו מדוע טיעון זה אינו נכון.

ג. (15 נק') הוכיחו כי אם $\mathrm{PSPACE} \subseteq \mathrm{P/poly}$ אז $\mathrm{PSPACE} = \mathrm{MA}$.

רמז: שימו לב שהמוכיח בפרוטוקול ההוכחה האינטראקטיבית עבור TQBF משתמש בזיכרון חסום פולינומית.

ד. (10 נק') הסיקו מכך שאם $\mathrm{PSPACE} \subseteq \mathrm{P/poly}$ אז ההיררכיה הפולינומית קורסת.

שאלה 3 (35 נק')

בשאלה זו נתייחס למערכות הוכחה אינטראקטיביות הזהות במאפייניהן למערכות המקוריות שהוגדרו בכיתה, פרט לכך שהמוודא הוא מ"ט מטילת מטבעות עם גישה לאוב עבור השפה SAT. לפרוטוקול הוכחה כזה נקרא פרוטוקול עם אוב ל-SAT.

בפרט נתייחס למחלקה $\mathrm{IP}_{priv}^{\mathrm{SAT}}$ שהיא מחלקת השפות הניתנות לחישוב ע"י פרוטוקול הוכחה עם אוב ל-SAT המשתמש במטבעות פרטיים, ולמחלקה $\mathrm{IP}_{pub}^{\mathrm{SAT}}$ שהיא מחלקת השפות הניתנות לחישוב ע"י פרוטוקול הוכחה עם אוב ל-SAT המשתמש במטבעות ציבוריים.

א. (15 נק') תארו במפורש פרוצדורה ההופכת פרוטוקול הוכחה עם אוב ל-SAT המשתמש במטבעות ציבוריים לפרוטוקול הוכחה IP רגיל (בו למוודא אין גישה לאוב) המשתמש במטבעות ציבוריים.

ב. (5 נק') הסבירו בקצרה מדוע הבניה של הסעיף הקודם לא עובדת עבור פרוטוקולים עם מטבעות פרטיים.

ג. (15 נק') הראו ש $\mathrm{IP}_{priv}^{\mathrm{SAT}} = \mathrm{IP}$.