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

הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב
חיפה 32000

י' באייר, התשס"ח

15 במאי 2008

תורת הסיבוכיות (236313)

מבחן סיום מועד א'

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!

<u>שאלה 1 (30 נק')</u>

בשאלה זו נתייחס למחלקה BPL המוגדרת כדלהלן:

$L\in\text{BPL}$ אם קיימת מ"ט מטילת מטבעות M העובדת <u>בזיכרון לוגריתמי</u> <u>ובזמן פולינומי</u> כך ש:

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

המחלקה $\exists\text{BPL}$ היא אוסף השפות L כך שקיים יחס דו-מקומי $A_L\in\text{BPL}$ ופולינום $p(\cdot)$ המקיימים:

$$x\in L \quad\Leftrightarrow\quad \exists y:\left(|y|\leq p(|x|) \;\wedge\; (x,y)\in A_L\right)$$

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

ב. (8 נק') לאיזו מחלקה מוכרת שווה $\exists\text{BPL}$? הוכיחו את תשובתכם.

ג. (12 נק') הוכיחו כי $\text{BPL}\subseteq\text{DSPACE}(\log^2(n))$

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.

<u>שאלה 2 (30 נק')</u>

בשאלה זו נוכיח את משפט Karp-Lipton הטוען כי אם NP⊆P/poly אז ההיררכיה הפולינומית קורסת.

תזכורת: השפה $\forall\mathrm{QSAT}_2$ היא שפה Π_2^{P}-שלמה, כאשר $\psi \in \forall\mathrm{QSAT}_2$ אם

$$\left(\psi = \forall\overline{x} \in \{0,1\}^m \quad \exists\overline{y} \in \{0,1\}^m \;\; \varphi(\overline{x},\overline{y})\right) \quad \wedge \quad \left(\varphi \in \mathrm{CNF}\right) \quad \wedge \quad \left(\psi \equiv \mathrm{TRUE}\right)$$

א. (12 נק') הוכיחו כי אם NP⊆P/poly אז קיימת סדרה פולינומית של מעגלים המחשבת לכל $\varphi\in$SAT השמה x שמספקת את φ.

הערה: עבור $\varphi\notin$SAT, הפלט של המעגל יכול להיות כלשהו.

ב. (12 נק') הוכיחו כי אם NP⊆P/poly אז $\forall\mathrm{QSAT}_2 \in \Sigma_2^{\mathrm{P}}$.

רמז: התבוננו בשפה:

$$L = \left\{ (\psi, C, \overline{u}) \;\middle|\; \begin{array}{l} \left(\psi = \forall\overline{x} \in \{0,1\}^m \;\; \exists\overline{y} \in \{0,1\}^m \;\; \varphi(\overline{x},\overline{y})\right) \;\wedge\; \left(\varphi \in \mathrm{CNF}\right) \\ \wedge \;\; \left(C \text{ is an } m\text{-output circuit}\right) \;\wedge\; \left(\overline{u} \in \{0,1\}^m\right) \\ \wedge \;\; \left(\varphi(\overline{u}, C(\varphi|_{\overline{x}\leftarrow\overline{u}})) = \mathrm{TRUE}\right) \end{array} \right\},$$

כאשר $\varphi|_{\overline{x}\leftarrow\overline{u}}$ הינה הנוסחא המתקבלת מ-φ ע"י הצבת ערכי $\overline{u}$ במשתנים של $\overline{x}$.

ג. (6 נק') הוכיחו כי אם NP⊆P/poly אז ההיררכיה הפולינומית קורסת.

שאלה 3 (40 נק')

בשאלה זו נראה כי אם P=NP אזי ניתן לקרב כל פונקציה ב-#P.

הערה: לא ידוע אם P=NP גורר שניתן לחשב כל פונקציה ב-#P <u>במדויק</u>.

תזכורות:

- **#SAT:** הפונקציה #SAT סופרת לכל נוסחת CNF φ את מספר ההשמות המספקות שלה.
- **פונקציות hash:** תהי $\mathcal{H}_{n,k}$ קבוצת המטריצות הבינאריות בגודל nxk. אז לכל זוג $x_1 \neq x_2 \in \{0,1\}^n$ השונים שניהם מ-0^n מתקיים $\Pr_{h\in\mathcal{H}_{n,k}}\left[h\cdot x_1 = h\cdot x_2 = 0^k\right] = 2^{-2k}$.

א. (10 נק') תארו רדוקציה אקראית f מ-#SAT ל-SAT הניתנת לחישוב בזמן פולינומי, ומקיימת:

$$\#\mathrm{SAT}(\varphi) \geq 8K \quad \Rightarrow \quad \Pr\left[f(\varphi,K)\in \mathrm{SAT}\right] \geq a$$

$$\#\mathrm{SAT}(\varphi) \leq K \quad \Rightarrow \quad \Pr\left[f(\varphi,K)\in \mathrm{SAT}\right] \leq b$$

(כאשר a,b קבועים כלשהם בתחום $[0,1]$, ומתקיים $b<a$)

ב. (10 נק') תחת ההנחה ש P=NP, תארו אלגוריתם אקראי ופולינומי A המקיים עבור קבוע כלשהו $c>1$:

$$\Pr\left[\frac{1}{c} \leq \frac{\mathrm{A}(x)}{\#\mathrm{SAT}(x)} \leq c\right] > 1-2^{-n}$$

ג. (12 נק') הראו שאם P=NP אז קיים אלגוריתם פולינומי <u>דטרמיניסטי</u> המקרב את #SAT (עד כדי קבוע כפלי כלשהו $c'>1$).

רמז: היזכרו בהוכחת המשפט $\mathrm{BPP}\subseteq\Sigma_2^{\mathrm{P}}$ שהוצגה בכיתה (בפרט, בלמה המרכזית שבהוכחה, הנותנת אפיון לשפות ב-BPP ע"י כמתים) .

ד. (8 נק') הוכיחו כי אם ל-#SAT ישנו אלגוריתם קרוב פולינומי ודטרמיניסטי, אז לכל פונקציה ב-#P ישנו אלגוריתם קרוב פולינומי ודטרמיניסטי.