מבחן במודלים חישוביים + פתרון מוצע

סמסטר ב' התשס"ט, מועד ב'

תאריך: 1.9.2009

מרצים: ד"ר מירי פרייזלר, פרופ' בני שור

מתרגלים: יהונתן ברנט, רני הוד

מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.

- משך הבחינה שעתיים ו־45 דקות.
- חומר עזר מותר: שני דפי A4, כתובים משני הצדדים.
- בראש כל עמוד בטופס המבחן יש למלא מספר ת"ז ומספר מחברת; בטופס התשובות יש למלא מספר ת"ז, **מספר גירסא** ומספר מחברת.
- במבחן שני חלקים. בחלק הראשון שתי שאלות פתוחות (30 נק' כל אחת) ובחלק השני 8 שאלות סגורות (5 נק' כל אחת). כדי לקבל ציון 100 בבחינה יש לענות נכונה על כל השאלות.
  - תשובות לשאלות הסגורות יש לסמן במקום המתאים לכך <u>בטופס התשובות</u>. בכל שאלה יש לסמן תשובה יחידה.
  - על התשובה לכל שאלה פתוחה להופיע במסגרת המתאימה <u>בטופס המבחן</u> (טופס זה). יש לענות תשובות ברורות ותמציתיות. תשובות מסורבלות או לא ניתנות פיזית לקריאה יזכו לניקוד חלקי בלבד.
  - ודא/י היטב את תשובתך לפני כתיבתה בטופס המבחן. בסוף הטופס מצורפת מסגרת לשימוש במקרי "חירום".
  - מחברת הבחינה משמשת כטיוטא בלבד ולא תיבדק, אך יש להגישה עם המבחן.
- על סעיף של שאלה פתוחה ניתן לענות *"אינני יודע/ת"* כתשובה; על סעיף זה יינתנו 20% מהנקודות. במקרה זה <u>אין</u> להוסיף שום הסבר.
- מותר להשתמש בכל טענה שהוכחה בכיתה (בהרצאה, בתירגול או בתרגיל הבית) בתנאי שמצטטים אותה באופן מדויק. טענות שהוכחו במקום אחר (כגון: בספר הלימוד, בויקיפדיה, ב־MIT, בסמסטר קודם) יש להוכיח מחדש.
- אלא אם נאמר אחרת במפורש, כל המספרים המופיעים בשאלות הם שלמים, אי־שליליים ונתונים בייצוג בינארי.
- בשאלות בהן יש לתאר מכונת טיורינג ניתן להסתפק בתיאור מילולי *משכנע* של אופן פעולת המכונה. אין צורך להגדיר במדויק את פונקצית המעברים δ אלא אם השאלה מבקשת זאת במפורש.
- בכל השאלות ניתן להניח כי $\mathcal{NP} \neq \mathcal{P}$ ו־co-$\mathcal{NP} \neq \mathcal{NP}$ אלא אם השאלה מציינת אחרת.

בהצלחה!

א1		ב1		ג1	
א2		ב2		ג2	

חלק I

שאלה 1

נתונה שפה $L \subseteq \Sigma^*$.

סעיף א' (10 נק')

הוכח/הוכיחי כי אם $L \in \mathcal{R}$ ו־$L \neq \varnothing, \Sigma^*$ אזי $\bar{L} \leq_m L$.

הוכחה:

$L \neq \varnothing, \Sigma^*$ ולכן קיימים $y \in L$ ו־$n \notin L$. $L \in \mathcal{R}$ ולכן גם $\bar{L} \in \mathcal{R}$ ויש מ"ט M המכריעה את $\bar{L}$.
נראה $\bar{L} \leq_m L$ ע"י רדוקצית המיפוי הבאה.
עבור קלט x נריץ את M כדי לבדוק אם הוא ב־$\bar{L}$; אם כן, נחזיר את y ואחרת נחזיר את n.
קל לראות שהרדוקציה חשיבה ונכונה.

סעיף ב' (10 נק')

הוכח/הוכיחי כי אם $L \notin \mathcal{R}$ ו־$\bar{L} \leq_m L$ אזי $L \notin \mathcal{RE} \cup \text{co-}\mathcal{RE}$.

הוכחה:

נניח כי $L \in \mathcal{RE}$ (ההוכחה עבור המקרה $L \in \text{co-}\mathcal{RE}$ היא סימטרית) ולכן $\bar{L} \in \text{co-}\mathcal{RE}$.
מהנתון $\bar{L} \leq_m L$ נובע כי $\bar{L} \in \mathcal{RE}$ כלומר $L \in \text{co-}\mathcal{RE}$.
בסה"כ קיבלנו $L \in \mathcal{RE} \cap \text{co-}\mathcal{RE} = \mathcal{R}$ בסתירה לנתון.

סעיף ג' (10 נק')

תהיה שפה $A \in \mathcal{RE} \setminus \mathcal{R}$ **מעל** $\Sigma = \{0,1\}$ **ונגדיר** $B = \{0w : w \in A\} \cup \{1w : w \notin A\}$.
הוכח/הוכיחי $B \notin \mathcal{RE} \cup \text{co-}\mathcal{RE}$ **בהסתמך על סעיף ב' לעיל (גם אם לא פתרת אותו).**
<u>הערה</u>: **הוכחות שלא ישתמשו בסעיף ב' יזכו בניקוד חלקי (5 נק' לכל היותר).**

הוכחה:

ראשית נוכיח כי $A \leq_m B$ **(ולכן** $B \notin \mathcal{R}$**) ע"י רדוקצית המיפוי** $f(w) = 0w$.
זו כמובן חשיבה ומהגדרת B **מקיימת** $w \in A \Leftrightarrow f(w) \in B$.

כעת נבחר מילה כלשהי $z \in A$ **(יש כזו כי** A **לא ריקה) ונוכיח** $\bar{B} \leq_m B$ **ע"י רדוקצית המיפוי**

$$g(x) = \begin{cases} 0z, & x = \epsilon \\ 0w, & x = 1w \\ 1w, & x = 0w \end{cases}$$

זו רדוקציה חשיבה וקל לראות כי $x \notin B \Leftrightarrow g(x) \in B$. **נפעיל את סעיף ב' והדרוש נובע.**

שאלה 2

עבור נוסחת CNF או DNF בוליאנית ϕ והצבה v למשתניה נגדיר את $N(\phi, v)$ כמספר הפסוקיות (clauses) המסופקות ע"י הצבה זו.

<u>תזכורת</u>: נוסחת CNF היא AND של פסוקיות וכל פסוקית היא OR של ליטרלים; נוסחת DNF היא OR של פסוקיות וכל פסוקית היא AND של ליטרלים.

נגדיר את השפות הבאות (שימו לב שהמספר הטבעי k נתון בייצוג בינארי):

$$\text{Count-CNF} = \{\langle \phi, k \rangle : \phi \text{ is a CNF formula and there exists } v \text{ such that } N(\phi, v) = k\}$$
$$\text{Count-DNF} = \{\langle \phi, k \rangle : \phi \text{ is a DNF formula and there exists } v \text{ such that } N(\phi, v) = k\}$$

סעיף א' (10 נק')

הוכח/הוכיחי כי $\text{Count-CNF} \leq_p \text{3-Sat}$. האם מכך נובע כי Count-CNF היא $\mathcal{NP}$-שלמה?

הוכחה:

כשההצבה v נתונה, ניתן לחשב את $N(\phi, v)$ בזמן פולינומי ולהשוות ל-k. זהו מוודא פולינומי ומכאן ש-$\text{Count-CNF} \in \mathcal{NP}$ וע"פ משפט Cook מתקיים $\text{Count-CNF} \leq_p \text{3-Sat}$.

לא הוכחנו (עדיין) ש-Count-CNF בעיה $\mathcal{NP}$-קשה ולכן לא נובע שהיא ב-$\mathcal{NPC}$. ייתכן, למשל, שהיא ב-$\mathcal{P}$ או שהיא ב-$\mathcal{P} \setminus (\mathcal{NP} \cap \text{co-}\mathcal{NP})$.

סעיף ב' (10 נק')

הוכח/הוכיחי כי $\text{3-SAT} \leq_p \text{COUNT-CNF}$.

הוכחה:

נראה זאת ע"י הרדוקציה הבאה. בהנתן נוסחת 3-CNF ϕ, **הרדוקציה תספור כמה פסוקיות בה** $m = |\phi|$ **ותחזיר את הזוג** $\langle \phi, m \rangle$. **נשים לב ש־**ϕ**נוסחת** CNF **כדרוש. ברור שהרדוקציה פועלת בזמן פולינומי. כמו כן, לפי הגדרה** ϕ **ספיקה אמ"מ קיימת השמה המספקת בדיוק** m **פסוקיות בה.**

כעת, אגב, נובע ש־$\text{COUNT-CNF} \in \mathcal{NPC}$.

סעיף ג' (10 נק')

הוכח/הוכיחי כי $\text{COUNT-CNF} \leq_p \text{COUNT-DNF}$.

הוכחה:

נראה זאת ע"י הרדוקציה הבאה. בהנתן נוסחת CNF ϕ **ומספר** k **נבנה נוסחת** DNF $\bar{\phi}$ **ומספר** $\bar{k}$ **כך: לכל פסוקית** $C = x_1 \vee \cdots \vee x_r$ **של** ϕ**,** $\bar{\phi}$ **תכיל את הפסוקית** $\bar{C} = \bar{x}_1 \wedge \cdots \wedge \bar{x}_r$. **הפסוקיות יחוברו כמובן ע"י** OR. **נבחר** $\bar{k} = |\phi| - k$.
הבניה פולינומית. קל לראות מכללי דה־מורגן שהשמה v **כלשהי מספקת פסוקית** C **של** ϕ **אמ"מ היא לא מספקת את הפסוקית** $\bar{C}$ **המקבילה ב־**$\bar{\phi}$ **ועל כן קיימת השמה המספקת בדיוק** k **פסוקיות של** ϕ **אמ"מ קיימת (אותה) השמה המספקת בדיוק** $\bar{k}$ **פסוקיות של** $\bar{\phi}$.

חלק II

1. תהי u פונקציה המוגדרת באופן הבא: הקלט הוא שלשה $\left(\langle M\rangle, x, 1^k\right)$ כאשר $\langle M\rangle$ הוא קידוד של מ"ט דטרמיניסטית חד־סרטית בעלת א"ב קלט $\Sigma = \{0,1\}$ וא"ב מכונה $\Gamma = \{0,1,2,\$,\sqcup\}$, $x \in \Sigma^*$ היא מילה ו־1^k הוא קידוד אונארי של המספר הטבעי $k \in \mathbb{N}$. הפלט של u הוא 1 אם M מקבלת את x תוך לכל היותר k צעדים ו־0 אחרת. איזו מהאפשרויות הבאות מתקיימת?

(א) הפונקציה u אינה ניתנת לחישוב.

(ב) הפונקציה u ניתנת לחישוב בזמן פולינומיאלי.

(ג) הפונקציה u ניתנת לחישוב אך לא בזמן פולינומיאלי.

(ד) התשובות א'-ג' לעיל אינן נכונות.

- ניתן לסמלץ את ריצת M על x למשך k צעדים בזמן $O\left(|M| \cdot k\right)$ וכך לבדוק אם x התקבל. המספר k נתון בייצוג אונארי ולכן זה פולינומיאלי ב־$\left|\left(\langle M\rangle, x, 1^k\right)\right|$.

2. עבור שפה $L \subseteq \Sigma^*$ נגדיר $sub\left(L\right) = \{y \in \Sigma^* : \exists x,z \in \Sigma^* \quad xyz \in L\}$. במילים אחרות, $sub\left(L\right)$ מכילה את כל תת־המחרוזות הרצופות של מילות L. איזו מהאפשרויות הבאות מתקיימת?

(א) אם השפה L רגולרית אזי גם $sub\left(L\right)$ רגולרית; כמו כן, אם $L \in \mathcal{RE}$ אזי גם $sub\left(L\right) \in \mathcal{RE}$.

(ב) אם השפה L רגולרית אזי גם $sub\left(L\right)$ רגולרית; לעומת זאת, קיימת שפה $L \in \mathcal{RE}$ עבורה $sub\left(L\right) \notin \mathcal{RE}$.

(ג) יש שפה L רגולרית עבורה $sub\left(L\right)$ אינה רגולרית; לעומת זאת, אם $L \in \mathcal{RE}$ אזי גם $sub\left(L\right) \in \mathcal{RE}$.

(ד) יש שפה L רגולרית עבורה $sub\left(L\right)$ אינה רגולרית; כמו כן, קיימת שפה $L \in \mathcal{RE}$ עבורה $sub\left(L\right) \notin \mathcal{RE}$.

- בהנתן DFA המקבל את L, קל לבנות NFA המקבל את $sub\left(L\right)$ – מנחשים רישא x וסיפא z ומריצים את ה־DFA על xyz (בדומה לשאלה 7 בתרגיל בית 2).
- בהנתן מ"ט M שמקבלת את L, אפשר לבנות מ"ט המקבלת את $sub\left(L\right)$ ופועלת כדקלמן. עוברים בסדר לקסיקוגרפי על כל האפשרויות ל־$\langle x,z,k\rangle \in \Sigma^* \times \Sigma^* \times \mathbb{N}$ ומריצים את M למשך k צעדים על xyz; אם M קיבלה אז מקבלים ואחרת עוברים לאפשרות הבאה.

3. נתונה שפה $L \subseteq \Sigma^*$ ונתון אלגוריתם (enumerator) המדפיס את רשימת כל המילים בשפה L (כל מילה בשפה מודפסת בדיוק פעם אחת).[1] נתון שלכל שתי מילים בשפה $x, y \in L$ עבורן $|x| < |y|$, המילה x מודפסת אחרי המילה y (אבל לאו דוקא מיד אחריה). מה ניתן לומר אודות L?

(א) השפה L היא תמיד רגולרית.

(ב) השפה L היא תמיד חסרת הקשר ולעיתים אינה רגולרית.

(ג) השפה L היא תמיד כריעה ולעיתים אינה חסרת הקשר.

(ד) לעיתים השפה L אינה כריעה.

- אם $L = \varnothing$ סיימנו. אחרת, תהיה x_0 המילה הראשונה שמדפיס האלגוריתם ונסמן $n = |x_0|$. מהנתון נובע שכל המילים בשפה L אורכן לכל היותר n ועל כן L שפה סופית ובפרט רגולרית.

4. נגדיר $L = \{\langle M\rangle : M \text{ is a TM, } L(M) \text{ is finite and } |L(M)| \text{ is a multiple of } 7\}$. איזו מהאפשרויות הבאות מתקיימת?

(א) $L \in \mathcal{R}$.

(ב) $L \in \mathcal{RE} \setminus \mathcal{R}$.

(ג) $L \in \text{co-}\mathcal{RE} \setminus \mathcal{R}$.

(ד) $L \notin \mathcal{RE} \cup \text{co-}\mathcal{RE}$.

- ראינו בשיעור ו/או בתרגול שהשפה $L_{fin} = \{\langle M\rangle : M \text{ is a TM, } L(M) \text{ is finite}\}$ מקיימת $L_{fin} \notin \mathcal{RE} \cup \text{co-}\mathcal{RE}$ ולכן די להראות $L_{fin} \leq_m L$. בהנתן מ"ט M מעל הא"ב Σ, הרדוקציה תבנה מכונה M' מעל הא"ב $\Sigma \times \{1, 2, \ldots, 7\}$ כך שהרצת M' על $\langle x, i\rangle$ מסמלצת ריצת M על x ומחזירה אותה תוצאה. כעת מתקיים $L(M') = L(M) \times \{1, 2, \ldots, 7\}$ והדרוש נובע.

5. נתונות שלוש השפות הבאות מעל הא"ב $\Sigma = \{a, b\}$:

$$\begin{aligned} L_1 &= \left\{(ab)^k a (ba)^k : k \in \mathbb{N}\right\}, \\ L_2 &= \left\{(ab)^k b (ba)^k : k \in \mathbb{N}\right\}, \\ L_3 &= \left\{(ab)^k (ba)^k (ab)^k : k \in \mathbb{N}\right\}. \end{aligned}$$

איזו מהאפשרויות הבאות מתקיימת?

(א) כל השפות הן חסרות הקשר ואינן רגולריות.

(ב) שתיים מהשפות הן חסרות הקשר ואינן רגולריות והשפה הנותרת אינה חסרת הקשר.

(ג) אחת מהשפות היא רגולרית, אחת חסרת הקשר ואינה רגולרית והשפה הנותרת אינה ח"ה.

(ד) שתיים מהשפות הן רגולריות ואחת חסרת הקשר ואינה רגולרית.

- $L_1 = \left\{(ab)^{2k} a : k \in \mathbb{N}\right\}$ רגולרית; L_2 חסרת הקשר (דקדוק: $S \to abSba|b$) אך אינה רגולרית (ניפוח); L_3 אינה חסרת הקשר (ניפוח עבור ח"ה).

[1] האלגוריתם אינו מקבל קלט ואינו חייב לעצור. במהלך פעולתו הוא מדפיס מילים המופרדות זו מזו ע"י סימן רווח. מילים שאינן בשפה לא מודפסות.

6. נאמר שנוסחא בוליאנית ϕ היא טאוטולוגיה אם כל השמה בוליאנית למשתני ϕ תתן ערך אמת. תהי $T = \{\phi : \phi \text{ is a CNF formula and } \phi \text{ is a tautology}\}$. מהי מחלקת הסיבוכיות הקטנה ביותר (ביחס להכלה) אליה שייכת T?

   (א) $\mathcal{P}$.

   (ב) $\mathcal{NP} \cap \text{co-}\mathcal{NP}$.

   (ג) $\mathcal{NPC}$.

   (ד) $\text{co-}\mathcal{NPC}$.

- די שפסוקית אחת בנוסחת CNF לא תסתפק כדי שהנוסחא כולה לא תסתפק. נבדוק, אם כן, כל פסוקית של ϕ בנפרד. אם הפסוקית מכילה משתנה ושלילתו, כל השמה מספקת אותה ונעבור לפסוקית הבאה; אחרת, יש השמה שלא מספקת פסוקית זו וניתן לקבוע ש־ϕ אינה טאוטולוגיה. רק אם כל הפסוקיות מכילות משתנה ושלילתו אזי ϕ טאוטולוגיה.

7. נניח כי $\mathcal{P} = \mathcal{NP}$. איזו מהאפשרויות הבאות מתקיימת?

   (א) $\mathcal{P} \subsetneq \mathcal{NPC}$.

   (ב) $\mathcal{P} = \mathcal{NPC}$.

   (ג) $\mathcal{P} \supsetneq \mathcal{NPC}$.

   (ד) התשובות א'-ג' לעיל אינן נכונות.

- קל לראות כי $\mathcal{P} \subsetneq \mathcal{P}\text{-complete} = \mathcal{P} \setminus \{\varnothing, \Sigma^*\}$.

8. תהי $\mathcal{C}$ מחלקת שפות כלשהי ותהיינה A, B שפות. ידוע ש־$B \in \mathcal{C}$ וכן שיש רדוקצית מיפוי מ־A ל־B. באיזה מהמקרים הבאים <u>לא בהכרח</u> מתקיים $A \in \mathcal{C}$?

   (א) $\mathcal{C} = \mathcal{RE} \cap \text{co-}\mathcal{RE}$ והרדוקציה היא חשיבה.

   (ב) $\mathcal{C} = \mathcal{RE} \cap \text{co-}\mathcal{RE}$ והרדוקציה היא חשיבה בזמן פולינומי.

   (ג) $\mathcal{C} = \mathcal{RE} \setminus \mathcal{R}$ והרדוקציה היא חשיבה בזמן פולינומי.

   (ד) $\mathcal{C} = \mathcal{P}$ והרדוקציה היא חשיבה בזמן פולינומי.

- ניקח $A \in \mathcal{P} \subset \mathcal{R}$ ו־$B = H_{TM}$. מתקיים $A \leq_p B$ כי ניתן לפתור את A תוך כדי הרדוקציה ולהחזיר אחד מבין שני פלטים קבועים (מכונה שתמיד עוצרת/לעולם לא עוצרת וקלט ϵ עבורה).