# תורת הסיבוכיות (236313)

מועד א׳

20.02.18

מרצה: פרופ׳ איל קושילביץ
מתרגלת: מיכל כהן

**הנחיות**

- המבחן הוא עם חומר סגור.
- חל איסור מפורש על החזקת אמצעי תקשורת נייד, דוגמת טלפון סלולרי ברשות הנבחן בעת בחינה.
- נמקו את כל תשובותיכם.
- בכל סעיף ניתן לקבל $20\%$ מהניקוד אם במקום תשובה כותבים ״לא יודע/ת״.
- מותר להשתמש בכל טענה שהוכחה בהרצאה או בתרגול, בתנאי שמצטטים אותה באופן מדויק.
- השתדלו לא להתעכב יתר על המידה בסעיף מסויים, כדי לצבור מקסימום נקודות בזמן העומד לרשותכם.

**בהצלחה!**

## שאלה 1 (שאלת ש"ב, 15 נקודות)

נגדיר: $\mathrm{BP}\cdot\mathrm{NP}=\left\{L|L\leq_R^{BPP}3\mathrm{SAT}\right\}$ כאשר $L_1\leq_R^{BPP}L_2$ אם קיימת $M$ פולינומית הסתברותית ופולינום $p(n)$ כך שלכל $x$ מתקיים

$$\Pr\left[x\in L_1\iff M(x)\in L_2\right]\geq\frac{1}{2}+\frac{1}{p(|x|)}.$$

הגדרה: MA היא מחלקת כל השפות עבורה קיימת מערכת הוכחה אינטראקטיבית $(V,P)$ המקיימת:

- $V$ הוא מוודא פולינומי הסתברותי
- $P$ הוא מוכיח בעל משאבים לא מוגבלים
- לכל $x\in L$ מתקיים שבאינטראקציה עם $P$, $V$ מקבל בהסתברות של לכל הפחות $2/3$.
- לכל $x\notin L$ ולכל $P^*$ מתקיים שבאינטראקציה עם $P^*$, $V$ מקבל בהסתברות של לכל היותר $1/3$.
- בהינתן הקלט $x$, המוכיח שולח רק הודעה אחת למוודא, שלאחר מכן מחליט האם לקבל או לדחות. המוודא לא שולח הודעות למוכיח.

1. (8 נקודות) הוכיחו כי $\mathrm{AM}[2]=\mathrm{BP}\cdot\mathrm{NP}$.
2. (7 נקודות) הוכיחו כי $\mathrm{MA}\subseteq\Sigma_2^p$.

## שאלה 2 (15 נקודות)

נגדיר את הפונקציה הבאה: $\#2SAT(\varphi)$ מחזירה את כמות ההשמות המספקות עבור פסוק $\varphi$ מהצורה $2CNF$ (כלומר, פסוק $CNF$ שכל פסוקית שלו מכילה בדיוק שני ליטרלים).

1. (3 נקודות) הוכיחו כי $\#2SAT\in\#P$.
2. (12 נקודות) הוכיחו כי $\#2SAT$ היא $\#P$ קשה.
ניתן להניח כי הפונקציה $M(G)$ המקבלת גרף ומחזירה את מספר השידוכים ב-$G$ היא $\#P$ שלמה.

## שאלה 3 (15 נקודות)

נגדיר את השפה $BPG$ להיות שפת כל הגרפים הדו צדדיים. הוכיחו ש-$BPG\in NL$.

## שאלה 4 (30 נקודות)

נגדיר את $US$ כמחלקת כל השפות שקיימת עבורן מ"ט א"ד פולי' $M$ כך ש-$x\in L$ אם"ם קיים בדיוק מסלול מקבל אחד ל-$M$ על $x$.

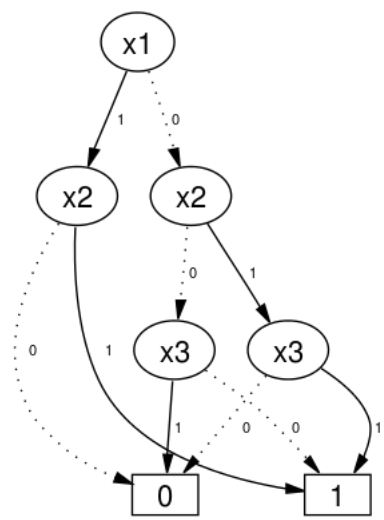
1. (2 נקודות) תזכורת: ראינו בתרגול את השפה $UniqSAT=\{\varphi|\exists!x:\varphi(x)=T\}$. הוכיחו כי $UniqSAT\in US$.
2. (5 נקודות) הוכיחו כי $UniqSAT$ היא $US$ קשה ביחס לרדוקציות העתקה פולינומית.
3. (5 נקודות) הוכיחו או הפריכו: תהא $M^A$ מכונת $US$ עם אוב לשפה $A\in US$. תהא $M_2$ מכונת $US$ עבור $A$. נבנה מכונת $US$, $M'$, באופן הבא: $M'$ פועלת כמו $M^A$, ובכל פעם שבה $M^A$ פונה לאוב $A$, $M'$ מסמלצת את $M_2$. מתקיים כי $L(M')=L\left(M^A\right)$.
4. (8 נקודות) הוכיחו כי $coNP\subseteq US$.
5. (5 נקודות) הוכיחו כי $P^{\Sigma_1^p}\subseteq P^{US}\subseteq P^{\Sigma_2^p}$.
6. (5 נקודות) הוכיחו כי $P^{US}=P^{NP}$.

## שאלה 5 (25 נקודות)

דיאגרמת החלטה בינארית ($BDD$) מוגדרת כמו עץ החלטה, למעט שגרף התשתית שלה הוא $DAG$ שאינו בהכרח עץ.
באופן פורמלי, $BDD$ הוא מודל חישוב הדומה לתכניות מתפצלות שבו $G$ הוא $DAG$ מושרש ב־$r$ בו לכל צומת דרגת יציאה 2. הצמתים הפנימיים מסומנים ע"י משתנים ואילו העלים מסומנים ע"י קבועים $\{0,1\}$. כמו כן, הקשתות מסומנות ע"י קבועים $\{0,1\}$ כך שמכל צומת פנימי יוצאת קשת אחת עם הערך 1 וקשת אחת עם הערך 0. נאמר ש $bdd$ מקבל קלט $x$ אם"ם כשמתחילים מהשורש $r$ ומתקדמים בכל פעם לפי הערך של המשתנה $x_i$ שמופיע בצומת (אם ערכו $1$ נתקדם על הקשת שערכה $1$ ולהפך) מגיעים לעלה שערכו 1. ניתן להניח שקיים עלה אחד שמסומן ב־1 ועלה אחד שמסומן ב־0 (ראו דוגמה).
נאמר שפונקציה $f:\{0,1\}^*\rightarrow\{0,1\}$ מחושבת על ידי סדרת $BDD$: $\{bdd_n\}_{n\in\mathbb{N}}$ אם לכל $n\in\mathbb{N}$ ולכל $x\in\{0,1\}^n$ מתקיים כי $f(x)=1$ אם"ם $bdd_n$ מקבלת את $x$.
נאמר ששפה $L\subseteq\{0,1\}^*$ מוכרעת על ידי סדרת $BDD$: $\{bdd_n\}_{n\in\mathbb{N}}$ אם לכל $n\in\mathbb{N}$ ולכל $x\in\{0,1\}^n$ מתקיים כי $x$ שייך ל־$L$ אם"ם $bdd_n$ מקבלת את $x$. נסמן ב־$PBDD$ את אוסף השפות שמוכרעות על ידי סדרה של $BDD$ בגודל פולינומי.
הערה: ידוע כי מחלקת הפונקציות להן קיים $BDD$ שקולה למחלקת הפונקציות להן קיימת תכנית מתפצלת דטרמיניסטית.

### דוגמה ל־$BDD$

מקבל את כל המחרוזות $x\in\{0,1\}^3$ עבורם הפסוק הבא מסתפק $(\neg x_1\wedge x_1\wedge x_3)\vee(\neg x_1\wedge\neg x_2\wedge\neg x_3)\vee(x_1\wedge x_2)$.




המחלקה $P/poly$ מכילה את כל השפות, $L$, שקיימת עבורן מ"ט בעלת סיבוכיות זמן פולינומית, $M$, וסדרת עצות $\{a_n\}_{n\in\mathbb{N}}$ בגודל פולינומי כך ש־$x\in L$ אם"ם $M(x\#a_{|x|})=acc$.
המחלקה $DL/poly$ מוגדרת להיות מחלקת כל השפות שקיימת להן מכונה בעלת סיבוכיות זיכרון לוגריתמי הנעזרת בעצה באורך פולינומי. מכונות אלה מקבלות כקלט לקריאה בלבד את $x$ משורשר לעצה המתאימה לאורך של $x$: $x\#a_{|x|}$.

1. (5 נקודות) הראו פונקציה בוליאנית, $f:\{0,1\}^*\rightarrow\{0,1\}$ שסדרת עצי החלטה בינאריים שמחשבת אותה חייבת להיות בגודל אקספוננציאלי, אך קיימת לה סדרת $BDD$ בגודל $\mathcal{O}(n)$ המחשבת אותה. נמקו.
2. (15 נקודות) הוכיחו כי $DL/poly=PBDD$.
3. (5 נקודות) הוכיחו כי $P/poly^{P/poly}=P/poly$.