# תורת החישוביות – 236343 – תרגיל בית 2

## 1 אינטואיציות שגויות

בסעיפים הבאים אין צורך להוכיח את תשובתכם, אלא רק למצוא שפות/פונקציות מתאימות.

### א. פונקציות מלאות ופונקציות ניתנות לחישוב

מטרת סעיף זה להבהיר את העובדה שאין כל קשר בין היותה של פונקציה מלאה והיותה ניתנת לחישוב.

1. מצאו פונקציה $f:\Sigma^*\to\Sigma^*$ שהיא מלאה וניתנת לחישוב.
2. מצאו פונקציה $f:\Sigma^*\to\Sigma^*$ שאיננה מלאה אך היא ניתנת לחישוב.
3. מצאו פונקציה $f:\Sigma^*\to\Sigma^*$ שהיא מלאה אך איננה ניתנת לחישוב.
   **רמז:** חשבו על קשר בין שפות לפונקציות.
4. מצאו פונקציה $f:\Sigma^*\to\Sigma^*$ שאיננה מלאה וגם אינה ניתנת לחישוב.

### ב. שפות כריעות ולא כריעות ותת שפות

מטרת סעיף זה להבהיר את העובדה שאין כל קשר בין יחס ההכלה של שפות ובין השייכות או אי השייכות שלהן ל־$\mathrm{R}$.

1. מצאו שלוש שפות $L_1,L_2,L_3$ כך ש־$L_1\subseteq L_2\subseteq L_3$ וגם $L_1,L_3\in\mathrm{R}$ אך $L_2\notin\mathrm{RE}$.
2. מצאו שלוש שפות $L_1,L_2,L_3$ כך ש־$L_1\subseteq L_2\subseteq L_3$ וגם $L_1,L_3\notin\mathrm{RE}$ אך $L_2\in\mathrm{R}$.

## 2 אפיונים אלטרנטיביים של המחלקה $RE$

### א. אפיון באמצעות מנייה

כזכור, $RE$ הם ראשי תיבות של Recursively Enumerable, ובעברית "ניתן למניה רקורסיבית". בשאלה זו נבין את משמעות השם. ראשית יש לדעת כי מסיבות היסטוריות (הטרמינולוגיה שבה השתמש קורט גדל במאמר שבו הוכיח את משפטי אי השלמות שלו) המילה "רקורסיבית" משמשת בהקשר של תורת החישוביות כמילה נרדפת ל"ניתן לחישוב". מכאן ש־$RE$ מייצג שפות שניתן למנות את אבריהן באופן אלגוריתמי (**כל** שפה היא בת מניה, ולכן הדגש כאן הוא על "באופן אלגוריתמי"). כזכור, קבוצה אינסופית $L$ היא בת מניה (או ניתנת למניה) אם קיימת פונקציה מלאה ועל $f:\mathbb{N}\to L$.

1. הראו כי עבור כל שפה $L$ לא ריקה, $L\in RE$ אם ורק אם קיימת פונקציה $f:\mathbb{N}\to L$ שהיא מלאה, על **וניתנת לחישוב**.

### ב. אפיון באמצעות מוודאים

כעת נראה כיצד ניתן לתת פורמליזם בסגנון תורת החישוביות למושג המתמטי המקובל של "הוכחה", וכיצד מושג זה משתלב עם המושגים המוכרים לנו בקורס.

מוודא $V$ עבור שפה $L$ הוא מכונת טיורינג בעלת שני מצבים סופיים, $q_{acc},q_{rej}$, המקבלת זוג קלטים, $(w,\pi)$ כאשר $w\in\Sigma^*$ היא המילה ש־$V$ בודק את שייכותה ל־$L$ ו־$\pi\in\Sigma^*$ היא "הוכחה" לשייכות $w$ ל־$L$ ובה $V$ יכול להיעזר.

לכל זוג $(w,\pi)$ המוודא **חייב** לעצור. נסמן $V(w,\pi)=\mathrm{acc}$ אם המוודא עוצר במצב $q_{acc}$ על הקלט $(w,\pi)$, ונסמן $V(w,\pi)=\mathrm{rej}$ אם הוא עוצר ב־$q_{rej}$. בנוסף, על המוודא לקיים את התכונות הבאות:

1. (שלמות) אם $w\in L$ אז קיימת $\pi$ כך ש־$V(w,\pi)=\mathrm{acc}$ (עבור טענה נכונה קיימת הוכחה שאותה המוודא יכול לאשר).
2. (נאותות) אם $w\notin L$ אז לכל $\pi$ מתקיים $V(w,\pi)=\mathrm{rej}$ (עבור טענה שגויה, אי אפשר "לעבוד" על המוודא באמצעות "הוכחה" שגויה).

הראו כי עבור כל שפה $L$, $L\in RE$ אם ורק אם קיים מוודא $V$ עבור השפה $L$.

## 3 שפות ופונקציות

בהינתן שפה $L\subseteq\{0,1\}^*$ ופונקציה מלאה $f:\{0,1\}^*\to\{0,1\}^*$ נגדיר $f(L)=\{f(x):x\in L\}$. הוכח/הפרך:

1. $L\in\mathrm{R} \Leftarrow f(L)\in\mathrm{RE}$.
2. $L\in\mathrm{R}$ ו־$f$ ניתנת לחישוב $\Leftarrow f(L)\in\mathrm{R}$.
3. $L\in\mathrm{RE}$ ו־$f$ ניתנת לחישוב $\Leftarrow f(L)\in\mathrm{RE}$.

## 4 פתרון לבעיית ראשוניי פרמה?

שאלה זו מצביעה על נקודה עדינה **ומרכזית** בחלק הראשון של הקורס – המרחק שבין המשמעות האינטואיטיבית של שייכות שפה ל־$\mathrm{R}$ והמשמעות האמיתית של שייכות שכזו.

**ראשוני פרמה** הוא מספר ראשוני מהצורה $F_n=2^{2^n}+1$ עבור $n\geq 0$. פרמה ידע כי $F_n$ הוא ראשוני עבור $0\leq n\leq 4$ (המספרים המתאימים הם 3,5,17,257,65537) והעלה השערה לפיה $F_n$ הוא ראשוני לכל $n\geq 0$. אוילר הוכיח כי $F_5$ אינו ראשוני, ולמעשה עד היום טרם נתגלה ולו ראשוני פרמה אחד נוסף פרט לחמשת הראשונים. השאלה אם קיים ראשוני פרמה נוסף – ובאופן כללי יותר, האם יש אינסוף ראשוניי פרמה – היא שאלה פתוחה ידועה בתורת המספרים.

נגדיר שפה $L=\{w\in\Sigma^*|$ קיים ראשוני פרמה גדול מ־$|w|\}$.

כלומר, מילה $w$ שייכת לשפה אם ורק אם קיים ראשוני פרמה שגדול מאורכה של $w$. כך למשל כל מילה מאורך לכל היותר 65536 בבירור שייכת ל־$L$.

האם $L\in\mathrm{R}$? הוכיחו תשובתכם.

## 5 משפט אי־השלמות של גדל (שאלת העשרה שאינה בחומר)

**הבהרה: שאלה זו היא שאלת העשרה לסטודנטים המתעניינים בלוגיקה ואינה מהווה חלק מחומר הלימוד של הקורס.**

תזכורת: בהנתן קבוצת אקסיומות $\mathcal{A}$, הוכחה פורמלית לפסוק $\varphi$ היא סדרה של פסוקים שכל אחד מהם או שייך ל־$\mathcal{A}$ או נובע מקודמיו ע"י אחד ממספר כללי היסק ידועים, ו־$\varphi$ הוא הפסוק האחרון בה. בשאלה זו ניתן להשתמש בעובדה שקיימת מ"ט $M_1$ שבהנתן מחרוזת $x$ מכריעה האם $x$ מייצגת פסוק חוקי, וקיימת מ"ט $M_2$ שבהנתן פסוק $\varphi$ ופסוקים $\varphi_1,...,\varphi_k$, מכריעה האם $\varphi$ נובע מ־$\varphi_1,...,\varphi_k$ באמצעות אחד מכללי ההיסק.

- הראו שאם $\mathcal{A}$ שייכת ל־$\mathrm{R}$, אז קבוצת כל ההוכחות החוקיות שייכת ל־$\mathrm{R}$.
- הראו כי קיימת מ"ט שעל קלט $x$ מפרשת את $x$ כפסוק ובודקת האם קיימת הוכחה ל־$x$ (אם קיימת הוכחה כזו אז המכונה צריכה לעצור ולקבל, ואחרת יכולה לדחות או לא לעצור).

תזכורת: אומרים שמבנה $\mathcal{M}$ מספק פסוק $\varphi$, וכותבים $\mathcal{M}\models\varphi$, אם הפסוק $\varphi$ מתקיים ב־$\mathcal{M}$. אומרים שמבנה $\mathcal{M}$ הוא **מודל של** $\mathcal{A}$, וכותבים $\mathcal{M}\models\mathcal{A}$, אם $\mathcal{M}$ מספק את כל האקסיומות ב־$\mathcal{A}$. מנאותות נובע כי אם קיימת לפסוק $\varphi$ הוכחה מ־$\mathcal{A}$, אז לכל $\mathcal{M}$ כך ש־$\mathcal{M}\models\mathcal{A}$ מתקיים $\mathcal{M}\models\varphi$.

נניח כעת שקבוצת המספרים הטבעיים היא מודל של האקסיומות שלנו, כלומר $\mathbb{N}\models\mathcal{A}$. בנוסף, נניח שקיימת נוסחה בשני משתנים $\varphi(\langle M\rangle,x)$ כך שמתקיים: $\mathbb{N}\models\varphi(\langle M\rangle,x)$ אמ"מ המכונה $M$ עוצרת על הקלט $x$.

- הניחו בשלילה שלכל $(\langle M\rangle,x)$, קיימת הוכחה או ל־$\varphi(\langle M\rangle,x)$ או לשלילתו. הסיקו כי $HP\in\mathrm{R}$.
- השתמשו בעובדה שאם מכונה $M$ עוצרת על הקלט $x$ אז קיימת הוכחה פורמלית ל־$\varphi(\langle M\rangle,x)$ שמסתמכת על מסלול החישוב ש־$M$ עושה על $x$, והסיקו כי קיימים מכונה $M$ וקלט $x$ כך ש־$M$ אינה עוצרת על $x$ אבל לא ניתן להוכיח זאת.