תורת החישוביות – תרגול מספר 3
בעיות בלתי כריעות

מבוא

ראינו עד כה מכונות טיורינג לחישוב פונקציות, ומכונות טיורינג לזיהוי שפות. נזכיר את הגדרת הקבוצה השנייה: מכונת טיורינג לזיהוי שפות מיוחדת בכך שקבוצת המצבים הסופיים שלה היא מהצורה $F=\{q_{acc},q_{rej}\}$. בהינתן מכונה שכזו M, מגדירים שפה $L\left(M\right)$ כאוסף כל המילים שעליהם M עוצרת במצב q_{acc} (שימו לב שלמכונה יש פלט, אך אנו מתעלמים ממנו).

תהינה $L\subseteq\Sigma^{*}$ שפה ו־L מכונת טיורינג.

- אם מתקיים $L\left(M\right)=L$, אז אומרים ש־M מקבלת את L.
- אם מתקיים $L\left(M\right)=L$, ובנוסף M עוצרת **לכל** קלט, אז אומרים ש־M מכריעה את L.

ההבדל בין שתי ההגדרות הוא בכך שאם M מקבלת את L, אז עבור $w\notin L$ ייתכן ש־M כלל לא תעצור, בעוד שאם M מכריעה את L אז מובטח שלכל $w\notin L$ המכונה תעצור במצב q_{rej}. בשני המקרים אנו דורשים כי אם $w\in L$ המכונה תעצור ב־q_{acc}.

חשוב לשים לב כי קבלה של שפה מוגדרת בצורה לא סימטרית (עבור מילה $w\in L$ חייבים לעצור, ועבור מילה $w\notin L$ לא חייבים).

לדוגמה, נעיין בשתי השפות הבאות:

- $\mathrm{HP}=\{(\langle M\rangle,x)\mid$ M עוצרת על הקלט $x\}$
- $\mathrm{COMPOSITE}=\{n\in\mathbb{N}\mid$ n פריק$\}$

(נזכיר כי מספר n הוא פריק אם יש מספר טבעי x, $1<x<n$ שמחלק אותו ללא שארית.)

האם קיימת מכונת טיורינג שמקבלת את HP? התשובה היא כן: נוכל להשתמש במכונה האוניברסלית כדי לסמלץ את ריצת M על הקלט x, ואם המכונה עצרה, נקבל. הנכונות ברורה. האם מכונה זו גם מכריעה את HP? כמובן שלא, מכיוון שאם המילה לא בשפה, המכונה לעולם לא תעצור. בהמשך הקורס נראה כי אין אף מכונת טיורינג שמכריעה את השפה הנ"ל.

לעומת זאת, עבור השפה COMPOSITE קיימת מכונה שמכריעה אותה: המכונה תעבור על המספרים השלמים מ־2 עד $n-1$, ותבדוק האם הם מחלקים את n ללא שארית (ראינו בתרגול הקודם שפעולות אריתמטיות ניתן לבצע בקלות). אם מצאה מספר שמחלק, המכונה תקבל, ואם עברה על כולם ולא מצאה כזה, תדחה.

בהתבסס על ההגדרות של קבלה והכרעה, מוגדרות מחלקות של שפות:

- $\mathrm{R}=\{L\mid$ קיימת מכונה M המכריעה את $L\}$
- $\mathrm{RE}=\{L\mid$ קיימת מכונה M המקבלת את $L\}$

(הערה טכנית – יש להגדיר מעל איזה א"ב השפות; אנו מניחים תמיד כי מדובר על $\Sigma=\{0,1\}$.)

שימו לב: קל להיווכח כי $\mathrm{R}\subseteq\mathrm{RE}$ (מדוע?).

בסימונים אלו, ראינו כי $\mathrm{HP}\in\mathrm{RE}$, וכן $\mathrm{COMPOSITE}\in\mathrm{R}$.

הרצה מבוקרת

נציג כעת שיטה חזקה להוכחה ששפות מסוימות הן ב־RE. בתור דוגמה נתבונן בשפה הבאה:

- $L = \{\langle M\rangle \mid f_M(x) = x$ קיים x כך ש־$\}$.

זוהי שפת כל המכונות שיש "נקודת שבת" לפונקציה שהן מחשבות.

בהינתן $\langle M\rangle$, לא ברורה דרך לבדוק האם קיימת נקודת שבת שאינה פשוט חיפוש מבוסס כוח גס: להריץ את M על כל קלט אפשרי x ולבדוק האם הפלט הוא גם x. לצורך כך, נצטרך מספור של אברי Σ^*.

דרך אחת למספר את המילים ב־Σ^* היא באמצעות סדר לקסיקוגרפי: $w_1 < w_2$ אם $|w_1| < |w_2|$ או אם $|w_1| = |w_2|$ אבל w_1 באה לפני w_2 בסדר מילוני רגיל (דהיינו, כשמשווים אות־אות). נמספר את המילים ב־Σ^* כ־$w_1, w_2, w_3, \ldots$.

נשתמש במניה שהצגנו ונקבל את האלגוריתם הבא:

1. לכל $i = 1, 2, \ldots$
   (א) הרץ את M על w_i וסמן $y = M(w_i)$.
   (ב) אם $y = w_i$, קבל.

נשים לב שאם ל־M אין נקודת שבת, האלגוריתם לא יסתיים לעולם. דבר זה אינו מפריע לנו כי כל מטרתנו היא להראות ש־$L \in \mathrm{RE}$, ולכן על מילים שאינן שייכות ל־L "מותר לנו" לא לעצור. כמו כן, נשים לב כי כדי ליישם את האלגוריתם, צריך "לזכור" רק את i ואת w_i, ומהם קל למצוא את $i+1$ ואת w_{i+1}.

לרוע המזל האלגוריתם לא עובד, שכן לא מובטח לנו ש־M עוצרת לכל x, וייתכן שלא תעצור עבור w_i כאשר קיימת נקודת שבת w_j, $j > i$. הפתרון הוא לבצע הרצה מבוקרת. נתאר זאת פורמלית:

1. לכל $j = 1, 2, \ldots$
   (א) לכל $i = 1, 2, \ldots, j$
      i. הרץ את M על w_i במשך j צעדים, ואם סיימה סמן $y = M(w_i)$.
      ii. אם $y = w_i$, קבל.

כלומר, באיטרציה הראשונה אנו מריצים את M צעד אחד על הקלט w_1. באיטרציה השנייה אנו מריצים את M שני צעדים על שני הקלטים w_1, w_2 וכן הלאה.

אם $\langle M\rangle \in L$ אז קיימת מילה w_i כך ש־$f_M(w_i) = w_i$, וריצת M על w_i נמשכת k צעדים. אז באיטרציה ה־$j = \max\{i, k\}$ נריץ את M על w_i ונעשה זאת למשך k צעדים לפחות, ועל כן נקבל.

שיקולי ספירה וטיעוני לכסון

נראה כעת כי קיימות שפות שאינן ב־R ואף לא ב־RE. הטיעון שלנו יהיה מבוסס על שיקולי ספירה. באופן כללי שיקולי ספירה הם כלי רב עצמה בהוכחת קיום או אי־קיום של דבר מה.

כזכור מתורת הקבוצות, קבוצה שיש העתקה על מהמספרים הטבעיים אליה נקראת בת מניה, והעתקה כזו נקראת מניה. ראינו לעיל מניה של Σ^* (שכינינו בשם "סדר לקסיקוגרפי"), ולכן אנחנו יודעים שהיא בת מניה. נציג כעת הוכחה חלופית למסקנה ש־Σ^* היא בת מניה: קל לראות כי לכל א"ב סופי Σ, מתקיים ש־Σ^* היא בת מניה, שכן $\Sigma^* = \bigcup_{n\geq 0} \Sigma^n$, כל Σ^n (אוסף כל המילים מעל Σ מאורך בדיוק n) היא סופית, ואיחוד בן מניה של קבוצות סופיות הוא בן־מניה. מטיעון זה נובע שקיים רק מספר בן מניה של מכונות טיורינג, שכן ראינו כי כל מכונה ניתן לקודד באמצעות מחרוזת סופית, כלומר איבר של Σ^*.

מצד שני, ניתן להראות בטיעון דומה לזה של האלכסון של קנטור כי קיים מספר לא בן מניה של שפות. נניח כי $L_1, L_2 \ldots$ היא מניה של כל השפות מעל Σ ונבנה שפה $L' = \{w_i \mid w_i \notin L_i\}$. דהיינו, לכל אחת מהמילים $w_i \in \Sigma^*$, היא נמצאת ב־L' אם ורק אם היא לא נמצאת ב־L_i. מכאן שלכל i בהכרח $L' \neq L_i$ שכן הן נבדלות במילה w_i, ומכאן ש־L' אינה במניה של השפות – סתירה. מכאן שיש מספר לא בן מניה של שפות.

מנגד, כל מכונת טיורינג מקבלת שפה אחת בדיוק. מכאן שיש רק מספר בן מניה של שפות שמתקבלות על ידי מכונות טיורינג, אך יש מספר לא בן מניה של שפות באופן כללי, ולכן קיימות שפות שאינן מתקבלות על ידי מכונת טיורינג.

הלכסון הוצג כאן אך ורק כתזכורת, מכיוון שבהמשך הקורס נציג לכסונים מחוכמים יותר. ניתן באופן כללי להסתפק באמירה שאוסף כל השפות מעל Σ הוא בדיוק אוסף כל התת קבוצות של Σ^*, כלומר הוא קבוצת החזקה של Σ^* ועל פי משפט קנטור מתורת הקבוצות, עצמתו גדולה מעוצמת Σ^*.

נעבור כעת לשימוש נוסף של שיקולי ספירה, שהופיע באחד המבחנים: יש להוכיח כי לכל שפה אינסופית $L \in \mathrm{R}$ קיימת תת־שפה $L' \subseteq L$ כך ש־$L' \notin \mathrm{RE}$. הטיעון זהה למה שכבר ראינו: L היא אינסופית בת מניה, ועל כן ממשפט קנטור נובע שעוצמת קבוצת החזקה שלה, שהיא אוסף כל תת השפות של L, איננה בת מניה, ולכן קיימת תת־שפה שאינה מתקבלת על־ידי אף מכונת טיורינג.