הרצאה 5 – יום רביעי 6.8

שימוש ברדוקציות

$$L_{BIG} \coloneqq \{\langle M\rangle : |L(M)| > 1\}$$

ראשית, נוכיח ש- $L_{BIG} \in RE$. נתאר מונה בשבילה:

עם 3 לולאות מקוננות: לכל אורך של קידוד מכונה, לכל אורך של מילת קלט, לכל מספר צעדים – נרוץ עד שנמצא 2 מילים שמתקבלות.

אם מצאנו, נדפיס את המכונה הזו.

נתאר רדוקציה $HALT \le L_{BIG}$. עבור קלט $\langle M, x\rangle$ נחזיר $\langle M_x^*\rangle$, כאשר:

עבור קלט x, $M_x^*(x)$ מריצה את $M(x)$. אז אם $M(x)$ עוצרת, $M_x^*(x) = 1$. אחרת, $M_x(x)$ לא עוצרת.

ועבור קלט $1x$ (שרשור), M_x^* מחזירה 1.

לכל קלט אחר, M_x^* מחזירה 0.

אם $M_x^* \in L_{BIG}$ זה אומר שיש לה 2 מילים בשפה, כלומר $M(x)$ עוצרת. אז אם $L_{BIG} \in R$, גם $HALT \in R$, סתירה.

או בקצרה: תיארנו רדוקציה $HALT \le L_{BIG}$. מכיוון ש- $HALT \notin R$, גם $L_{BIG} \notin R$.

$$EQ \coloneqq \{\langle M_1\rangle\langle M_2\rangle : L(M_1) = L(M_2)\}$$

<u>טענה</u>: $EQ \notin RE$.

<u>הוכחה</u>: נעשה רדוקציה $A_{TM} \le EQ$. בהינתן קלט $\langle M, x\rangle$, נחשב את $\langle M', M''\rangle$, כאשר:

M' היא מ"ט שמקבלת כל קלט (כלומר $L(M') = \Sigma^*$).

M'' מחזירה את $M(x)$ לכל קלט. כלומר אם $\langle M, x\rangle \in A_{TM}$, אז $L(M'') = \Sigma^*$. ואם $\langle M, x\rangle \notin A_{TM}$, אז $L(M'') = \emptyset$.

$$\langle M, x\rangle \in A_{TM} \Leftrightarrow \langle M', M''\rangle \in EQ$$

<u>טענה</u>: $EQ \notin coRE$.

<u>הוכחה</u>: נעשה רדוקציה $A_{TM} \le \overline{EQ}$. בהינתן קלט $\langle M, x\rangle$, נחשב את $\langle M', M''\rangle$, כאשר:

M' היא מ"ט שדוחה כל קלט (כלומר $L(M') = \emptyset$).

M'' מחזירה את $M(x)$ לכל קלט. כלומר אם $\langle M, x\rangle \in A_{TM}$, אז $L(M'') = \Sigma^*$. ואם $\langle M, x\rangle \notin A_{TM}$, אז $L(M'') = \emptyset$.

$$\langle M, x\rangle \in A_{TM} \Leftrightarrow \langle M', M''\rangle \in \overline{EQ}$$

בסה"כ, $EQ \in \overline{RE \cup coRE}$.

שפות שלמות – *Complete Languages*

מושגים מוכרים מאלגו 2 – קושי ושלמות של מחלקה. *Hardness, Completeness*. נגדיר:

תהי C מחלקה של שפות (כמו $R, RE, coRE$).

שפה L תיקרא ***C*-קשה** (*C-hard*) אם ניתן לעשות רדוקציה מכל שפה ב-C ל-L.

שפה $L \in C$ תיקרא ***C*-שלמה** (*C-complete*) אם היא C-קשה.

<u>טענה</u>: השפה $HALT$ היא *RE-complete*.

<u>הוכחה</u>: ראשית, ניזכר ש- $HALT \in RE$ (הרצאה 4).

נוכיח שכל שפה $L \in RE$ מקיימת $L \le HALT$. תהי $L \in RE$ כלשהי. אז קיימת מ"ט M כך ש- $M(x) = 1$ לכל $x \in L$.

נעשה רדוקציה ל-*HALT*: בהינתן $\langle M, x\rangle$, נחזיר $\langle M^*, x\rangle$, כאשר M^* שקולה ל-M אבל אם M דוחה, M^* נכנסת ללולאה אינסופית.

אם M מקבלת את x אז $M^*(x)$ עוצרת.

אם M דוחה את x או נכנסת ללולאה, $M^*(x)$ נכנסת ללולאה.

$$\langle M, x\rangle \in L \Leftrightarrow F(\langle M, x\rangle) = \langle M^*, x\rangle \in HALT$$

כנדרש.

אפשר לעשות רדוקציה מכל $L \in RE$ ל-*HALT*, אז $HALT$ היא *RE-hard*. ומכיוון ש- $HALT \in RE$, היא גם *RE-complete*.

ומכיוון שרדוקציה היא טרנזיטיבית, זה אומר שאם נעשה רדוקציה מ-*HALT* לכל שפה L, זה מראה ש-L היא *RE-hard*.

משפט רייס – *Rice's Theorem*

שיטה להוכיח ששפה לא ניתנת להכרעה (לא ב-R) בלי להשתמש ברדוקציות.

נגדיר: **תכונה סמנטית** (*semantic property*) של מ"ט היא קבוצת "תיאורים" של מכונות, כך שלכל M_1, M_2 שמקיימות $L(M_1) = L(M_2)$ מתקיים $\langle M_1\rangle, \langle M_2\rangle \in P$ או $\langle M_1\rangle, \langle M_2\rangle \notin P$.

תכונה סמנטית **לא טריוויאלית** היא תכונה כך שקיימות M', M'' כך ש: $\langle M'\rangle \in P, \langle M''\rangle \notin P$.

דוגמאות:

$$P \coloneqq \{\langle M\rangle \mid L(M) \in R\}, \qquad P \coloneqq \{\langle M\rangle \mid L(M) = \emptyset\}, \qquad P \coloneqq \{\langle M\rangle \mid 001 \in L(M)\}$$

הערה חשובה: תכונה סמנטית היא תכונה של התוצאה של המכונה, או תכונה של השפה של המכונה. היא לא תלויה בייצוג הספציפי של המכונה.

לא להתבלבל עם תכונה סינטקטית (*syntactic property*), היא תכונה של התיאור של המכונה. תכונות סינטקטיות ניתנות להכרעה בקלות – לפי התיאור של המכונה.

<u>משפט רייס</u>: לכל $P \subseteq RE, P \neq \emptyset, P \neq RE$, מתקיים: $L_P \coloneqq \{\langle M\rangle \mid \langle M\rangle \in P\} \notin R$.

במילים: כל תכונה סמנטית לא טריוויאלית אינה ניתנת להכרעה.

<u>הוכחה</u>: נוכל להניח ש- $P \neq \emptyset$ (כי אחרת פשוט ניקח את $\bar{P} = RE \setminus P$).

P היא לא טריוויאלית, אז קיימת שפה $L \in P$ שמתקבלת ע"י מ"ט כלשהי, T.

נניח (בשלילה) שקיימת מ"ט D שמכריעה את P: $D(\langle M\rangle) = 1$ אם $\langle M\rangle \in P$, ו- $D(\langle M\rangle) = 0$ אחרת.

נבנה רדוקציה $A_{TM} \leq P$.

בהינתן קלט $\langle M, x\rangle$, אנחנו צריכים לבנות M' כך ש- $D(\langle M'\rangle) = 1 \Leftrightarrow M(x) = 1$.

המכונה M', בהינתן קלט y:

מריצה את $M(x)$ ודוחה אם M דוחה. (אם M לא עוצרת, גם M' לא עוצרת). אם M מקבלת את x, נמשיך:

מריצה את $T(y)$ ומקבלת אם T מקבלת.

אם M מקבלת את x, אז $L(M') = L(T) = L \in P$, ואז $D(\langle M'\rangle) = 1$. אם M לא מקבלת את x, אז $L(M') = \emptyset \notin P$ ואז $D(\langle M'\rangle) = 0$.

כלומר, $D(\langle M'\rangle) = 1 \Leftrightarrow \langle M, x\rangle \in A_{TM}$. בסה"כ, $D(\langle M'\rangle)$ מכריעה את A_{TM}, סתירה.

שימוש במשפט רייס

בהינתן שפה, נתייחס לתיאור השפה כמו תכונה, וצריך להראות שני דברים:

1. לא טריוויאלית: קיימת מכונה שיש לה את התכונה, ומכונה שאין לה.
2. תכונה של שפה: אם שתי מכונות מקבלות את אותה השפה, לשתיהן יש את התכונה או לשתיהן אין.

ואז, התכונה לא ניתנת להכרעה, כלומר השפה לא ב-R.

דוגמה: $L_{BIG} \coloneqq \{\langle M\rangle : |L(M)| > 1\} \notin R$.

התכונה $|L(M)| > 1$ היא לא טריוויאלית:

המכונה שדוחה כל קלט מקיימת $M_{REJ} \notin L_{BIG}$, כי $|L(M_{REJ})| = 0$.

המכונה שמקבלת כל קלט מקיימת $M_{ACC} \in L_{BIG}$, כי $|L(M_{ACC})| > 1$.

היא תכונה של שפה: אם שתי מכונות מקבלות את אותה השפה, אז לא יכול להיות שמכונה אחת מקיימת את התכונה (השפה בגודל 2 לפחות) והמכונה השנייה לא (השפה בגודל קטן מ-2).

אז לפי משפט רייס, התכונה לא ניתנת להכרעה, כלומר $L_{BIG} \notin R$.

דוגמה שלא עובדת: $L_{0\text{-}cell} \coloneqq \{\langle M\rangle : on\ input\ 0,\ \ the\ 0\text{-}cell\ of\ the\ tape\ never\ overwrites\}$.

כל המכונות שאם מריצים קלט 0, אף פעם לא כותבים במיקום ה-0 בסרט.

זו תכונה לא טריוויאלית:

המכונה שדוחה כל קלט מייד, מקיימת $M_{REJ} \in L_{0\text{-}cell}$ כי לא נוגעים באף תא.

המכונה שלכל קלט, הולכת לתא 0 וכותבת בו 1, מקיימת $M_{REJ} \notin L_{0\text{-}cell}$.

אבל זו לא תכונה של שפה:

המכונה מקבלת כל קלט מייד, מקיימת $M_{REJ} \in L_{0\text{-}cell}$ כי לא נוגעים באף תא. והשפה שלה היא Σ^*.

המכונה שלכל קלט, הולכת לתא 0 וכותבת בו 1, ואז מקבלת, מקיימת $M_{REJ} \notin L_{0\text{-}cell}$. והשפה שלה היא גם Σ^*.

שתי המכונות מקבלות את אותה שפה, אבל אחת מקיימת את התכונה והשנייה לא.

אז אי אפשר להשתמש במשפט רייס פה.

עוד דוגמה שלא עובדת: $L_{all\text{-}halt} \coloneqq \{\langle M\rangle : M\ halts\ on\ any\ input\}$.

זה נראה דומה לבעיית העצירה. אבל נשים לב שבעיית העצירה מדברת על מכונה וקלט ספציפי.

זו תכונה לא טריוויאלית:

המכונה שדוחה כל קלט מייד, מקיימת $M_{REJ} \in L_{all\text{-}halt}$ כי תמיד עוצרים.

המכונה שלכל קלט, זזה ימינה עד אינסוף, מקיימת $M_{right} \notin L_{all\text{-}halt}$, כי אף פעם לא עוצרים.

אבל זו לא תכונה של שפה:

המכונה מקבלת כל קלט שנגמר ב-1.

המכונה שעוברת על כל הקלט. אם התו האחרון הוא 1, נקבל. אם לא, נמשיך עד אינסוף.

שתי המכונות מקבלות את אותה שפה, אבל אחת מקיימת את התכונה והשנייה לא.

עוד דוגמה שלא עובדת: $L_{bounded\text{-}halt} \coloneqq \{\langle M, x\rangle : M\ halts\ on\ x\ after\ no\ more\ than\ n\ steps\}$.

זו תכונה לא טריוויאלית:

המכונה שדוחה כל קלט מייד, מקיימת $M_{REJ} \in L_{bounded\text{-}halt}$.

המכונה שלכל קלט, זזה ימינה עד אינסוף, מקיימת $M_{right} \notin L_{bounded\text{-}halt}$, כי אף פעם לא עוצרים.

אבל זו לא תכונה של שפה:

המכונה מקבלת כל קלט שמתחיל ב-1.

המכונה שאם התו הראשון הוא 1, נקבל. אם לא, נמשיך עד אינסוף.

שתי המכונות מקבלות את אותה שפה, אבל אחת מקיימת את התכונה והשנייה לא.

משפט רייס החזק – SRT

תהי P תכונה לא טריוויאלית של מ"ט, כך שקיימת $\langle M' \rangle \notin P$ כך ש- $L(M') = \Sigma^*$.

אזי, P לא ניתנת לזיהוי (לא קיימת מ"ט שמקבלת אותה). כלומר $C_P \coloneqq \{\langle M \rangle \mid L(M) \in P\} \notin RE$.

במילים: כל תכונה סמנטית לא טריוויאלית שלא כוללת את Σ^*, היא לא ב-RE.

<u>הוכחה</u>: נוכיח ע"י רדוקציה $\overline{A_{TM}} \leq C_P$. (כי $\overline{A_{TM}} \notin RE$, אז $C_P \notin RE$).

P לא טריוויאלית, כלומר קיימת $T \in P$.

בהינתן קלט $\langle M, x \rangle$, נבנה מ"ט M' שלכל קלט y מריצה את $M(x), T(y)$ במקביל. אם אחד מהם מקבל, נחזיר 1.

אם M לא מקבלת את x אז $L(M') = L(T) \in P$, אם M מקבלת את x אז $L(M') = \Sigma^* \in P$.

עכשיו, נוכל לזהות את $\overline{A_{TM}}$:

נניח (בשלילה) שקיימת M_P שמקבלת את P.

אם $\langle M, x \rangle$ לא קידוד תקין, נחזיר 1.

נריץ את $M_P(\langle M' \rangle)$ ונחזיר את מה שהיא מחזירה.

אם M לא מקבלת את x, אז $L(M') = L(T) = L \in P$. אם M מקבלת את x, אז $L(M') = \Sigma^* \notin P$ ואז נחזיר 0 או ניכנס ללולאה.

כלומר, קיבלנו דרך לזהות את $\overline{A_{TM}}$ – סתירה.

דוגמה: $L_{SMALL} \coloneqq \{\langle M \rangle : |L(M)| \leq 1\} \notin RE$.

התכונה לא טריוויאלית:

המכונה שדוחה כל קלט מקיימת $M_{REJ} \in L_{SMALL}$, כי $\left|L\left(M_{REJ}\right)\right| = 0$.

המכונה שמקבלת כל קלט מקיימת $M_{ACC} \notin L_{BIG}$, כי $|L(M_{ACC})| > 1$.

היא תכונה של שפה: אם שתי מכונות מקבלות את אותה השפה, אז לא יכול להיות שמכונה אחת מקיימת את התכונה (השפה בגודל לכל היותר 1) והמכונה השנייה לא (השפה בגודל יותר מ-1).

היא לא כוללת את Σ^*: קיימת שפה M_{ACC} שמקבלת את Σ^*, ולא מקיימת את התכונה.

אז לפי משפט רייס החזק, התכונה לא ניתנת לזיהוי, כלומר $L_{SMALL} \notin RE$.

מסקנות ממשפט רייס החזק

תהי P תכונה לא טריוויאלית של מ"ט, כך שקיימת $\langle M' \rangle \in P$ כך ש- $L(M') = \Sigma^*$.

אזי, P לא נמצאת ב- $coRE$. כלומר $C_P \coloneqq \{\langle M \rangle \mid L(M) \in P\} \notin coRE$.

במילים: כל תכונה סמנטית לא טריוויאלית שכוללת את Σ^*, היא לא ב-$coRE$.

<u>הוכחה</u>: נעשה רדוקציה $A_{TM} \leq \overline{L_P}$.

בהינתן קלט $\langle M, x \rangle$, נבנה מ"ט M':

בהינתן קלט y, מריצה את $M(x)$.

אם M לא מקבלת את x, נריץ את T שמקבלת את Σ^*.

אם M מקבלת את x, נדחה הכל.

אם M לא מקבלת את x אז $L(M') = L(T) \in P$, אם M מקבלת את x אז $L(M') = \emptyset \notin P$.

כלומר, אם $\langle M, x\rangle \in A_{TM}$, אז $L(M') = \emptyset \notin P$, כלומר $\langle M'\rangle \in \overline{L_P}$.

ואם $\langle M, x\rangle \notin A_{TM}$, אז $L(M') = \Sigma^* \in P$, כלומר $\langle M'\rangle \notin \overline{L_P}$.

$$\langle M, x\rangle \in A_{TM} \Leftrightarrow \langle M'\rangle \in \overline{L_P}$$

אז $\overline{L_P} \notin RE$, כלומר $L_P \notin coRE$, או במילים אחרות $P \notin coRE$.

ניסוחים אחרים:

$$\exists M' \in P: L(M') = \emptyset \Longrightarrow C_P \coloneqq \{\langle M\rangle : L(M) \in P\} \notin RE$$

$$\exists M' \notin P: L(M') = \emptyset \Longrightarrow C_P \coloneqq \{\langle M\rangle : L(M) \in P\} \notin coRE$$

דוגמה: $L_1 \coloneqq \{\langle M\rangle : |L(M)| = 1\}$.

התכונה לא טריוויאלית: מכונה שמקבלת רק את 0, מכונה שמקבלת את 0 ואת 1.

היא תכונה של שפה: אם שתי מכונות מקבלות את אותה השפה, אז לא יכול להיות שהשפה של כל מכונה בגודל אחר.

היא לא כוללת את Σ^*.

אז מכיוון ש- $L(M_{ACC}) = \Sigma^* \notin L_1$, נקבל לפי SRT ש- $L_1 \notin RE$. ובגלל ש- $L(M_{REJ}) = \emptyset \notin L_1$, נקבל לפי המסקנה ש- $L_1 \notin coRE$.

$$L_1 \in \overline{RE \cup coRE}$$