הרצאה 4 – יום רביעי 30.7

המשלים של *RE* – *coRE*

נגדיר את שפת $coRE$:

$$coRE \coloneqq \{L \mid \bar{L} \in RE\}$$

קבוצת כל השפות שהמשלים שלהן ב-RE.

הוכחנו ש- $L \in R \Longrightarrow \bar{L} \in R$. זה לא מתקיים עבור RE. כלומר, אם $\bar{L} \in RE$, זה אומר ש- $L \in coRE$. אבל זה לא אומר ש- $L \in RE$.

טענה: $R = RE \cap coRE$.

הוכחה: כיוון ראשון, נוכיח $R \subseteq RE \cap coRE$.

תהי $L \in R$. צ"ל $L \in RE \wedge L \in coRE$.

מתקיים $L \in RE$ כי L מוכרעת ולכן גם מתקבלת ע"י מ"ט M. (באופן כללי, כבר אמרנו ש- $R \subseteq RE$).

עבור שפה $\bar{L}$, נבנה מ"ט $\bar{M}$ שזהה ל-M אבל מחזירה 1 כאשר M מחזירה 0, ומחזירה 0 כאשר M מחזירה 1. אז $\bar{L} \in RE$, כלומר $L \in coRE$.

בכיוון השני, נוכיח $RE \cap coRE \subseteq R$.

תהי $L \in RE \cap coRE$. צ"ל $L \in R$.

קיימות M_1 שמקבלת את L ו-M_2 שמקבלת את $\bar{L}$. נבנה מ"ט M כך:

עבור קלט x, נריץ את M_1, M_2 במקביל ונעצור ברגע שאחד מהן עוצרת, ונחזיר $M_1(x)$ או $\neg M_2(x)$.

אם $x \in L$, אז M עוצרת ומחזירה 1 (כי החזרנו את $M_1(x) = 1$ או את $\neg M_2(x)$).

$x \notin L$, אז M עוצרת ומחזירה 0 (כי החזרנו את $\neg M_2(x) = 0$ או את $\neg M_1(x)$).

כלומר M מכריעה את L, אז $L \in R$.

מחלקת A_{TM}

$$A_{TM} \coloneqq \{\langle M, x\rangle \mid M \; accepts \; x\}$$

מחלקת הזוגות של מכונה ומילה שהיא מקבלת. בהמשך, נקרא לה פשוט A.

טענה: $A \in RE$.

הוכחה: מספיק לבנות TM שמקבלת זוג של מכונה ומילה, ומחזירה 1 אם המכונה מקבלת את המילה.

תהי U מ"ט אוניברסלית. נריץ את U על הקלט $\langle M, x\rangle$, ונחזיר את מה ש-U מחזירה.

אם $M(x) = 1$, אז $U(\langle M, x\rangle) = 1$. אם $M(x) = 0$, אז $U(\langle M, x\rangle) = 0$. אם $M(x) = \infty$, אז $U(\langle M, x\rangle) = \infty$.

אז אם M מקבלת את x אז U מקבלת את $\langle M, x\rangle$, אז $A \in RE$.

טענה: $A \notin R$.

הוכחה: אנחנו מנסים להוכיח שלא קיימת מ"ט שמכריעה את A. נב"ש שקיימת מכונה D_A שמכריעה את A. כלומר, בהינתן $\langle M, x\rangle$, מחזירה 1 אם M מקבלת את x, ו-0 אחרת. ונבנה את M_A – מכונה שפועלת הפוך מ- D_A:

בהינתן קלט x, נריץ את $D_A(\langle M_A, x\rangle)$ ונקבל 0 או 1. נחזיר את ההפוך. כלומר: $M_A(x) \coloneqq \neg D_A(\langle M_A, x\rangle)$.

וניזכר שלפי הגדרה, $D_A(\langle M, x\rangle) \coloneqq M(x)$. אז $D_A(\langle M_A, x\rangle) \coloneqq M_A(x)$. קיבלנו ש- $M_A(x) = \neg M_A(x)$, סתירה.

הוכחה שנייה ל- $A \notin R$ – שיטת האלכסון:

נב"ש ש- $A \in R$, אז קיימת מ"ט D_A שמכריעה אותה. נבנה מכונה M_A כך:

נריץ את $D_A(\langle M, \langle M \rangle \rangle)$, ונחזיר את ההפך של מה שיוצא (0 או 1).

בהינתן x כלשהו, לכל המכונות טיורינג $M_1, M_2, M_3 \ldots$ נבנה טבלה (אינסופית) שמסמנת האם M_i מקבלת את $x := \langle M_j \rangle$.

המכונה D_A יכולה למלא את התאים באלכסון. כלומר, נגדיר $(i, i) := D_A(\langle M_i, \langle M_i \rangle \rangle)$:

	$<M_1>$	$<M_2>$	$<M_3>$	$<M_4>$	…
M_1	1	0	1	1	
M_2	1	0	0	0	
M_3	0	1	1	0	
M_4	1	1	0	1	
…					

מה יקרה בתא של M_A? אם $M_A(\langle M_A \rangle) = 1$, אז $D_A(\langle M_A, \langle M_A \rangle \rangle) = 1$, אבל אז לפי הגדרת M_A, אמרנו שמגדירים $M_A(\langle M_A \rangle) = 0$.

ואם $M_A(\langle M_A \rangle) = 0$, אז $D_A(\langle M_A, \langle M_A \rangle \rangle) = 0$, אבל אז לפי הגדרת M_A, אמרנו שמגדירים $M_A(\langle M_A \rangle) = 1$. סתירה.

מחלקת SA

$$SA := \{\langle M \rangle \mid M \text{ accepts } \langle M \rangle\}$$

מחלקת המכונות שמקבלות את עצמן. SA – *Self-Accepting*.

<u>טענה</u>: $SA \in RE$.

<u>הוכחה</u>: מספיק לבנות מ"ט שמחזירה 1 אם M מקבלת את $\langle M \rangle$. נריץ את M על $\langle M \rangle$ ונחזיר מה ש-M מחזירה.

אם $\langle M \rangle$ התקבלה ע"י M אז $M(\langle M \rangle) = 1$, אחרת $M(\langle M \rangle) = 0$ או $M(\langle M \rangle) = \infty$. אז $SA \in RE$.

<u>טענה</u>: $SA \notin R$.

<u>הוכחה</u>: בדומה להוכחה ש- $A \notin R$, נב"ש ש- $SA \in R$. אז קיימת מכונה D_{SA} שמכריעה את SA. כלומר, בהינתן $\langle M \rangle$, מחזירה 1 אם M מקבלת את $\langle M \rangle$, ו-0 אחרת. ונבנה את M_{SA} – מכונה שפועלת הפוך מ- D_{SA}:

בהינתן קלט x, נריץ את $D_{SA}(\langle M_{SA} \rangle)$ ונקבל 0 או 1. נחזיר את ההפוך. כלומר: $M_{SA}(\langle M_{SA} \rangle) := \neg D_{SA}(\langle M_{SA} \rangle)$.

וניזכר שלפי הגדרה, $D_{SA}(\langle M \rangle) := M(\langle M \rangle)$. אז $D_{SA}(\langle M_{SA} \rangle) := M_{SA}(\langle M_{SA} \rangle)$. קיבלנו ש- $M_{SA}(\langle M_{SA} \rangle) := \neg M_{SA}(\langle M_{SA} \rangle)$, סתירה.

הוכחנו ש- $R \neq RE$ (ע"י זה ש- $A_{TM} \in RE \setminus R$), אז $R \subsetneq RE$. (תת-קבוצה לא שווה).

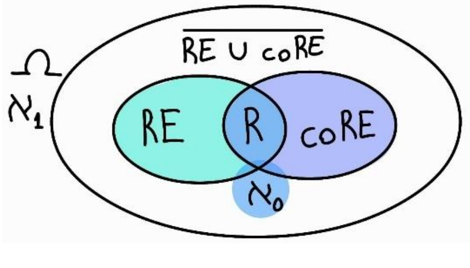
ונקבל ש- $RE \neq coRE$, כי אחרת:

$$A_{TM} \in coRE \Longrightarrow A_{TM} \in RE \cap coRE \Longrightarrow A_{TM} \in R$$

כי הוכחנו ש- $R = RE \cap coRE$.

יש $\aleph_1$ שפות אפשריות, כי מספר השפות הוא כל הקבוצות האפשריות של מחרוזות. $|\mathcal{P}(\Sigma^*)| = 2^{\aleph_0} = \aleph_1$.

ומספר המ"ט האפשריות הוא רק $\aleph_0$, כי כל מ"ט מקודדת ע"י מחרוזת סופית מעל א"ב סופי. $|\Sigma^*| = \aleph_0$.



בעיית העצירה – *The Halting Problem*

$$HALT \coloneqq \{\langle M, x\rangle \mid M \text{ } halts \text{ } on \text{ } x\}$$

שפת כל הזוגות של מ"ט M ומילה x, ש-M עוצרת בהינתן x.

<u>טענה</u>: $HALT \in RE$.

<u>הוכחה</u>: מספיק לבנות מ"ט שמחזירה 1 אם $M(x)$ עוצרת. נגדיר את המכונה M_H:

היא מריצה את $M(x)$. אם $M(x) = 0$ או $M(x) = 1$, נחזיר 1. אחרת, המכונה לא תעצור.

אם $M(x)$ עוצרת אז $M_H(\langle M, x\rangle) = 1$, כלומר $HALT \in RE$.

<u>טענה</u>: $HALT \notin R$.

<u>הוכחה</u>: נב"ש ש- $HALT \in R$, כלומר קיימת מ"ט D_H שמכריעה אותה. כלומר, $D_H(\langle M, x\rangle) = 1$ אם $M(x)$ עוצרת, ו-0 אחרת.

נבנה מ"ט M_H כך: בהינתן קלט $\langle M, x\rangle$, היא עוצרת אם $D_H(\langle M, x\rangle) = 0$, ואם $D_H(\langle M, x\rangle) = 1$, היא לא עוצרת.

נריץ את על $M_H(\langle M_H, x\rangle)$ ונקבל שאם $M_H(\langle M_H, x\rangle) = 1$ כלומר היא עוצרת, אז היא לא עוצרת.

ואם $M_H(\langle M_H, x\rangle) = 0$ כלומר היא לא עוצרת, אז היא עוצרת. סתירה.

<u>טענה</u>: $HALT \notin coRE$.

<u>נוכיח</u>: נב"ש שכן, כלומר קיימת מ"ט M_1 שמקבלת את כל הזוגות $\langle M, x\rangle$ כך ש-M לא עוצרת בהינתן x.

וכבר הוכחנו ש- $HALT \in RE$. אז קיימת מ"ט M_2 שמקבלת את כל הזוגות $\langle M, x\rangle$ כך ש-M עוצרת בהינתן x.

נוכל לבנות מ"ט שמכריעה את $HALT$: בהינתן $\langle M, x\rangle$ נריץ את M_1, M_2 במקביל – כל פעם, i צעדים בכל אחת.

אם $M(x)$ עוצרת, אז נקבל 1 מ- M_2. אם $M(x)$ לא עוצרת, נקבל 1 מ- M_1. כלומר $HALT \in R$, סתירה.

$$SHALT \coloneqq \{\langle M\rangle \mid M \text{ } halts \text{ } on \text{ } \varepsilon\}$$

שפת כל המכונות שעוצרות בהינתן המילה הריקה.

<u>טענה</u>: $SHALT \in RE \setminus R$.

<u>הוכחה</u>: כדי להוכיח ש- $SHALT \in RE$, מספיק לבנות מ"ט שמחזירה 1 אם $M(\varepsilon)$ עוצרת. נריץ את $M(\varepsilon)$. אם $M(\varepsilon) = 1$ או $M(\varepsilon) = 0$, נחזיר 1.

נוכיח ש- $SHALT \notin R$: נב"ש ש- $SHALT \in R$, כלומר קיימת מ"ט D_{SH} שמכריעה אותה. כלומר, $D_{SH}(\langle M\rangle) = 1$ אם $M(\varepsilon)$ עוצרת, ו-0 אחרת.

נבנה מ"ט M_{SH} כך: בהינתן קלט $\langle M\rangle$, היא עוצרת אם $D_{SH}(\langle M\rangle) = 0$, ואם $D_{SH}(\langle M\rangle) = 1$, היא לא עוצרת.

נריץ את על $M_{SH}(\langle M_{SH}\rangle)$ ונקבל שאם $M_{SH}(\langle M_{SH}\rangle) = 1$ כלומר היא עוצרת, אז היא לא עוצרת.

ואם $M_{SH}(\langle M_{SH}\rangle) = 0$ כלומר היא לא עוצרת, אז היא עוצרת. סתירה.

$$EMPTY \coloneqq \{\langle M\rangle \mid L(M) = \emptyset\}$$

<u>טענה</u>: $EMPTY \in coRE$.

<u>הוכחה</u>: מספיק להוכיח ש- $\overline{EMPTY} \in RE$.

נבנה מ"ט M^* שמקבלת קלט $\langle M\rangle$. בכל שלב i, היא מריצה i צעדים של $M(x)$ לכל $x \in \Sigma^i$. ברגע ש- $M(x)$ מחזיר 1, M^* מחזירה 1.

אם $|L(M)| > 0$ אז $M^*(\langle M\rangle) = 1$. אחרת, $M^*(\langle M\rangle) = \infty$.

כלומר, $\overline{EMPTY} \in RE$, אז $EMPTY \in coRE$.

<u>טענה</u>: $EMPTY \notin R$.

<u>הוכחה</u>: נב"ש ש- $EMPTY \in R$. אז קיימת מ"ט M_E שמכריעה אותה. כלומר, $M_E(\langle M\rangle) = 1$ אם $L(M) = \emptyset$, ו- $M_E(\langle M\rangle) = 0$ אם $L(M) \neq \emptyset$.

בהינתן מ"ט M ומילה x, נבנה מ"ט M_x: עבור קלט y, היא מחזירה 0 אם $x \neq y$, ואחרת מחזירה את $M(x)$.

כלומר, אם M מקבלת את x, אז $L(M_x) = \{x\}$. ואחרת, $L(M_x) = \emptyset$.

נבנה מ"ט A_D: עבור קלט $\langle M, x\rangle$, היא מריצה את $M_E(\langle M_x\rangle)$ ומחזירה את ההפך ממה שיוצא.

אם $M_E(\langle M_x\rangle) = 1$, זה אומר ש- $L(M_x) = \emptyset$, כלומר M לא מקבלת את x. אז A_D תחזיר 0.

אם $M_E(\langle M_x\rangle) = 0$, זה אומר ש- $L(M_x) \neq \emptyset$, כלומר M מקבלת את x. אז A_D תחזיר 1.

בנינו מכונה שמכריעה את A_{TM}, סתירה.

רדוקציות

בגדול אותה הגדרה מאלגו 2, פשוט יותר כללית. שיטה להעביר בעיה מסוג א לבעיה מסוג ב, ככה שאם יש לנו פתרון לבעיה ב אז יש לנו פתרון לבעיה א.
פורמלית, נכתוב שפונקציה R היא רדוקציה משפה L_1 לשפה L_2, אם מתקיים: $\forall x: x \in L_1 \Leftrightarrow R(x) \in L_2$. ונרשום: $L_1 \leq L_2$.

<u>טענה</u>: יהיו $L_1 \leq L_2$. אזי מתקיים:

א. $L_2 \in R \Longrightarrow L_1 \in R$

<u>הוכחה</u>: קיימת מ"ט M שמכריעה את L_2, ומ"ט F שמחשבת רדוקציה מ-L_1 ל-L_2. אז עבור קלט x, נחזיר את $M(F(x))$. מתקיים:

$$M(F(x)) = 1 \Leftrightarrow F(x) \in L_2 \Leftrightarrow x \in L_1, \qquad M(F(x)) = 0 \Leftrightarrow F(x) \notin L_2 \Leftrightarrow x \notin L_1$$

ב. $L_2 \in RE \Longrightarrow L_1 \in RE$

<u>הוכחה</u>: קיימת מ"ט M שמקבלת את L_2, ומ"ט F שמחשבת רדוקציה מ-L_1 ל-L_2. אז עבור קלט x, נחזיר את $M(F(x))$. מתקיים:

$$M(F(x)) = 1 \Leftrightarrow F(x) \in L_2 \Leftrightarrow x \in L_1, \qquad M(F(x)) \neq 1 \Leftrightarrow F(x) \notin L_2 \Leftrightarrow x \notin L_1$$

ג. $L_2 \in coRE \Longrightarrow L_1 \in coRE$

<u>הוכחה</u>: קיימת מ"ט M שמקבלת את $\overline{L_2}$, ומ"ט F שמחשבת רדוקציה מ-L_1 ל-L_2. אז עבור קלט x, נחזיר את $M(F(x))$.

אם $x \in \overline{L_1}$, אז $F(x) \in \overline{L_2}$ ואז $M(F(x)) = 1$. אחרת, $M(F(x)) = 0$ או $M(F(x)) = \infty$. מתקיים:

$$M(F(x)) = 1 \Leftrightarrow F(x) \in \overline{L_2} \Leftrightarrow x \in \overline{L_1}, \qquad M(F(x)) \neq 1 \Leftrightarrow F(x) \notin \overline{L_2} \Leftrightarrow x \notin \overline{L_1}$$

אז $\overline{L_1} \in RE$, משמע $L_1 \in CoRE$.

בנוסף, מתוך *contrapositive*, נקבל:

$$L_1 \notin R \Longrightarrow L_2 \notin R, \qquad L_1 \notin RE \Longrightarrow L_2 \notin RE, \qquad L_1 \notin coRE \Longrightarrow L_2 \notin coRE$$

עוד תכונות של רדוקציות:

$$(\text{א})\ L_1 \leq L_2 \Longrightarrow \overline{L_1} \leq \overline{L_2}, \qquad (\text{ב})\ L \leq L, \qquad (\text{ג})\ L_1 \leq L_2 \land L_2 \leq L_3 \Longrightarrow L_1 \leq L_3$$

א. כי לכל x, מתקיים $R(x) \notin \overline{L_2} \Leftrightarrow R(x) \in L_2$. אז:
$$x \in \overline{L_1} \Leftrightarrow x \notin L_1 \Leftrightarrow R(x) \notin L_2 \Leftrightarrow R(x) \in \overline{L_2}$$
ב. מתקבלת ע"י הרדוקציה: $R(x) \coloneqq x$.
ג. מתקבלת ע"י שרשור הרדוקציות.

שימוש ברדוקציות

נוכיח ש- $HALT \notin R$, ע"י רדוקציה $A_{TM} \leq HALT$. כי אם $A_{TM} \leq HALT$, אז $HALT \notin R \Longrightarrow A_{TM} \notin R$.

נגדיר את הרדוקציה F: בהינתן $\langle M, x\rangle$, נגדיר $F(\langle M, x\rangle) \coloneqq \langle M^*, x\rangle$, כאשר:

M^* זהה ל-M, חוץ מזה שאם M דוחה את x, אז M^* נכנסת ללולאה אינסופית. ואחרת, M^* עוצרת. אז:

$$\langle M, x\rangle \in A_{TM} \Longleftrightarrow F(\langle M, x\rangle) \coloneqq \langle M^*, x\rangle \in HALT$$

הוכחנו $A_{TM} \leq HALT$, אז $HALT \notin R \Longrightarrow A_{TM} \notin R$. כנדרש.

בהינתן שפה L כלשהי, כדי להוכיח ש- $L \notin R$ או $L \notin coRE$, מספיק לבנות רדוקציה $HALT \leq L$.

כי אם $L \in R$, אז לפי הרדוקציה נקבל ש- $HALT \in R$, סתירה. ובאופן דומה עבור $coRE$.

כדי להוכיח ש- $L \in RE$, נבנה רדוקציה $L \leq HALT$.

כי אז המכונה המקבלת עבור $HALT$ משמשת בתור מכונה מקבלת עבור L.

כדי להוכיח ש- $L \notin RE$, נבנה רדוקציה $\overline{HALT} \leq L$.

כי אם $L \in RE$, אז $\overline{HALT} \in RE$ ואז $HALT \in coRE$, סתירה.

דוגמאות

רדוקציה $SHALT \leq HALT$: בהינתן $\langle M\rangle$, נבדוק את $\langle M, \varepsilon\rangle$. כלומר $SHALT \in RE$.

רדוקציה $HALT \leq SHALT$: בהינתן $\langle M, x\rangle$, נייצר את $\langle M_x\rangle$, כאשר M_x היא המכונה M עם הקלט x. לכל קלט, היא מריצה את $M(x)$. מתקיים:

$$\langle M, x\rangle \in HALT \Longleftrightarrow \langle M_x\rangle \in SHALT$$

אז $SHALT \notin RE$.