הרצאה 6

אפיון אלגברי של שפות רגולריות

מוטיבציה: ראינו את למת הניפוח לשפות רגולריות. ראינו גם שקיימות שפות לא רגולריות שניתנות לניפוח. אפשר להוכיח גרסה מוכללת של למת הניפוח, שבה ניתן לטפל בחלק מהשפות האלו. אבל זה עדיין תנאי **הכרחי אך לא מספיק** לרגולריות. נרצה לפתח אפיון מלא, כלומר, "שפה רגולרית אמ"מ מתקיים ___".

1 יחסים

תזכורת מתורת הקבוצות: יחס ייקרא:

- **רפלקסיבי** אם $\forall x : R(x,x)$,
- **סימטרי** אם $\forall x,y : R(x,y) \Longrightarrow R(y,x)$,
- **טרנזיטיבי** אם $\forall x,y,z : R(x,y) \wedge R(y,z) \Longrightarrow R(x,z)$

יחס R המקיים את שלושת התכונות לעיל ייקרא **יחס שקילות.**

יחס שקילות משרה חלוקה של העולם לתתי קבוצות זרות ומשלימות הנקראות **מחלקות שקילות.**

לדוגמה – פעולת mod היא יחס שקילות, ומגדירה מחלקות שקילות על הטבעיים.

יהי R יחס שקילות על קבוצה A. נסמן $index(R)$ את מספר מחלקות השקילות.

נציג מתוך המחלקות יסומן: $[x] = \{y : R(x,y)\}$.

נאמר כי יחס R' **מעדן את** R אם $R' \subseteq R$, כלומר:

$$\forall x,y \in A : R'(x,y) \Longrightarrow R(x,y)$$

כל מחלקת שקילות של R' מוכלת במחלקת שקילות של R.

1.1 יחסי שקילות מעל Σ^*

הגדרה: יחס שקילות R מעל Σ^* ייקרא **אינווריאנטי מימין** אמ"מ הוא מקיים:

$$\forall x,y \in \Sigma^* : R(x,y) \Longrightarrow \forall z \in \Sigma^* : R(xz,yz)$$

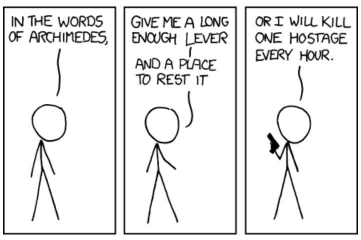
כלומר, אם נשרשר את אותה המילה מימין, היחס יישמר. לא בהכרח הם יישארו באותה מחלקת שקילות – יכול להיות ששניהם יעברו למחלקת שקילות אחרת (אבל שניהם יהיו באותה מחלקת שקילות).

דוגמאות ליחסים כאלו:

1. האות הימנית ביותר ב-x שווה לאות הימנית ביותר ב-y.
2. $|x| = |y|$

היחס $x = y^R$ אינו יחס שקילות אינוריאנטי מימין.

גם שני ילדים שקולים על מאזניים אינם אינווריאנטים מימין, כי בתוספת משקל זהה לצד ימין של שניהם, אחת התוספות רחוקה יותר מהמרכז ומשפיעה יותר, בגלל עיקרון המנוף:
וגם, מסיבה טכנית, זה לא מוגדר מעל Σ^*.



איור 1 - עקרון המנוף של ארכימדס

2 הקישור לאוטומט – יחס R_A

בהינתן $A = (Q, \Sigma, q_0, \delta, F)$, נגדיר יחס שקילות R_A:

$$R_A(x,y) \Leftrightarrow \hat{\delta}(q_0,x) = \hat{\delta}(q_0,y)$$

כלומר, שתי מילים שקולות אמ"מ הן מובילות אותנו לאותו מצב.

נוכיח תחילה שזה אכן יחס שקילות – נוכיח שהוא רפלקסיבי, סימטרי, וטרנזיטיבי:

- רפלקסיבי: $\forall x \in \Sigma^* :\ \hat{\delta}(q_0,x) = \hat{\delta}(q_0,x)$
- סימטרי: $\forall x,y \in \Sigma^* : R_A(x,y) \Longrightarrow \hat{\delta}(q_0,x) = \hat{\delta}(q_0,y) \Longrightarrow R_A(y,x)$
- טרנזיטיבי:

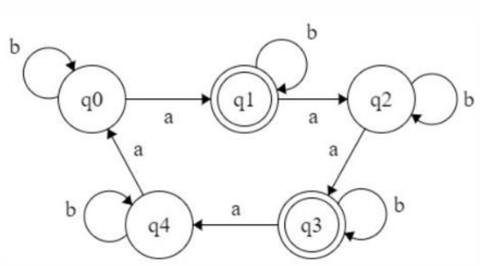
$$\forall x,y,z \in \Sigma^* : R_A(x,y) \wedge R_A(y,z) \Longrightarrow$$
$$\left[\hat{\delta}(q_0,x) = \hat{\delta}(q_0,y)\right] \wedge \left[\hat{\delta}(q_0,y) = \hat{\delta}(q_0,z)\right] \Longrightarrow$$
$$[\hat{\delta}(q_0,x) = \hat{\delta}(q_0,z)]$$

נניח כי $Q = \{q_0, q_1, \dots, q_{m-1}\}$, ונגדיר את השפות הבאות:

$$S_i = \{x : \hat{\delta}(q_0,x) = q_i\}$$

מחלקות השקילות של R_A הן ה-S_i שאינן ריקות. כלומר: באס"ד שבו כל המצבים ברי השגה, ל-R_A יש $|Q|$ מחלקות שקילות.

דוגמה:



$$S_0 = \left(b + a(b^*)a(b^*)a(b^*)a(b^*)a(b^*)\right)^*$$

$$S_1 = S_0 \cdot a(b^*)$$

$$S_2 = S_1 \cdot (b^*)a(b^*)$$

$$S_3 = S_2 \cdot (b^*)a(b^*)$$

$$S_4 = S_3 \cdot (b^*)a(b^*)$$

2.1 שפת האוטומט

כעת שהגדרנו את מחלקות השקילות בתור שפות מילים המגיעות למצבים, נוכל להיעזר בכך כדי להגדיר את שפת האוטומט:

$$L(A) = \cup_{q_i \in F} S_i = \{x : \exists q \in F : \hat{\delta}(q_0,x) = q\}$$

בדוגמה לעיל, המצבים המקבלים הם q_1, q_3 ולכן שפת האוטומט היא:

$$L(A) = L_1 \cup L_3$$

$$r = (b + a(b^*)a(b^*)a(b^*)a(b^*)a)^*$$

$$S_1 = r \cdot a(b^*)$$

$$S_3 = r \cdot a(b^*)a(b^*)a(b^*)$$

2.2 R_A אינווריאנטי מימין

תזכורת: יחס שקילות R מעל Σ^* ייקרא **אינווריאנטי מימין** אמ"מ הוא מקיים:

$$\forall x,y \in \Sigma^* : R(x,y) \Longrightarrow \forall z \in \Sigma^* : R(xz,yz)$$

כלומר, אם נשרשר את אותה המילה מימין, היחס יישמר.

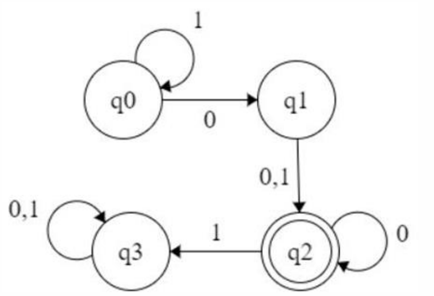
לפי הגדרה, R_A אומר ש $\hat{\delta}(q_0,x) = \hat{\delta}(q_0,y)$. נשרשר את z לשתי המילים:

$$\hat{\delta}(q_0,xz) = \hat{\delta}(\hat{\delta}(q_0,x),z) = \hat{\delta}(\hat{\delta}(q_0,y),z) = \hat{\delta}(q_0,yz)$$

כלומר, $R_A(xz,yz)$, כלומר R_A אינווריאנטי מימין.

2.3 עוד דוגמה

נתון האוטומט הבא:



מחלקות השקילות שלו הן:

$$S_0 = 1^*, \qquad S_1 = 1^*0, \qquad S_2 = 1^*0(0+1)0^*,$$
$$S_3 = 1^*0(0+1)0^*1(0+1)^*$$

$$L(A) = S_2$$

3 היחס R_L

הגדרה: עבור שפה $L \subseteq \Sigma^*$, היחס R_L מוגדר כך:

$$R_L(x,y) \Leftrightarrow (\forall z \in \Sigma^* : xz \in L \leftrightarrow yz \in L)$$

במילים: היחס R_L מקבל זוג מילים אמ"מ לכל סיפא z, שתי המילים המורחבות xz, yz שתיהן מתקבלות או שתיהן לא. במילים אחרות: x, y שקולות ביחס R_L אמ"מ לא קיימת סיפא המפרידה ביניהן.

בהמשך נראה שזה יחס שקילות.

3.1 דוגמאות

תהי $L_1 = \Sigma^*$, מהן מחלקות השקילות של R_L?

ליחס זה יש מחלקת שקילות אחת בלבד, שכן לכל $z \in \Sigma^*$ מתקיים $xz \in L_1$ וגם $yz \in L_1$.

כנ"ל לגבי $L_2 = \emptyset$ - לכל $z \in \Sigma^*$ מתקיים $xz \notin L_1$ וגם $yz \notin L_1$.

תהי $L_3 = \{w \in \{0,1\}^* : |w| \equiv 1(mod\ 2)\}$. מהן מחלקות השקילות של R_L?

יש 2 מחלקות שקילות – זוגי, אי זוגי. לפי הגדרה: $R_L(x,y) \Leftrightarrow |x| \equiv |y|(mod\ 2)$, ולכן:

$$S_1 = \{w \in \{0,1\}^* : |w| \equiv 0(mod\ 2)\}$$

$$S_2 = \{w \in \{0,1\}^* : |w| \equiv 1(mod\ 2)\}$$

תהי $L_4 = \{a, aa\}$. מהן מחלקות השקילות של R_L?

$$S_1 = \{\epsilon\}, \qquad S_2 = \{a\}, \qquad S_3 = \{aa\}, \qquad S_4 = \Sigma^* \setminus \cup_{i=1}^{3} S_i$$

תהי $L_5 = \{x \in \{a,b\}^* : \#_a(x) = \#_b(x)\}$. מהן מחלקות השקילות של R_L?

לכל $k \in \mathbb{Z}$ יש מחלקת שקילות מהצורה: $S_k = \{x \in \{a,b\}^* : \#_a(x) - \#_b(x) = k\}$. אינטואיטיבית, כי סופרים את ההפרש בין a ל-b בכל מילה.

כדי להוכיח שאלה מחלקות השקילות, צריך להוכיח את הדברים הבאים:

1. שהן לא ריקות, ומכסות את Σ^*
2. שכל זוג מילים x, y מאותה מחלקה אינן ניתנות להפרדה ע"י אותה סיפא. פורמלית: $\forall x, y \in S_j, \forall z \in S_i : xz \in S_{i+j} \wedge yz \in S_{i+j}$
3. כל זוג מילים ממחלקות שונות, כן ניתנות להפרדה ע"י סיפא כלשהי.

נראה את 3: יהיו $x \in S_i, y \in S_j$ עבור $i \neq j$ כלשהם. אזי, עבור: $z \in S_{-i}$, נקבל: $x \in L_5, y \notin L_5$.

3.2 עידון של שפה

יהי R יחס שקילות מעל Σ^*, ותהי $L \subseteq \Sigma^*$ שפה.

נאמר כי R **מעדן את** L אמ"מ מתקיים: $R(x,y) \Longrightarrow (x \in L \leftrightarrow y \in L)$.

כלומר, אם מתקיים ש: שתי מילים יהיו ביחס רק אם שתיהן בשפה או שתיהן לא בשפה. שקול ל: $(x \in L \; xnor \; y \in L)$.

טענה: לכל אס"ד A, היחס R_A מעדן את $L(A)$. (תזכורת: $R_A(x,y)$ אמ"מ שתי המילים מגיעות לאותו מצב).

הוכחה:

$$R(x,y) \Longrightarrow^{\text{א}} \left[\hat{\delta}(q_0,x) = \hat{\delta}(q_0,y)\right] \Longrightarrow^{\text{ב}} [x \in L(A) \leftrightarrow y \in L(A)]$$

א – הגדרת R_A, ב – הגדרת $L(A)$.

3.3 משפט האפיון של R_L

משפט: $\forall L \subseteq \Sigma^*$:

1. R_L הוא יחס שקילות אינווריאנטי מימין,
2. R_L מעדן את L,
3. אם R יחס שקילות אינווריאנטי מימין המעדן את L, אזי R מעדן גם את R_L.

במילים אחרות: R_L הינו יחס השקילות האינוריאנטי מימין המכיל הכי מעט מחלקות שקילות. כלומר, החלוקה ה"גסה" ביותר של Σ^* השומרת על העידון והאינווריאנטיות.

הוכחת 1: נוכיח שהוא יחס שקילות:

<u>רפלקסיבי</u>: נתון $\forall z \in \Sigma^* : [xz \in L \leftrightarrow xz \in L]$, ולכן לפי הגדרה: $R_L(x,x)$.

<u>סימטרי</u>: אם $R_L(x,y)$, זה אומר ש $xz \in L \leftrightarrow yz \in L$, כלומר $yz \in L \leftrightarrow xz \in L$, כלומר $R_L(y,x)$.

<u>טרנזיטיבי</u>: אם $R_L(x,y)$ וגם $R_L(y,w)$, אזי לכל $z \in \Sigma^*$ מתקיים: $[xz \in L \leftrightarrow yz \in L] \wedge [yz \in L \leftrightarrow wz \in L]$, ולכן גם מתקיים: $xz \in L \leftrightarrow wz \in L$. כלומר $R_L(x,w)$.

נוכיח שהוא אינווריאנטי מימין:

לפי הגדרה, אם $R_L(x,y)$ אזי $\forall z, w \in \Sigma^*$ מתקיים: $xzw \in L \leftrightarrow yzw \in L$.

לכן נוכל גם לכתוב: $\forall z \in \Sigma^*$ מתקיים: $(xz)w \in L \leftrightarrow (yz)w \in L$.

כלומר, $\forall z \in \Sigma^*$, מתקיים $R_L(xz, yz)$.

הוכחה 2: נוכיח ש R_L מעדן את L:

לפי הגדרה, $R_L(x,y) \Longrightarrow [\forall z \in \Sigma^* : xz \in L \leftrightarrow yz \in L]$.

בפרט, עבור $z = \epsilon$ נקבל $R_L(x,y) \Longrightarrow [x \in L \leftrightarrow y \in L]$.

כלומר, R_L מעדן את L.

הוכחה 3: כל יחס עם אותן תכונות מעדן את R_L:

יהי R יחס שקילות אינווריאנטי מימין המעדן את L. אזי:

$$R(x,y) \Longrightarrow^{\text{א}} [\forall z \in \Sigma^* : R(xz,yz)] \Longrightarrow^{\text{ב}} [\forall z \in \Sigma^* : (xz \in L \leftrightarrow yz \in L)] \Longrightarrow R_L(x,y)$$

א – אינווריאנטי מימין, ב – מעדן.

כלומר: $R(x,y) \Longrightarrow R_L(x,y)$, או במילים אחרות: $R \subseteq R_L$.

4 משפט נרוד

תהי $L \subseteq \Sigma^*$. אזי, הטענות הבאות שקולות:

1. L רגולרית,
2. קיים יחס שקילות R, שהוא אינווריאנטי מימין ומעדן את L ומקיים: $index(R) < \infty$,
3. $index(R_L) < \infty$.

תזכורת: עבור יחס שקילות R על קבוצה A. נסמן $index(R)$ את מספר מחלקות השקילות.

4.1 הוכחה $1 \rightarrow 2$

נתון: L רגולרית. צ"ל: קיים יחס שקילות R, שהוא אינווריאנטי מימין ומעדן את L ומקיים: $index(R) < \infty$.

אם L רגולרית, קיים עבורה אס"ד. כבר הראנו ש R_A הוא יחס שקילות אינווריאנטי מימין המעדן את L.

כמו כן, $index(R_A) \leq |Q_A|$ ובפרט $index(R_A) < \infty$, כנדרש.

4.2 הוכחה $2 \rightarrow 3$

נתון: קיים יחס שקילות R, שהוא אינווריאנטי מימין ומעדן את L ומקיים: $index(R) < \infty$. צ"ל: $index(R_L) < \infty$.

לפי משפט האפיון: כל יחס שקילות אינווריאנטי מימין המעדן את L מעדן גם את R_L. לכן מתקיים:

$$index(R_L) \leq index(R) < \infty$$

4.3 הוכחה $3 \rightarrow 1$

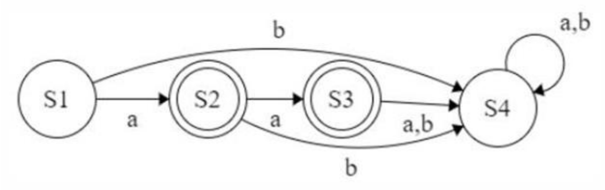
נתון: $index(R_L) < \infty$. צ"ל: L רגולרית.

הרעיון: נבנה אוטומט שמצביו הם מחלקות השקילות של R_L.

לדוגמה, עבור $L = \{a, aa\}$ מצאנו ארבע מחלקות שקילות:

$$S_1 = \{\epsilon\}, \qquad S_2 = \{a\}, \qquad S_3 = \{aa\}, \qquad S_4 = \Sigma^* \setminus \cup_{i=1}^{3} S_i$$

נבנה אס"ד ע"פ R_L:



נבנה אס"ד A_L המקבל את L.

קבוצת המצבים מוגדרת ע"י: $Q_{A_L} = \{[x] : x \in \Sigma^*\}$ כלומר, כל מחלקת שקילות היא מצב.

נתון $index(R_L) < \infty$ ולכן $|Q_{A_L}| < \infty$.

המצב ההתחלתי הוא $q_0 = [\epsilon]$.

פונקציית המעברים: $\delta([x], a) = [xa]$.

היות והיחס אינווריאנטי מימין, לא משנה איזה נציג נבחר מהמחלקה. שכן $[x] = [y] \Longrightarrow [xa] = [ya]$.

קבוצת המצבים המקבלים: $F = \{[x] : x \in L\}$.

4.4 $\boldsymbol{L = L(A)}$

נותר להראות שהאוטומט שבנינו אכן מתאים לשפה:

טענה 1: לכל x מתקיים: $\hat{\delta}(q_0, x) = [x]$.

הוכחה באינדוקציה על $|x|$:

בסיס: עבור $|x| = 0$, בהכרח $x = \epsilon$ ואכן $\delta(q_0, \epsilon) = q_0 = [\epsilon]$. (כך הגדרנו את q_0).

נניח שהטענה מתקיימת עבור $|w| = n$ ונוכיח עבור $w\sigma$.

$$\hat{\delta}(q_0, w\sigma) =^{א} \delta\big(\hat{\delta}(q_0, w), \sigma\big) =^{ב} \delta([w], \sigma) =^{ג} [w\sigma]$$

א – הגדרת $\hat{\delta}$, ב – הנ"א, ג – הגדרת δ.

טענה 2: לכל $x \in \Sigma^*$ מתקיים: $[x] \in F \iff x \in L$

כיוון ראשון: מיידי, מהגדרת F.

כיוון שני: נניח ש $[x] \in F$. מהגדרת F, קיימת מילה $y \in [x]$ כך ש $y \in L$ (המחלקות לא ריקות).

היות ו- $R_L(x, y)$, ו- R_L מעדן את L, נובע גם ש $x \in L$.

לכן קיבלנו סה"כ:

$$x \in L(A_L) \iff^{א} \hat{\delta}(q_0, x) \in F \iff^{ב} [x] \in F \iff^{ג} x \in L$$

א – הגדרת F, ב – טענה 1, ג – טענה 2.

4.5 שימושי משפט נרוד

1. אפיון אמ"מ לשפות רגולריות: **שפה L רגולרית אמ"מ** $\boldsymbol{index(R_L) < \infty}$
2. מינימליות אס"ד: כמות מחלקות השקילות של R_L יוצרות את האס"ד המינימלי לשפה.
3. שימושי לשאלות במבחן :)

5 דוגמאות לשימוש

5.1 הוכיחו כי: $L = \{b^*\} \cup \{a^k b^{2^n} : n, k \in \mathbb{N}\}$ אינה רגולרית.

למת הניפוח לשפות רגולריות לא עוזרת פה, כי "האויב" יכול לכפות ניפוח ב-a, ולא להפר את b^{2^i}.

לפי משפט נרוד, מספיק להראות ש $index(R_L) = \infty$.

איך מראים שיש אינסוף מחלקות שקילות? ע"י בחירת קבוצת מילים אינסופית, והוכחה כי כל שתי מילים ניתנות להפרדה ע"י סיפא כלשהי. מכאן ינבע כי כל שתי מילים שייכות במחלקות שקילות נפרדות, ומכאן שיש אינסוף מחלקות שקילות, כנדרש.

נגדיר את קבוצת המילים האינסופית $A = \{ab^{2^k} : k \in \mathbb{N}\}$.

יהיו $i \neq j$, ונסתכל על שתי המילים ab^{2^i}, ab^{2^j}. למילים אלו קיימת סיפא מפרידה: $z = b^{2^j}$.

$$ab^{2^i} b^{2^j} = ab^{2^i + 2^j} \notin L$$

$$ab^{2^j} b^{2^j} = ab^{2^{j+1}} \in L$$

כלומר, לכל שתי מילים קיימת סיפא מפרידה, ולכן ליחס R_L יש אינסוף מחלקות שקילות.

לכן, לפי משפט נרוד, השפה L אינה רגולרית.

5.2 תהי $L = \{a^n c^n\} \cup \{a^n b^n c^n\}$. הוכיחו כי השפה אינה רגולרית, בעזרת משפט נרוד.

נגדיר את קבוצת המילים האינסופית $A = \{a^n\}$. יהיו $i \neq j$. נסתכל על שתי המילים a^i, a^j. למילים אלו קיימת סיפא מפרידה $z = c^i$: $a^i c^i \in L,\ a^j c^i \notin L$. מצאנו סיפא מפרידה בין כל שתי מילים מהקבוצה האינסופית, ולכן ליחס R_L קיימות אינסוף מחלקות שקילות. לכן, לפי משפט נרוד, השפה L אינה רגולרית.

5.3 תהי $L = \{a^n b^m c^m\} \cup \{a^n b^n c^m\}$. הוכיחו כי השפה אינה רגולרית, בעזרת משפט נרוד.

נגדיר את קבוצת המילים האינסופית $A = \{a^n\}$. יהיו $i \neq j$. נסתכל על שתי המילים a^i, a^j. שתיהן בשפה.

למילים אלו קיימת סיפא מפרידה: $z = b^i c^{i+1}$. כי $a^i b^i c^{i+1} \in L, a^j b^i c^{i+1} \notin L$.

מצאנו סיפא מפרידה בין כל שתי מילים מהקבוצה האינסופית, ולכן ליחס R_L קיימות אינסוף מחלקות שקילות. לכן, לפי משפט נרוד, השפה L אינה רגולרית.

5.4 תהי $L = \{a^n b^{3n} c^n\} \cup \{a^n b^{3n} c^{3n}\}$. הוכיחו כי השפה אינה רגולרית, בעזרת משפט נרוד.

נגדיר את קבוצת המילים האינסופית $A = \{a^n b^{3n}\}$. יהיו $i < j$ (בה"כ). נסתכל על שתי המילים $a^i b^{3i}, a^j b^{3j}$. למילים אלו קיימת סיפא מפרידה $z = c^i$. כי $a^i b^{3i} c^i \in L, a^j b^{3j} c^i \notin L$ (כי $i < j$ אז לא יכול להיות ש $i = 3j$).

מצאנו סיפא מפרידה בין כל שתי מילים מהקבוצה האינסופית, ולכן ליחס R_L קיימות אינסוף מחלקות שקילות. לכן, לפי משפט נרוד, השפה L אינה רגולרית.