חישוביות - שיעור 2

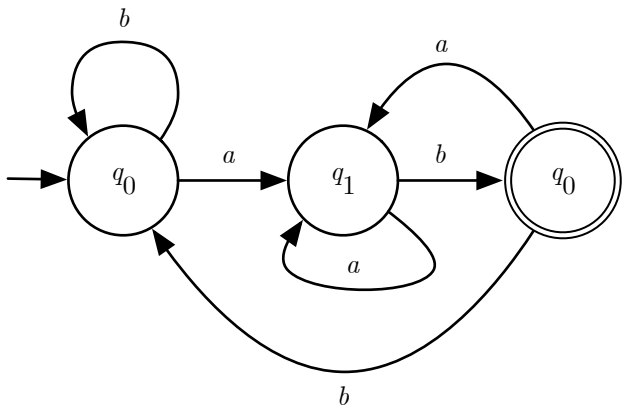
דוד קלוטה

12 באפריל 2026

בשיעור הקודם

בגדול, בקורס אנחנו רוצים לראות מה אלגוריתמים יכולים לעשות, אבל בשביל זה נצטרך להגדיר אלגוריתם ומודל חישובי. בחלק זה של הקורס אנחנו מדברים על "מודל צעצוע" (שעל אף שהוא לא יכול לעשות הכל הוא יכול לעשות הרבה) - האוטומט הסופי הדטרמיניסטי DFA.

דוגמה **2.0.1.** נתחיל עם א"ב $\Sigma = \{a, b\}$ ונסתכל על האוטומט הבא:



איור 1: אוטומט $\mathcal{A}$ המגדיר שפה

קל לראות שאוטומט זה מגדיר את השפה הבאה:

$$L(\mathcal{A}) = L \stackrel{\text{def}}{=\!=} \{w \in \Sigma^* \mid w \text{ ends in } ab\}$$

אבל איך אנחנו מוכיחים דבר כזה?

1. מוצאים חלוקה של המילים מעל Σ על פי המצבים שהאוטומט מגיע אליהם בריצתו על המילה
2. מוכיחים את נכונות החלוקה באינדוקציה על אורך המילה

כך בעצם ננסח למה שתיתן לנו להוכיח את האוטומט בעזרת one-liner. ננסח למה שכזו בעבור אוטומט $\mathcal{A}$:

טענה. ניתן לחלק את המילים ב־Σ^* באופן הבא:

1. *המילים שמגיעות ל־q_0 הן ε, b ומילים המסתיימות ב־bb*
2. *המילים שמגיעות ל־q_1 הן המילים שמסתיימות ב־a*
3. *המילים שמגיעות ל־q_2 הן המילים שמסתיימות ב־ab*

המסקנה המיידית מהטענה היא ש־$L(\mathcal{A})$ היא אכן מה שאמרנו מראש, שהיא שפה L.

הוכחה. נוכיח את הטענה באינדוקציה על $n = |w|$, כאשר $w \in \Sigma^*$:

מקרה בסיס $n = 0$ יש רק מילה אחת כזו, ε והיא מקיימת את הטענה.

מקרה בסיס $n = 1$ יש רק שתי מילים כאלה ב־Σ^* הן a, b. אם נריץ את האוטומט נראה שהמילים האלה נכנסות לאוטומט: $\delta(q_0, a) = q_1$ ו־$\delta(q_0, b) = q_0$

המקרה הכללי $n \geqslant 1$ תהי $w' \in \Sigma^{n+1}$. נכתוב את $w' = w \cdot \sigma$ כאשר $\sigma \in \Sigma$. נוכיח את הטענה על ידי חלוקה למקרים על σ:

1. $\sigma = a$ לפי איך שהאוטומט מוגדר, לכל $q \in Q$ מתקיים כי $\delta(q, a) = q_1$, ולכן $w' = w \cdot \sigma$ בהכרח נמצאת ב־q_1.
2. $\sigma = b$ נחלק למקרים על פי האות האחרונה של w (נשתמש בעובדה ש־$n \geqslant 1$):

(א) w מסתיימת ב־b: מכאן, w' מסתיימת ב־bb. על פי הנחת האינדוקציה w מגיעה ל־q_0 או ל־q_2, ובעבור שני המצבים האלה קבלת b תוביל אותנו ל־q_0 בהתאם ל־δ.

(ב) w מסתיימת ב־a: מהנחת האינדוקציה, w בהכרח נמצאת במצב q_1 ועל ידי קבלת b נגיע למצב q_2 - מכיוון ש־w' אכן מסתיימת ב־ab.

כל המצבים מתקיימים - וסיימנו את ההוכחה. □

התחלנו!

2.1 האוטומט הסופי הדטרמיניסטי ורגולריות

שאלה. *אילו שפות ניתן להכריע בעזרת DFA?*

הגדרה 2.1.1. תהי REG קבוצת השפות אשר קיים עבורן DFA המכריע אותן - מעל כל א"ב אפשרי. נקרא להן השפות הרגולריות.

שאלה (קלה יותר). *לאילו פעולות על שפות* REG *סגורה?*

דוגמה **2.1.1.** אם $L_1, L_2 \in \mathrm{REG}$ שפות מעל אותו א"ב Σ. האם $L_1 \cap L_2 \in \mathrm{REG}$? כן!
אפשר גם לשאול זאת לגבי $L_1 \cup L_2 \in \mathrm{REG}$? גם כן.
כנ"ל לגבי $\overline{L_1} \in \mathrm{REG}$. גם לזה התשובה היא כן.

הגדרה 2.1.2 (כל המילים מעל א"ב). אם Σ א"ב, אז $\Sigma^* \overset{\text{def}}{=\!=} \bigcup_{i=0}^{\infty} \Sigma^i$.

הגדרה 2.1.3 (משלים של שפה). אם L שפה מעל Σ, אז $\overline{L} \overset{\text{def}}{=\!=} \Sigma^* \backslash L$

טענה 2.1.1. *אם* $L \in \mathrm{REG}$, *אז גם* $\overline{L} \in \mathrm{REG}$

סקיצה של ההוכחה. אם L רגולרית, מהגדרה קיים אוטומט סופי דטרמיניסטי המגדיר אותה. תהי F קבוצת המצבים המקבלים של $\mathcal{A}$, האוטומט המגדיר את L. נסמן קבוצת מצבים מקבלים חדשה, $\overline{F} = Q \backslash F$, נבנה אוטומט חדש הזהה ל־$\mathcal{A}$ רק שקבוצת המצבים המקבלים שלו היא $\overline{F}$ וסיימנו. □

הגדרה 2.1.4 (הגדרה פורמלית של DFA). $\mathcal{A}$ אוטומט סופי דטרמיניסטי הוא חמישייה המכילה

$$\mathcal{A} \overset{\text{def}}{=\!=} (Q, \Sigma, \delta, q_0, F)$$

אשר איבריה:

1. Q - קבוצת המצבים של האוטומט
2. Σ - הא"ב של קלט האוטומט
3. $\delta : (Q \times \Sigma) \to Q$ - פונקציית המעברים
4. $q_0 \in Q$ - המצב ההתחלתי
5. $F \subseteq Q$ - המצבים המקבלים

הגדרה 2.1.5 (ריצה של אוטומט על מילה). הריצה של $\mathcal{A}$ על מילה $w \in \Sigma^n$ הסדרה $(s_i)_{i=0}^n$ שמקיימת

$$s_i \overset{\text{def}}{=\!=} \begin{cases} q_0 & i = 0 \\ \delta(s_{i-1}, w_i) & i \geqslant 1 \end{cases}$$

הגדרה 2.1.6 (פונקציית מעברים מורחבת). פונקציית המעברים המורחבת של $\mathcal{A}$ היא $\delta^* : (Q \times \Sigma^*) \to Q$ כאשר $\delta^*(q, w)$ היא המצב שאליו A יגיע אם יתחיל במצב q ואז יקרא את כל האותיות של w.

$$\delta^*(q, w) \overset{\text{def}}{=\!=} \begin{cases} q & w = \varepsilon \\ \delta(\delta^*(q, u), \sigma) & w = u \cdot \sigma \end{cases}$$

הגדרה 2.1.7 (שפה המוגדרת על ידי אוטומט). עבור האוטומט $\mathcal{A}$, נוכל להגדיר את השפה המוגדרת על ידי בתור

$$L(\mathcal{A}) \overset{\text{def}}{=\!=} \{w \in \Sigma^* \mid \delta^*(q_0, w) \in F\}$$

משפט 2.1.1. *אם* $L_1, L_2 \in \mathrm{REG}$*, אזי גם* $L_1 \cup L_2 \in \mathrm{REG}$.

הוכחה. יהיו $\mathcal{A}_1, \mathcal{A}_2$ אוטומטים סופיים דטרמיניסטיים המכריעים את L_1, L_2 בהתאמה. נכתוב:

$$\mathcal{A}_1 = (Q, \Sigma, \delta, q_0, F), \quad \mathcal{A}_2 = (P, \Sigma, \eta, p_0, G)$$

נבנה אוטומט מכפלה $\mathcal{B}$ שמכריע את איחוד השפות $L_1 \cup L_2$.

$$\mathcal{B} = (Q \times P, \Sigma, \varphi, (q_0 \times p_0), H)$$

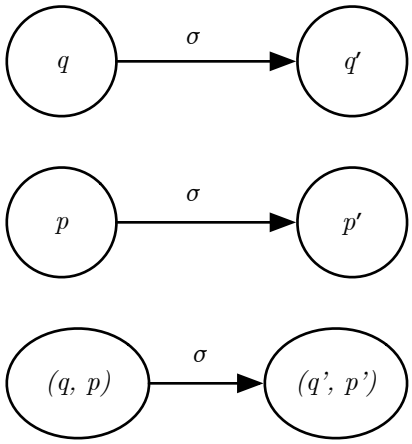
הרעיון הוא שאם $w \in \Sigma^*$ שמקיימת $\delta^*(q_0, w) = q$ ו־$\eta^*(p_0, w) = p$ אזי $\varphi^*((q_0, p_0), w) = (q, p)$ ולפיכך, נגדיר

$$H \stackrel{\text{def}}{=\!=} \{(q, p) \in Q \times P \mid q \in F \vee p \in G\}$$

וכעת גם נוכל להגדיר

$$\forall (q, p) \in Q \times P : \varphi((q, p), \sigma) \stackrel{\text{def}}{=\!=} (\delta(q, \sigma), \eta(p, \sigma))$$

פונקציה זו בעצם תעבוד על פי העיקרון הזה:



איור 2: עיקרון הפעולה של פונקציה φ

טענה 2.1.2. *φ מקיימת את הרעיון*

הוכחת טענה 2.1.2. נוכיח את הטענה באינדוקציה על $n = |w|$, כאשר $w \in \Sigma^*$.

מקרה הבסיס $n = 0$ המילה היחידה פה היא ε, ולכן ישירות מההגדרה של פונקציית המעברים המורחבת

$$\varphi^*((q_0, p_0), \varepsilon) = (q_0, p_0) = (\delta^*(q_0, \varepsilon), \eta^*(p_0, \varepsilon)$$

כנדרש.

המקרה הכללי נניח נכונות בעבור n ונוכיח עבור $n + 1$. עבור $w' \in \Sigma^{n+1}$ נכתוב $w' = w \cdot \sigma$. נכתוב $q \stackrel{\text{def}}{=\!=} \delta^*(q_0, w')$ ו־$p \stackrel{\text{def}}{=\!=} \eta^*(p_0, w')$. נחשב:

$$\begin{aligned}
\varphi^*((q_0, p_0), w') &= \varphi^*((q_0, p_0), w\sigma) \\
&= \varphi(\varphi^*((q_0, p_0), w), \sigma) \\
&\stackrel{\text{הנחת האינדוקציה}}{=\!=\!=} \varphi((\delta^*(q_0, w), \eta^*(p_0, w)), \sigma) \\
&\stackrel{\text{הגדרת } \varphi}{=\!=\!=} (\delta(\delta^*(q_0, w), \sigma), \eta(\eta^*(p_0, w), \sigma)) \\
&\stackrel{\text{הגדרת הפונקציה המורחבת}}{=\!=\!=\!=} (\delta^*(q_0, w'), \eta^*(p_0, w')) \\
&= (q, p)
\end{aligned}$$

כנדרש. $\square$

הצלחנו להגדיר את השפה על פי אוטומט סופי דטרמיניסטי, ולכן $L_1 \cup L_2$ רגולרית. $\square$

באותו אופן (על ידי החלפת הסימן $\vee$ בסימן $\wedge$ בהגדרת קבוצה H) נוכל להוכיח גם כי REG סגורה לחיתוך. אף על פעולות בינאריות אחרות, כמו XOR או הפרש!

הגדרה 2.1.8 (שרשור מילים). במידה ו־$v, w \in \Sigma^*$, נרשום $v \cdot w$ או vw בתור שרשור המילים.

הגדרה 2.1.9 (שרשור שפות). עבור $L_1, L_2 \subseteq \Sigma^*$ נגדיר

$$L_1 \circ L_2 \overset{\text{def}}{=\!=} \left\{ v \cdot w \middle|_{w \in L_2}^{v \in L_1} \right\}$$

נגדיר גם:

$$\forall n \in \mathbb{N}_0 : L^n \begin{cases} \{\varepsilon\} & n = 0 \\ L & n = 1 \\ L^{n-1} \circ L & n \geqslant 2 \end{cases}$$

ונסמן גם

$$L^* = \bigcup_{n=0}^{\infty} L^n$$

זה נקרא הסגור של קליני.

תרגיל 2.1.1. הוכיחו שחוקי חזקות בטבעיים עובדים על שרשורי שפות.

דוגמה 2.1.2. נסמן את השפות הבאות:

$$L_1 = \{w \in \{a,b\}^* \mid |w| \equiv 0 \bmod 3\}, \quad L_2 = \{w \in \{a,b\}^* \mid |w| \equiv 0 \bmod 2\}$$

מהו $L_1 \circ L_2$? במקרה הזה,

$$L_1 \circ L_2 = \{w \in \{a,b\}^* \mid |w| \in \{0, 2, 3, 4, 5 \ldots\}\}$$

שרשור היא רחוקה מפעולה פשוטה - זו פעולה מסובכת.

דוגמה 2.1.3. נסמן כעת $L_1 = \{a\}, L_2 = \{b\}$, השרשור שלהם הוא $L_1 \circ L_2 = \{ab\}$, בעוד סגור הקליני שלה הוא $(L_1 \circ L_2)^* = \{(ab)^n | n \in \mathbb{N}_0\}$

משפט 2.1.2. *מחלקת* REG *סגורה לפעולת השרשור ולסגור קליני*

לצורך זה נידרש להגדיר מחלקה חדשה, להוכיח את הטענה לגביה ולהוכיח כי היא זהה למחלקה REG

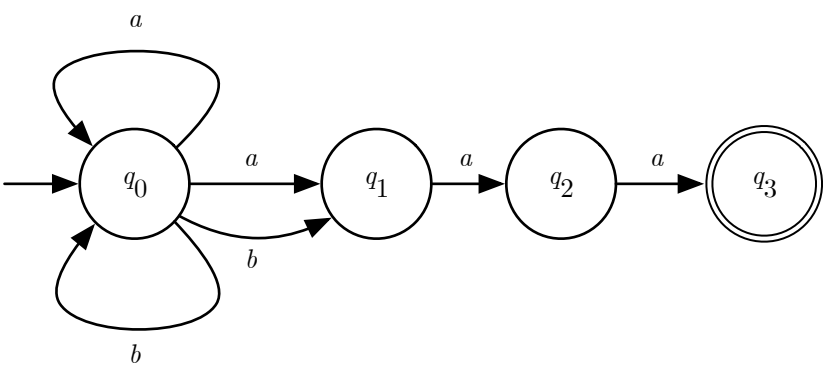
2.2 אי־דטרמיניזם

הגדרה 2.2.1 (שפות רגולריות לא דטרמיניסטיות). NREG היא קבוצת השפות אשר ניתן לזהות עם אוטומט סופי לא דטרמיניסטי

דוגמה 2.2.1 (לאוטומט סופי לא דטרמיניסטי). נגדיר את השפה הבאה:

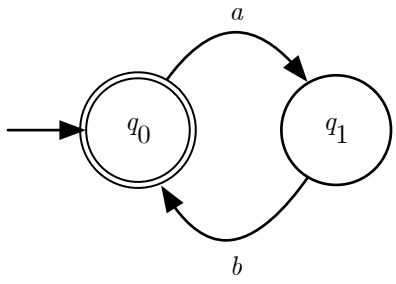
$$L_1 = \{w \in \{a,b\}^* \mid w \text{ ends with } aaa \text{ or } baa\}$$

להלן האוטומט שמזהה (לא מכריע!) את השפה:



איור 3: אוטומט $\mathcal{A}$ המגדיר את L_1

דוגמה 2.2.2. נוכל גם לעשות אוטומט לא דטרמיניסטי המזהה את $\{(ab)^n | n \in \mathbb{N}_0\}$:



איור 4: אוטומט $\mathcal{B}$ המגדיר את השפה בדוגמה

הגדרה 2.2.2 (אוטומט סופי לא דטרמיניסטי). $\mathcal{A}$ הוא אוטומט סופי לא דטרמיניסטי Nondeterministic finite automaton אם מתקיים

$$\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$$

כאשר:

1. Q היא קבוצת מצבים סופית
2. Σ היא א"ב
3. $\delta : (Q \times \Sigma) \to 2^Q$ היא פונקציית המעברים
4. $Q_0 \subseteq Q$ היא קבוצת המצבים ההתחלתיים האפשריים
5. $F \subseteq Q$ היא קבוצת המצבים המקבלים

הגדרה 2.2.3 (ריצה חוקית ב־NFA). ריצה חוקית של $\mathcal{A}$ על $w \in \Sigma^*$ היא סדרה $(s_i)_{i=0}^n$ המקיימת $s_0 \in Q_0$ ולכל $i > 0$ מתקיים $s_i \in \delta(s_{i-1}, w_i)$

דוגמה 2.2.3 (ריצות חוקיות של $\mathcal{A}$ מדוגמה 2.2.1 על baa). שלושת אלה הן ריצות חוקיות:

1. $q_0 \to q_0 \to q_0 \to q_0$
2. $q_0 \to q_1 \to q_2 \to q_3$
3. $q_0 \to q_0 \to q_0 \to q_1$

דוגמה 2.2.4 (ריצות חוקיות של $\mathcal{A}$ מדוגמה 2.2.1 על bbb). שתי אלה הן ריצות חוקיות:

1. $q_0 \to q_0 \to q_0 \to q_0$
2. $q_0 \to q_0 \to q_0 \to q_1$

הגדרה 2.2.4 (קבלת מילה על ידי $\mathcal{A}$). ריצה חוקית של $\mathcal{A}$ על w אם המצב הסופי בה הוא שייך ל־F. אומרים שמילה w מתקבלת על ידי $\mathcal{A}$ אם יש עבורה ריצה חוקית מקבלת של $\mathcal{A}$

הגדרה 2.2.5 (השפה של $\mathcal{A}$). השפה של $\mathcal{A}$ מוגדרת להיות

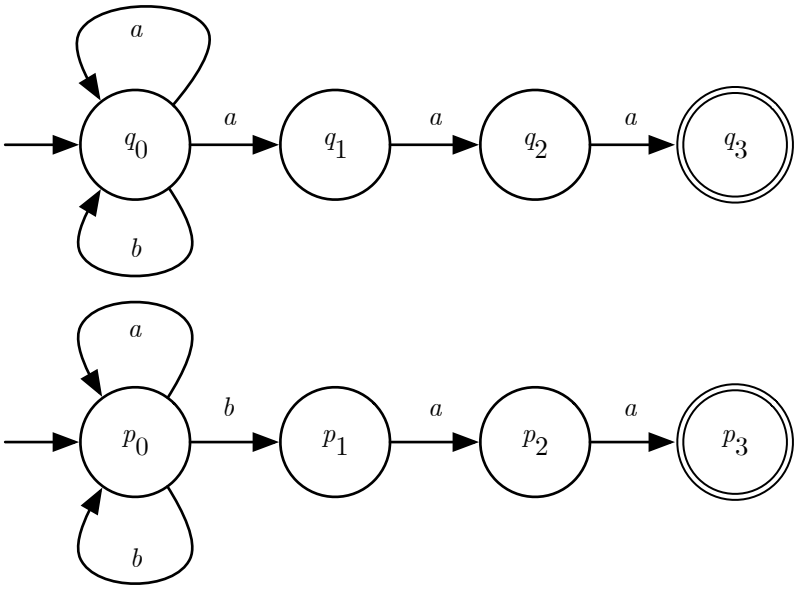
$$L(\mathcal{A}) = \{w \in \Sigma^* \mid w \text{ is accepted by } \mathcal{A}\}$$

$L(\mathcal{A})$ נקראת השפה המזוהה על ידי $\mathcal{A}$

דרך חשובה לחשוב על אוטומט לא דטרמיניסטי זה ככלי שאיתו מישהו יכול להוכיח כי מילה היא בשפה - ההוכחה ניתנת בזמן לינארי בהינתן פיתרון.

למרות שיש כאלה שקוראים ל־NFA מודל חישוב, הוא מתפקד יותר כמודל להוכחה.

דוגמה 2.2.5 (אוטומט אלטרנטיבי ל־L_1 מדוגמה 2.2.1). מדגים לנו שקל להשתמש בריבוי מצבים התחלתיים!



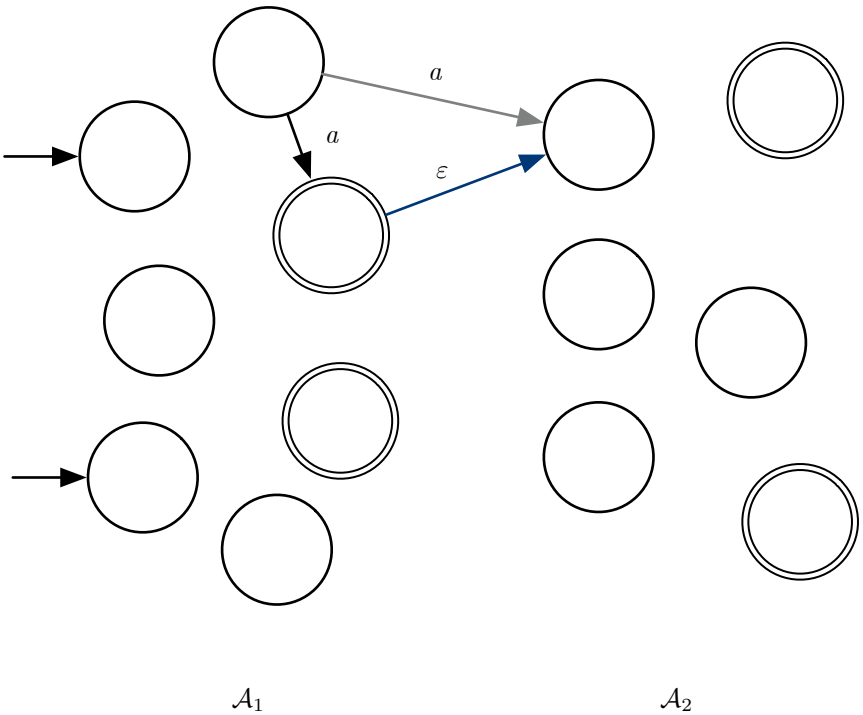
איור 5: דוגמה אלטרנטיבית לנ"ל

הגדרה 2.2.6 (הגדרה פורמלית ל-NREG). להלן הגדרה פורמלית:

$$\mathrm{NREG} = \{L \mid \text{there exists an NFA } \mathcal{A} \text{ such that } L(\mathcal{A}) = L\}$$

טענת עזר 2.2.1. *בהינתן* $L_1, L_2 \in \mathrm{NREG}$ *מעל* Σ *מתקיים כי* $L_1 \circ L_2 \in \mathrm{NREG}$

סקיצה להוכחה. אופציה אחת לה נוכל זה כי על כל אופציית מעבר למצב מקבל באוטומט הראשון תהיה לנו אפשרות להגיע לאחד המצבים המקבלים באוטומט השני. (באפור)
אופציה נוספת היא "קפיצה" ממצב מקבל לכל אחד מהמצבים ההתחלתיים האחרים. (בכחול)



איור 6: דוגמה עם שני "אוטומטים" ושני האפשרויות בצבעים שונים

□