מודלים חישוביים, חישוביות וסיבוכיות | 67521

הרצאות | פרופ׳ אורנה קופרמן

כתיבה | נמרוד רק

תשפ״ג סמסטר א׳

תוכן העניינים

שבוע $\mathbb{I}$ | מבוא לאוטומטים

הרצאה

חלק א' של ההרצאה

דוגמה נקפוץ לחלק האחרון של הקורס (סיבוכיות). בהינתן גרף לא מכוון $G = \langle V, E \rangle$, נרצה לדעת האם יש בו מעגל אוילר (כזה שעובר בכל צלע בדיוק פעם אחת).

אוילר הוכיח שיש מעגל כזה אם"ם דרגת כל הקודקודים זוגית, ולכן ניתן להכריע את הבעיה בזמן לינארית כי יש לבעיה אפיון מתמטי.

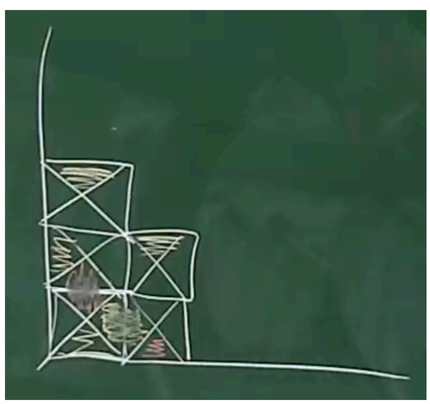
מעגל המילטון הוא מעגל שעובר בכל קודקוד בדיוק פעם אחת. לבעיה הזו אין אפיון מתמטי, והוכח שאין אלג' יותר טוב מאשר מעבר על כל האפשרויות, בסיבוכיות אקספוננציאלי.

דוגמה בהינתן $n = p \cdot q$, למצוא את p, q דורש זמן חישוב אקספוננציאלי באורך הייצוג, אפע"פ שהאלג' הוא לינארי במספר עצמו. זה משום שהפרמטר שלנו במקרה הזה הוא לא המספר אלא הייצוג (אנחנו מקבלים $\log n$ ספרות/אחדים ואפסים, לא את המספר במלואו).

דוגמה קלט: $\{t_i\}$ אריכים שלכל אחד מהם יש צלעות $\{l_i\}, \{r_i\}, \{d_i\}, \{u_i\}$ (למעלה, למטה, ימינה ושמאלה בהתאמה) כאשר הצלעות הם צבעים (אדום, צהוב, ירוק).

פלט: האם ניתן לרצף באופן חוקי ריבוע $n \times n$ לכל $n \geq 1$, כאשר "חוקיות" מתבטאת בכך שצלעות סמוכות מסכימות על הצבע.

דוגמת ריצה באופן אינטואיטיבי, במקרים מסוימים, נוכל להציב אחד מהאריכים בפינה, למצוא אילו אריכים מתאימים לו מבחינת הצלעות הסמוכות, להציב אריכים חוקיים נוספים, וכך לחזור חלילה. לעתים (כמו זה שבתמונה), נוצרת תבנית של אריכים חוקיים על האלכסון (כלומר אריך א' בפינה השמאלית התחתונה, ואז ב' מימינו ומעליו, ואז ג' מימין ומעל כל ב') ואז אפשר לגדום את התבנית האינסופית הזו לריבוע $n \times n$ כל פעם שצריך ולהחזיר ריבוע חוקי. במקרה כזה הפלט יהיה כן.



איור 1: דוגמה לתבנית שנוצרת, אפשר להמשיך לצייר את האלכסון בכיוון דרום-מזרח ולחזור על התבנית החוצה עוד ועוד

הבעיה היא שאין שום ערובה לכך שהתבנית באמת קיימת במקרה הכללי, או שהיא נשמרת, ואי אפשר לרוץ עד ∞. לכן התשובה היא שאין אלג' שפותר את הבעיה.

דוגמה (בעיית העצירה) קלט: תכנית מחשב P וקלט x.

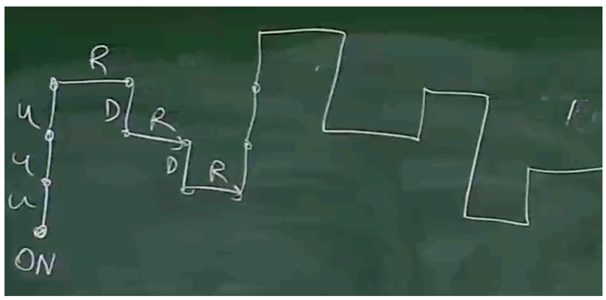
פלט: האם P עוצרת על x.

אין לבעיה זו אלג' שפותר אותה בכל המקרים (תחת הנחות מסוימות, אפשר לפעמים לתת תשובה).

אוטומטים

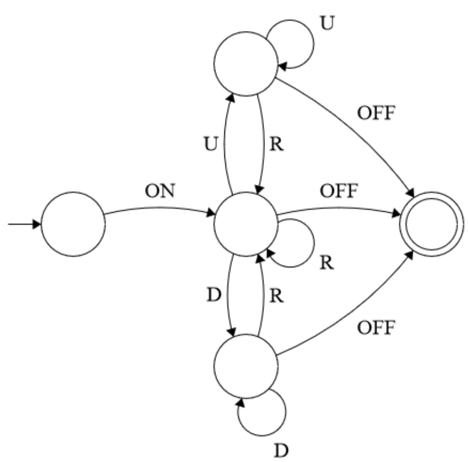
הגדרה <u>אוטומט</u> הוא מחשב עם זכרון מוגבל.

דוגמה נתון עט דיגיטלי שיכול לבצע אחת משש פקודות, $\text{ON, OFF, U, D, L, R}$. סדרת פקודות היא חוקית אם היא מתחילה ב-ON, מסתיימת ב-OFF ומייצרת קו רקיע משמאל לימין.



איור 2: דוגמה לקו רקיע חוקי, אסור ללכת שמאלה ואסור לעלות מיד אחרי שיורדים (ולהפך)

נכתוב אוטומט שמחליט האם סדרת פקודות היא חוקית. אם נצליח לעבור בין המצבים (העיגולים), החל מהמצב הראשון (זה עם חץ ללא מקור) ועד למצב המקבל (עם העיגול הכפול) על קשתות קיימות, הרי שהסדרה חוקית.



איור 3: אוטומט חוקי

אינטואיטיבית, המצב האמצעי הוא זה שממנו אפשר לעשות מה שרוצים, העליון הוא אחרי עלייה והתחתון הוא אחרי ירידה. נשים לב כי מכולם אפשר לפנות ימינה.

הגדרה אוטומט (automaton, DFA) הוא חמישייה $A = \langle Q, \Sigma, \delta, q_0, F\rangle$ שהם המצבים, הא"ב, פונקציית המעברים, המצב ההתחלתי וקבוצת המצבים המקבלים שמוכלת ב-Q.

- δ היא פ' $Q \times \Sigma \mapsto Q$.
- Σ היא קבוצה סופית של אותיות, לדוגמה $\Sigma = \{0,1\}, \{0,1\}^4$ וכו'.
- מילה היא $w = w_1, \dots, w_n$ סדרה סופית של אותיות, ו-ϵ היא המילה הריקה.
- שפה היא קבוצה של מילים, $L \subseteq \Sigma^*$ כאשר $\Sigma^* = \{w :$ w מילה סופית מעל הא"ב $\Sigma\}$.

דוגמה A_1 הוא האוטומט בציור. במקרה הזה $\Sigma = \{0,1\}$, $Q = \{q_0, q_1\}$, $F = \{q_0\}$ ופ' המעברים היא.

δ	0	1
q_0	q_0	q_1
q_1	q_1	q_0

הגדרה ריצה על מילה $w = w_1 \dots w_n$ מעל Σ היא סדרה של מצבים $r = r_0 \dots r_n$ כך ש:

- $r_0 = q_0$ (הריצה מתחילה ב-q_0).
- לכל $i \geq 0$, $r_{i+1} = \delta(r_i, w_{i+1})$ (הריצה מכבדת את δ).

דוגמה עבור A_1 והמילה 011, הריצה היא $q_0q_0q_1q_0$.

הגדרה r היא ריצה מקבלת (accepting) אם $r_n \in F$ (המצב האחרון בריצה הוא מקבל). אחרת, r הוא דוחה (rejecting).

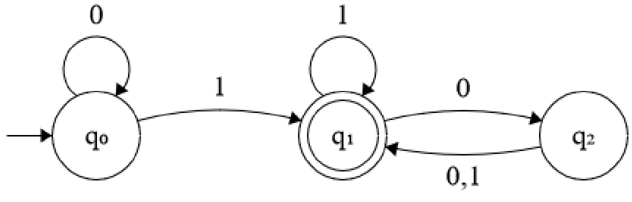
A מקבל את w אם הריצה של A על w היא מקבלת.

$L(A)$, השפה של האוטומט היא אוסף המילים ש-A מקבל עליהן.

דוגמה עבור A_1, $L(A_1) = \{w :$ מספר ה- 1 -ים ב-w הוא זוגי$\}$ (אפשר להוכיח באינדוקציה).

הערה אם לא קיים מעבר עבור אות ומצב, אפשר או להחליט ש-δ לא מוגדרת על כל $Q \times \Sigma$ או להחליט שכל קשת לא קיימת מובילה לבור דוחה, כלומר מצב לא מקבל שאי אפשר לצאת ממנו.

דוגמה נצייר אוטומט נוסף, A_2, ונחשב את השפה שלו.



איור 4: האוטומט A_2

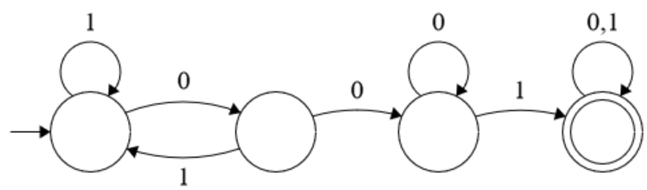
נסמן בצבע האם כמה מילים נבחרות הן בשפה או לא, 00000, 11, 1, 001110, 011, 010.

אם נחשוב עוד קצת, נגלה ש-

$$L(A_2) = \{w : \text{יש ב- } w \text{ לפחות 1 אחד, ואחרי ה-1 האחרון יש מספר זוגי (או אפס) של 0-ים}\}$$

בתרגול נוכיח את זה באופן פורמלי.

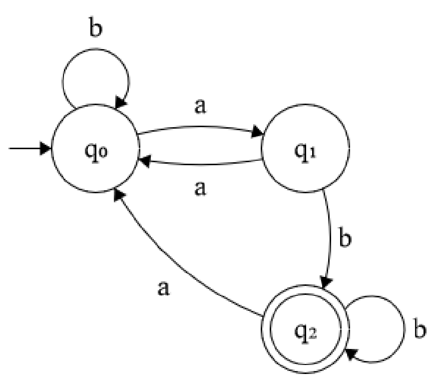
דוגמה בהינתן שפה, ננסה לחשב את האוטומט. השפה היא $L_3 = \{w : 001 \text{ מכילה את הרצף } w\}$.



איור 5 : אוטומט שנגזר מ-L_3

חלק ב' של ההרצאה

דוגמה $\Sigma = \{a, b\}$, $L = \{w : \#_a w \text{ אי זוגי } \wedge w_n = b\}$ (כאשר $\#_a w$ הוא מספר ה-a-ים ב-w ו-w_n האות האחרונה במילה).



איור 6 : אוטומט שאנחנו טוענים שנגזר מ-L

המצב ההתחלתי לא מקבל כי $\epsilon \notin L$. b כאות ראשונה לא מקדם אותנו כי זו לא מילה חוקית. הרעיון בהלוך-חזור ב-q_0, q_1 הוא שרק אם המספר הוא אי זוגי של a-ים, נגיע ל-q_1 ומשם נעצור במצב מקבל רק אם אנחנו נגמרים ב-b.

לכל מצב נוכל להתאים סטטוס - מה מאפיין את המילה שמגיעה אליו (לאחר מכן נשתמש בסטטוסטים האלה, נפרמל אותם ונוכיח איתם את נכונות האוטומט):

- q_0 - $\#_a w$ זוגי.
- q_1 - $\#_a w$ אי זוגי ו-w מסתיימת ב-a.
- q_2 - $\#_a w$ אי זוגי ו-w מסתיימת ב-b.

טענה $L(A) = L$.

הוכחה: $\forall w \in \Sigma^*$ (אוסף המילים האפשריות) מתקיים $\delta^*(q_0, w) = q_0$ (כאשר $\delta^* : Q \times \Sigma^* \mapsto Q$, כלומר הפעלה שוב ושוב של δ על המילה החל ממצב נתון).

נוכיח את שלוש הטענות הבאות ומשם ינבע כי

$$w \in L \iff \delta^*(q_0, w) = q_2 \iff \delta^*(q_0, w) \in F$$

האם"ם נובע משתי הטענות הראשונות, הטענה השלישית מספקת לנו רק כיוון אחד.

1. אם $\delta^*(q_0, w) = q_0$ אז $\#_a w$ זוגי.
2. אם $\delta^*(q_0, w) = q_1$ אז $\#_a w$ אי זוגי ו-w מסתיימת ב-a.
3. אם $\delta^*(q_0, w) = q_2$ אז $\#_a w$ אי זוגי ו-w מסתיימת ב-b.

באינדוקציה על $|w|$:

בסיס ($|w| = 0$): $w = \epsilon$ ולכן $\delta^*(q_0, \epsilon) = q_0$ ואכן $\#_a \epsilon$ זוגי.

צעד ($|w| \to |w| + 1$): נוכיח את הטענה על $w \cdot a, w \cdot b$ בהנחה שהיא נכונה על w. נוכיח רק את המקרה של $w \cdot a$ ונשאיר לסטודנטית המשקיעה להוכיח את המקרה השני.

- אם $\delta^*(q_0, w \cdot a) = q_0$ אז בהכרח $\delta^*(q_0, w) \in \{q_1, q_2\}$ ($\delta(q_0, a) \neq q_0$) ולכן מה"א $\#_a w$ אי זוגי (מטענות 2 ו-3) ולכן $\#_a w \cdot a$ זוגי.
  - אם $\delta^*(q_0, w \cdot a) = q_1$ אז $\delta^*(q_0, w) = q_0$ ומה"א $\#_a w$ זוגי ולכן $\#_a w \cdot a$ אי זוגי ו-w נגמרת ב-a.
  - אם $\delta^*(q_0, w \cdot a) = q_2$ אז זה לא ייתכן (מהגדרת האוטומט).

■

דוגמה $\Sigma = \{a, b\}$, $L = \{w : \#_a w = \#_b w\}$. אין אוטומט סופי ששפתו L! זה בגלל שאחרי ה-a הראשון, נצטרך "לזכור" שיש לנו 1 לטובת a, ואז אם שוב יש a נצטרך לזכור עוד 1, ואם b אז אחד לטובת b וזה אינסופי בעצם.

הגדרה שפה רגולרית היא שפה שניתנת לזיהוי ע"י אוטומט, ונסמן $L \in \mathrm{REG}$, פורמלית, L היא רגולרית אם קיים DFA כך ש-$L = L(A)$.

פעולות על שפות

תהיינה $L_1, L_2 \in \Sigma^*$. כל הפעולות עובדות על שפות מעל $\Sigma_1 \neq \Sigma_2$ ובמקרה כזה נסמן $\Sigma = \Sigma_1 \cup \Sigma_2$.

1. איחוד (union): $L_1 \cup L_2 = \{w : w \in L_1 \vee w \in L_2\}$ (שפות הן קבוצות, זו לא פעולה חדשה).
2. שרשור (concatenation): $L_1 \cdot L_2 = \{w_1 \cdot w_2 : w_1 \in L_1, w_2 \in L_2\}$ (הצמדה של כל צמד מילים משתי השפות).
3. כוכב (star): $L^* = \{w_1 \cdot \ldots \cdot w_k : k \geq 0 \wedge w_i \in L, \forall i \leq k\}$ (שרשור של 0 או יותר מילים ב-L כולל את ϵ עבור $k = 0$).

דוגמה $L_1 = \{1, 333\}, L_2 = \{22, 4444\}$.

$$L_1 \cup L_2 = \{1, 333, 22, 4444\}$$
$$L_1 \cdot L_2 = \{122, 1444, 33322, 3334444\}$$
$$L^* = \{\epsilon, 1, 333, 11, 1333, 3331, 333333, ...\}$$

הערה אם $L = \varnothing$ אז $L^* = \{\epsilon\}$ וכך גם עבור $L = \{\epsilon\}$. כל שפה אחרת היא אינסופת (יש לפחות מילה אחת לא ריקה, נשרשר אותה כמה פעמים שרק נרצה).

תרגול

הגדרה נאמר כי $R \subseteq S \times T$ הוא יחס מעל S, T (לרוב $S = T$).

דוגמה $A = \{1, 2, 3, 4\}$, $R = \{(a, b) : |a - b| \leq 1\}$.

תכונות של יחסים

- רפלקסיביות: $\forall a \in A$, $(a, a) \in A$ או בסימון חלופי, aRa (היחס הנ"ל הוא רפלקסיבי).
- סימטריה: $\forall a, b \in A$, אם aRb אז bRa (היחס הנ"ל הוא סימטרי).
- טרנזיטיביות: $\forall a, b, c \in A$, אם aRb ו-bRc אז aRc.

- יחס שקילות: יחס שמקיים את שלושת הנ"ל.

יחס שקילות R מעל A מחלק את A למחלקות שקילות זרות המוגדרות ע"י $[a]_R = \{b \in A : aRb\}$, כי אם קיים $x \in [a]_R \cap [b]_R$ אבל $[a]_R \neq [b]_R$ אז קיים $c \in [a]_R \setminus [b]_R$ ולכן

$$aRc \Rightarrow cRx \Rightarrow cRb \Rightarrow c \in [b]_R$$

סתירה.

דוגמה $G = \langle V, E \rangle$ גרף לא מכוון והיחס $R \subseteq V \times V$ שמשמעותו "כל זוגות הקודקודים שיש ביניהם מסלול ב-G". קל לראות שזהו יחס רפלקסיבי, טרנזיטיבי וסימטרי ולכן זהו יחס שקילות.

הגדרה עוצמה של קבוצה היא מדד ל"גודל" הקבוצה. עבור קבוצה סופית A, העוצמה שלה היא $|A|$.

הגדרה $|\mathbb{N}| = \aleph_0$.

הערה ראינו ש-$\aleph_0 = |\mathbb{Q}| = |\mathbb{Z}|$ (כאשר שוויון עוצמות משמעו קיום פ' חחע"ל בין שתי הקבוצות).

הערה נאמר כי $|A| \leq |B|$ אם יש העתקה חח"ע מ-A ל-B ו-$|A| < |B|$ אם בנוסף אין העתקה חח"ע מ-A על B.

טענה (האלכסון של קנטור) $|[0,1]| = 2^{\aleph_0} > \aleph_0$.

הגדרה $\Sigma^n = \underbrace{\Sigma \times \ldots \times \Sigma}_{n \text{ פעמים}}$ ונגדיר $\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n$.

הערה רבים מתבלבלים כאן אבל חשוב לזכור ש-Σ סופית וכך גם Σ^n, אבל Σ^* אין סופית.

דוגמאות לשפות

$\Sigma = \{a, b\}$.

- $L_1 = \{\epsilon, a, aa, b\}$.
- $L_2 = \{w : w_1 = a\}$ (מילים שמתחילות ב-a).
- $L_3 = \{\epsilon\}$.
- $L_4 = \varnothing$ וזו אינה אותה קבוצה כמו L_3!
- $L_5 = \{w : |w| < 24\}$.

- $L_1 = \{w : w_1 = a\}$ ו-$L_2 = \{w : w_n = b\}$ (סימון לקוני למילים שמסתיימות ב-b). שפה נוספת היא

$$L_1 \cup L_2 = \{w : w_1 = a \vee w_n = b\}$$

$$L_2 \cdot L_1 = \{w : \text{מכילה את הרצף } ab\ w\}$$

$$L_1 \cap L_2 = \{w : w_1 = a \wedge w_n = b\}$$

$$L_1 \cdot L_2 = L_1 \cap L_2$$

כאשר השוויון האחרון נכון כי המילה הראשונה בצמד מתחילה ב-a והשנייה נגמרת ב-b ובאמצע לא משנה מה יש, בדומה ל-$L_1 \cap L_2$.

- $L = \{ww : w \in \Sigma^*\}$.

$$\overline{L} = \Sigma^* \backslash L = \{w : 2 \nmid |w|\} \cup \{w = w_1 \ldots w_{2n} : w_1, \ldots, w_n \neq w_{n+1} \ldots w_{2n}\}$$

$$L \cdot L = \{wwxx : w, x \in \Sigma^*\}$$

הערה כל שפה מקיימת $L \subseteq \Sigma^*$, או באופן שקול $L \in P(\Sigma^*)$.

כמה מילים יש ב-Σ^*? $|\Sigma^*| = \aleph_0$.

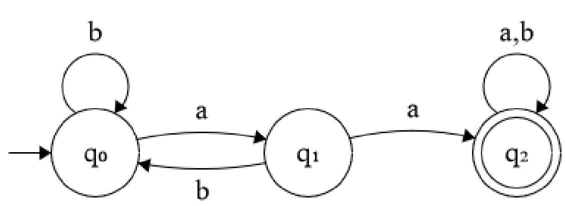
כמה שפות יש מעל Σ^*? $2^{|\Sigma^*|} = 2^{\aleph_0}$.

כמה שפות רגולריות יש מעל Σ^*? $\aleph_0$, כי כל אוטומט מוגדר ע"י מחרוזת מעל א"ב סופי (המצבים, הא"ב של האוטומט וכו') ולכן מהנ"ל עוצמת אוסף המחרוזות ששקולות לאוטומטים היא $\aleph_0$. לחלופין, כל אוטומט אפשר לצייר ויש מספר בן מנייה של פיקסלים על canvas (במחשב).

מסקנה קיימות שפות לא רגולריות, ויש "יותר" לא רגולריות מאשר לא (השפות הרגולריות הן קבוצה במידה 0 מתוך כל השפות).

הגדרה בהינתן אוטומט A, נגדיר
$$\delta^*(q, w) = \begin{cases} q & w = \epsilon \\ \delta(\delta^*(q, w'), \sigma) & w = w'\sigma, \sigma \in \Sigma \end{cases}.$$

דוגמה נביט באוטומט הבא.



איור 7: אוטומט לדוגמה

נחשב ערך של δ^*.

$$\delta^*(q_1, ba) = \delta(\delta^*(q,b), a) = \delta(\delta(\delta^*(q,\epsilon), b), a) = q_1$$

.

דוגמה עבור $\Sigma = \{0, \ldots, 9, \#\}$ והשפה

$$L = \left\{x\#a : x \in \{0, \ldots, 0\}^*, a \in \{0, \ldots, 9\}, a \in x\right\}$$

נמצא את האוטומט המתאים ל-L. ראשית נשים לב לדוגמה כי $64424\#5 \notin L$ אבל $1243\#2 \in L$.

הבעיה באוטומט זה שאין לנו זיכרון ולכן נצטרך "לזכור" מספיק מידע כדי לזכור האם ראינו # עד עכשיו ואילו ספרות ראינו עד כה.

נבחר $Q = \left(2^{\{0,\ldots,9\}} \times \{1,2\}\right) \cup \{q_{acc}, q_{sink}\}$ כאשר מצב מייצג את אוסף הספרות שראינו עד כה והאם ראינו את סולמית עד עכשיו (2 כן ראינו).

$q_0 = \langle \varnothing, 1\rangle$ כלומר לא ראינו את סולמית ולא ראינו אף ספרה, $F = \{q_{acc}\}$ ו-$\Sigma = \{0, \ldots, 9, \#\}$.

$$\delta(\langle c, i\rangle, \sigma) = \begin{cases} \langle c \cup \{\sigma\}, 1\rangle & \sigma \in \{0, \ldots, 9\}, i = 1 \\ \langle c, 2\rangle & \sigma = \#, i = 1 \\ q_{acc} & \sigma \in c, i = 2 \\ q_{sink} & \sigma \notin c, i = 2 \end{cases}$$

עברו על כל המצבים והבינו את המשמעות, הרעיון בסוף הוא שאם ראינו סולמית ונתקלנו באות נוספת, נקבל או נשלול בהתאם להאם ראינו את הספרה או לא. לשם השלמות גם נגדיר $\delta(q_{acc}, \sigma) = \delta(q_{sink}, \sigma) = q_{sink}$ כי אם הגענו למצב המקבל והוספנו עוד תו זה כבר לא בשפה.

טענת עזר בהינתן $w \in \{0, \ldots, 9\}^*$, נגדיר $S(w) = \left\{\sigma \in \{0, \ldots, 9\}^* : w \text{ מופיעה ב- } \sigma\right\}$ (אוסף הספרות שמופיעות ב-w). נוכיח כי $\delta^*(q_0, w) = \langle S(w), 1\rangle$.

הוכחה: באינדוקציה על $|w|$.

בסיס ($w = \epsilon$): $\delta^*(q_0, w) = \delta(q_0, \epsilon) = \langle \varnothing, 1\rangle$ כנדרש.

צעד ($|w| - 1 \to |w|$): נסמן $w' = w\sigma$

$$\delta^*(q_0, w') = \delta(\delta^*(q_0, w), \sigma) \overset{\text{ה"א}}{=} \delta(\langle S(w), 1\rangle, \sigma) = \langle S(w'), 1\rangle$$

■

טענה $L = L(A)$.

הוכחה: נוכיח הכלה דו-כיוונית באינדוקציה על אורך המילה; זו דרך ההוכחה המקובלת לטענות על שפות ואוטומטים.

$L \subseteq L(A)$: נניח כי $w \in L$ ונראה שריצה של A על w מקבלת. $w = x\#a$ כאשר $x \in [0, \ldots, 9]^*$, $a \in \{0, \ldots, 9\}$ ו-$a \in S(x)$.

$$\begin{aligned} \delta^*(q_0, w) &= \delta(\delta^*(q_0, x\#), a) \\ &= \delta\left(\delta\left(\underbrace{\delta^*(q_0, x)}_{\langle S(x), 1\rangle}, \#\right), a\right) \\ \text{הגדרת } \delta \quad &= \delta(\langle S(x), 2\rangle, a) \\ \text{הגדרת } \delta \quad &= q_{acc} \end{aligned}$$

$L(A) \subseteq L$: מספיק שנוכיח שאם $w \notin L$ אז $w \notin L(A)$. נעבור על כל המילים $w \notin L$.

- אם $w \in \{0, \ldots, 9\}^*$ אז מטבענת העזר $\delta(q_0, w) = \langle S(w), 1\rangle \neq q_{acc}$.
- אם $w \in \{0, \ldots, 9\}^* \times \{\#\}$ אז

$$\delta^*(q_0, w) = \delta\left(\underbrace{\delta^*(q_0, w)}_{\langle S(x), 1\rangle}, \#\right) = \langle S(x), 2\rangle \neq q_{acc}$$

- אם $w = x\#y$ עבור $|y| > 1$ אז

$$\delta^*(q_0, w) = \delta^*(\langle S(x), 2\rangle, y) \neq q_{acc}$$

כאשר השוויון נובע מכך שניתן לפצל את הריצה על $x\#$ ואז על y. הריצה על $x\#$ מביאה אותנו ל-$\langle S(x), 2\rangle$ מהגדרה של δ. האי-שוויון נובע מכך ש-$|y| > 1$ ולכן גם אם אחרי הספרה הראשונה של y הגענו ל-q_{acc}, בהכרח כל הספרות האחרות יובילו אותנו תמיד לבור דוחה.

- אם $w = x\#a$ אבל $a \notin S(x)$ אז

$$\begin{aligned} \delta^*(q_0, w) &= \delta(\delta(\delta^*(q_0, x), \#), a) \\ &= \delta(\langle S(x), 2\rangle, a) \\ a \notin S(x) \quad &= q_{sink} \end{aligned}$$

■

שבוע III | אוטומטים אי-דטרמיניסטיים

הרצאה

חלק א' של ההרצאה

משפט השפות הרולגריות סגורות לאיחוד, כלומר, אם $L_1, L_2 \in \mathrm{REG}$ אז $L_1 \cup L_2 \in \mathrm{REG}$.

הוכחה: בהינתן DFA-ים $A_1 = \langle Q_1, \Sigma, \delta_1, s_1, F_1 \rangle, A_2 = \langle Q_2, \Sigma, \delta_2, s_2, F_2 \rangle$, נבנה $A = \langle Q, \Sigma, \delta, s_0, F \rangle$ שעבורו $L(A) = L(A_1) \cup L(A_2)$.

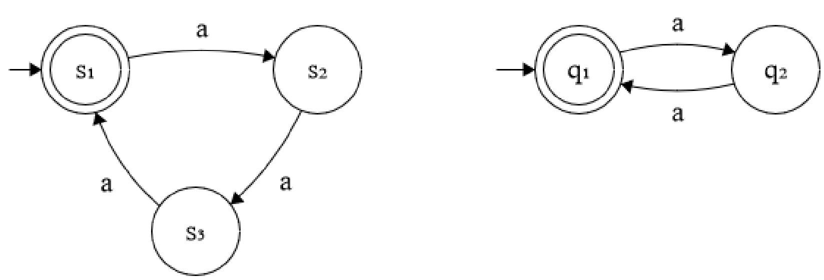
הרעיון הוא ש-A מסמלץ את A_1 ו-A_2 יחד, ואוטומט בבנייה כזו נקרא אוטומט המכפלה. נבחר $Q = Q_1 \times Q_2$, $s_0 = \langle s_1, s_2 \rangle$, ופ' מעברים

$$\delta(\langle q_1, q_2 \rangle, \sigma) = \langle \delta_1(q_1, \sigma), \delta(q_2, \sigma) \rangle$$

כאשר אנחנו מניחים ש-A_1, A_2 לא נתקעים כי אפשר להוסיף בור דוחה במקרה הצורך.

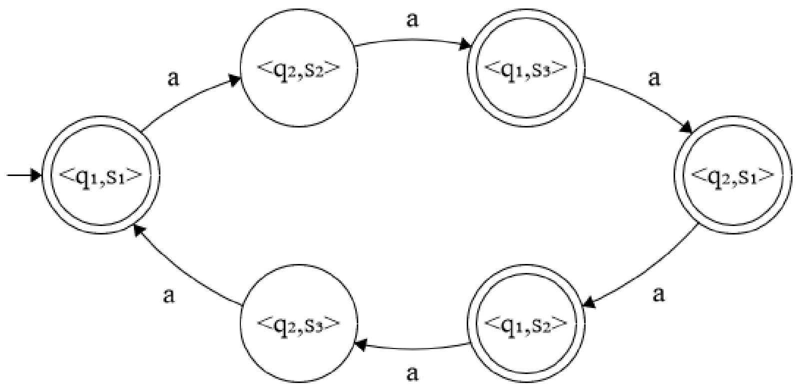
הערה אם $L \subseteq \{a\}^*$ אז היא מגדירה תת קבוצה של $\mathbb{N}$ - כל האורכים של מילים בשפה, כלומר $\{i : a^i \in L\}$.

דוגמה נבחר את האוטומטים A_1, A_2 כבתמונה,



איור 8: האוטומטים A_1 (מימין) ו-A_2 (משמאל)

במקרה הזה, אוטומט המכפלה יראה כבאיור, כאשר בכל מעבר אנחנו "צועדים" קדימה גם במצבים של A_1 וגם בשל A_2.



איור 9 : A אוטומט המכפלה

ולא קשה לראות שהאוטומט מקבל על מספרים זוגיים וכאלה שמתחלקים בשלוש, כלומר $L(A)=\{w:|w| \mod 2=0 \vee |w| \mod 3=0\}$.

הערה מהדוגמה הנ"ל ניתן לראות שאם היינו רוצים לבנות אוטומט שהשפה שלו היא $L(A_1)\cap L(A_2)$ היינו בוחרים

$$F=\{\langle q_1,q_2\rangle : q_1\in F_1 \wedge q_2\in F_2\}$$

כאשר ההבדל כאן הוא "וגם" במקום "או" על המצבים המקבלים.

הערה אם היינו רוצים A עם $L(A)=\Sigma^*\backslash L(A_1)$, מספיק שהיינו מגדירים $A=\langle Q_1,\Sigma,\delta_1,s_1,Q_1\backslash F_1\rangle$ כי הריצה מגיעה ל-$Q_1\backslash F_1$ אם"ם A_1 דוחה את w.

נוכיח כי $L(A)=L(A_1)\cup L(A_2)$. תהי $w=w_1w_2\dots w_n$ מילה ב-Σ^* ותהי $r=r_0r_1\dots r_n$ הריצה של A על w. נסמן $r_i=\left\langle q_1^i,q_2^i\right\rangle$.

מהגדרת A, $q_1^0=s_1, q_2^0=s_2$ ולכן $i\geq 0$,

$$q_1^{i+1}=\delta_1\left(q_1^i,w_i\right), q_2^{i+1}=\delta_2\left(q_2^i,w_i\right)$$

ולכן $\rho_1=q_1^0,q_1^1,\dots,q_1^n$ היא ריצה של A_1 על w ובהתאמה $\rho_2=q_2^0,q_2^1,\dots,q_2^n$ היא ריצה של A_2 על w.

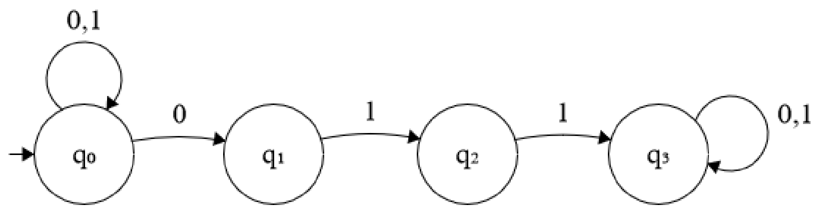
מכאן, r מקבלת אם"ם $\langle q_1^n,q_2^n\rangle\in F$ אם"ם $q_1^n\in F_1$ או $q_2^n\in F_2$ אם"ם r_1 מקבלת או r_2 מקבלת אם"ם $w\in L(A_1)$ או $w\in L(A_2)$.

■

הערה בדרך להוכחה ש-REG סגור לשרשור, נתקעים בקושי הוכחתי. לכאורה נפרק מילה לשני החלקים, נריץ כל חלק באוטומט המתאים לו ונסיים. הבעיה היא שלכל מילה יכולים להיות כמה פירוקים. לשם כך נצטרך "לנחש" מתי לקפוץ.

אוטומטים אי-דטרמיניסטיים

דוגמה נביט באוטומט הבא,



איור 10 : אוטומט אי-דטרמיניסטי

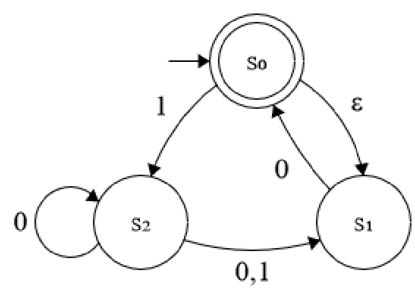
לכאורה פ' המעברים לא מוגדרת היטב עבור $q_0, 0$, אבל כאן הרעיון הוא שהאוטומט יכול לבחור מתוך כמה אפשרויות בעצמו לאיזה מצב הוא עובר, כאשר מילה מתקבלת ע"י האוטומט אם"ם קיימת ריצה עם ניחושים כלשהם שמקבלת, ובמקרה כזה נגדיר $\delta\left(q_0, 0\right) = \{q_0, q_1\}$.

הגדרה <u>אוטומט אי-דטרמיניסטי</u> הוא אוטומט שבו פ' המעברים ממפה מצב ואות (או אפסילון) לקבוצה של מצבים עוקבים אפשריים, כלומר

$$\delta : Q \times (\Sigma \cup \{\epsilon\}) \to 2^Q$$

ומילה מתקבלת אם"ם קיימת ריצה מקבלת של A על המילה.

דוגמה נביט באוטומט הבא עם "צעד אפסילון",



איור 11 : אוטומט אי-דטרמיניסטי עם "צעד אפסילון"

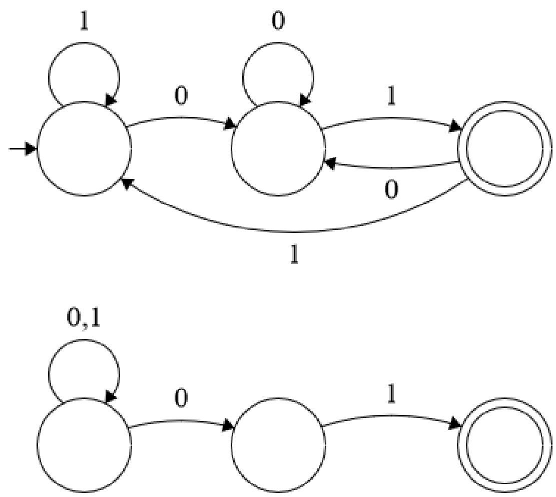
המילים הבאות מתקבלות : $\epsilon, 0, 00, 00110$ (כי נוכל להשתמש קודם בצד אפסילון במקום ליפול לבור דוחה מ-s_0) ואילו $001, 00111$ לא מתקבלות.

הגדרה <u>אוטומט אי-דטרמיניסטי</u> הוא חמשייה מהצורה $A = \langle Q, \Sigma, \delta, Q_0, F \rangle$ שעבורה $Q_0 \subseteq Q$ (יכולים להיות כמה מצבים התחלתיים) ו-$\delta : Q \times (\Sigma \cup \{\epsilon\}) \to 2^Q$.

ריצה של A על מילה $w=\sigma_1\sigma_2\ldots\sigma_n$ היא סדרת מצבים $r=r_0r_1\ldots r_m$ (כאשר $m\geq n$ בגלל ריפודי אפסילון) כך שניתן לכתוב את w כ-$w'=x_1x_2\ldots x_m$ כאשר $x_i\in\Sigma\cup\{\epsilon\}$ ומתקיים $r_0\in Q_0$ וכן $r_{i+1}\in\delta\left(r_i,x_{i+1}\right)$ ($\in$ בניגוד ל-$=$ ב-DFA). בנוסף, r מקבלת אם"ם $r_m\in F$.

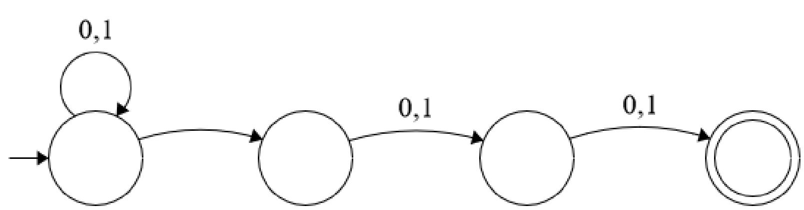
נאמר כי A מקבלת את w אם"ם קיימת ריצה של A על w שמקבלת.

דוגמה NFA מעל $\Sigma=\{0,1\}$. $L=\{w:0,1$ מסתיימת ב- $w\}$, באיור למעלה DFA שהשפה שלו היא L ולמטה NFA שקול (ויותר פשוט),



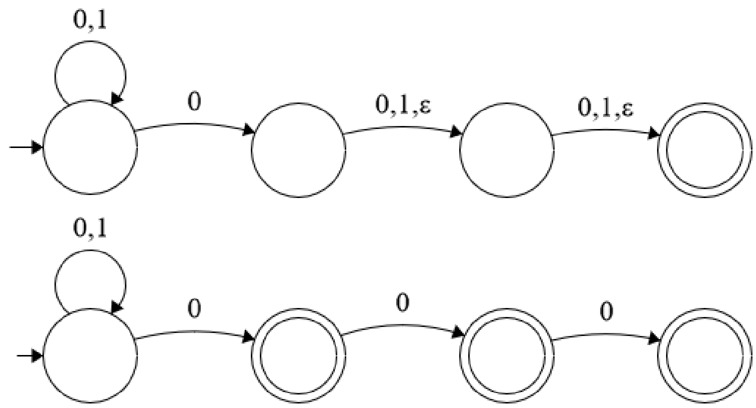
איור 12 : אוטומט דטרמיניסטי (למעלה) ואי-דטרמיניסטי (למטה) שמשרתים אותה המטרה

דוגמה עבור $L=\{w:0\left(0+1\right)\left(0+1\right)$ מסתיימת ב- $w\}$, האוטומט הבא מקבל אם"ם מילה היא ב-L (הוכחה פורמלית פשוטה בעל פה),



איור 13 : אוטומט עם השפה הנ"ל

דוגמה עבור $L'=\{0$ במקום הלפני לפני אחרון, הלפני אחרון או האחרון$\}$, האוטומטים הבאים הם בעלי השפה L',



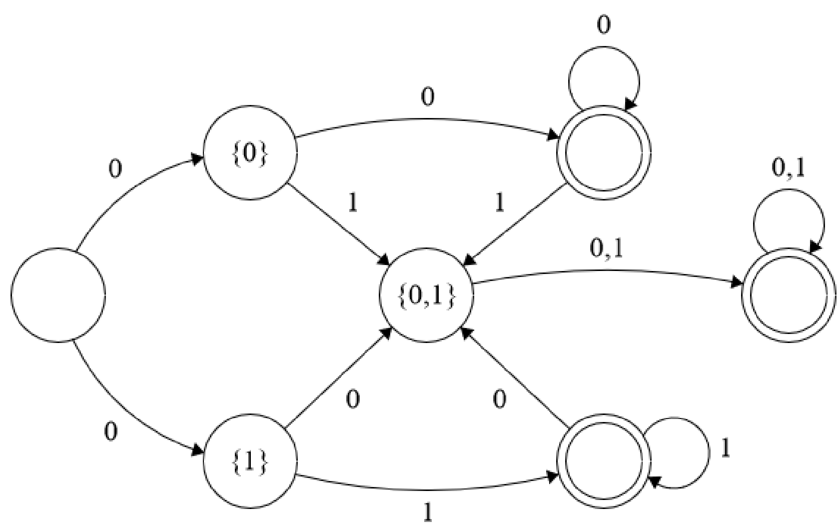
איור 14 : שני אוטומטים אי-דטרמיניסטיים ששפתם L'

דוגמה מצבים התחלתיים רבים הם שימושיים לדוגמה במקרה של אוטומט המכפלה, שם אם היינו יכולים להגדיר כמה מצבים התחלתיים יכולנו לעשות בניה יותר פשוטה עם $Q = Q_1 \cup Q_2$.

ההוכחה למשפט בסוף ההרצה עבר לתחילת חלק ב' של ההרצאה.

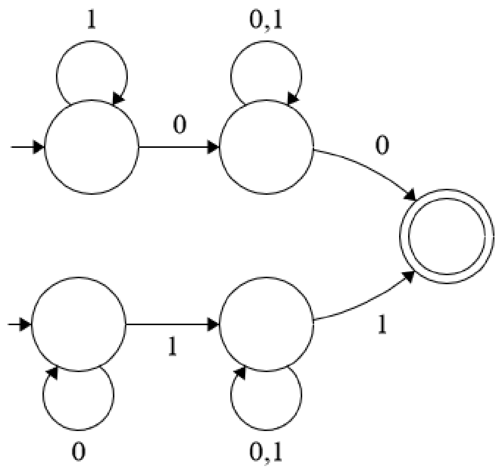
חלק ב' של ההרצאה

דוגמה L היא השפה שבה כל המילים שבהן האות האחרונה הופיע לפניכן במילה, מעל $\Sigma = \{0, 1\}$. ראו DFA שמתאים לה באיור,



איור 15 : DFA שמתאים ל-L

ועתה NFA מתאים (שקול), כאשר הרעיון כאן הוא שהחלק העליון מתאים לריצה שבה יש 0 אחד לפחות ובסוף 0 ולמטה זו כזו בהתאם שמסתיימת ב-1.



איור 16: NFA שמתאים ל-L

משפט לכל NFA A קיים DFA A' שקול כך ש-$L(A) = L(A')$.

הוכחה: בהינתן $A = \langle Q, \Sigma, Q_0, \delta, F \rangle$, נבנה $A' = \langle Q', \Sigma, q_0', \rho, F' \rangle$ כך ש-$L(A) = L(A)'$. נבחר $Q' = 2^Q$ ואז הרעיון הוא ש-A' מגיע למצב S בריצה אחרי קריאת w אם"ם A יכול להגיע לבדיוק כל המצבים ב-S אחרי קריאת w.

באופן אינדוקטיבי, δ^* מוגדרת ע"י $s = \delta^*(s, \epsilon)$, $\delta^*(S, \sigma) = \bigcup_{s \in S} \delta(s, \sigma)$ ובצעד ה-n-י, $\delta^*(S, w \cdot \sigma) = \delta^*(\delta^*(S, w), \sigma)$.

נבחר $q_0' = Q_0$ שהוא קבוצה, אבל $q_0' \in Q'$ כי Q' זו קבוצה של קבוצות ולכן זה בסדר.

נגדיר $\rho(S, \sigma) = \bigcup_{s \in S} \delta(s, \sigma)$ לכל $s \in Q'$ ו-$\sigma \in \Sigma$.

טענה לכל $w \in \Sigma^*$ מתקיים $\rho^*(q_0', w) = \delta^*(Q_0, w)$ או במילים, המצב ב-A' ש-A' מגיע אליו אחרי קריאת w (המצב הוא קבוצה בפני עצמו), שווה לקבוצת המצבים ש-A יכול להיות בה (באחת הריצות שלו) על A.

נבחר $F' = \left\{ S \in 2^Q : S \cap F \neq \varnothing \right\}$ כי אנחנו מקבלים אם הגענו למצב ב-Q' שאחד מ(תתי-)המצבים שבו הם מקבלים (כי זה אומר שאנחנו יכולים להגיע אליו בריצה כלשהי של A').

נוכיח כי $L(A) = L(A')$. $w \in L(A)$ אם"ם קיימת ריצה מקבלת של A על w אם"ם $\delta^*(Q_0, w) \cap F \neq \varnothing$ אם"ם (עכשיו נוכיח) $\rho^*(q_0', w) \in F'$ אם"ם $w \in L(A)$.

הוכחה: (של הטענה המקוננת) באינדוקציה על w:

בסיס $(w = \epsilon)$: $\rho^*(q_0', \epsilon) = q_0' = Q_0 = \delta^*(Q_0, \epsilon)$.

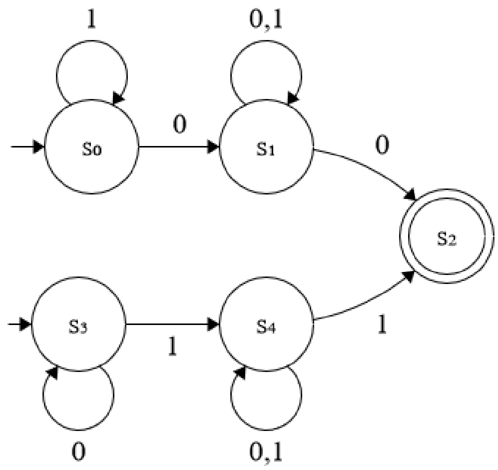
צעד $(|w| \to |w + 1|)$:

$$\rho^*(q_0', w \cdot \sigma) = \rho(\rho^*(q_0', w), \sigma) \overset{\text{הגדרת } \delta}{=} \delta^*(\rho^*(q_0', w)) \overset{\text{ה"א}}{=} \delta^*(\delta^*(Q_0, w), \sigma) = \delta^*(Q_0, w \cdot \sigma)$$

■

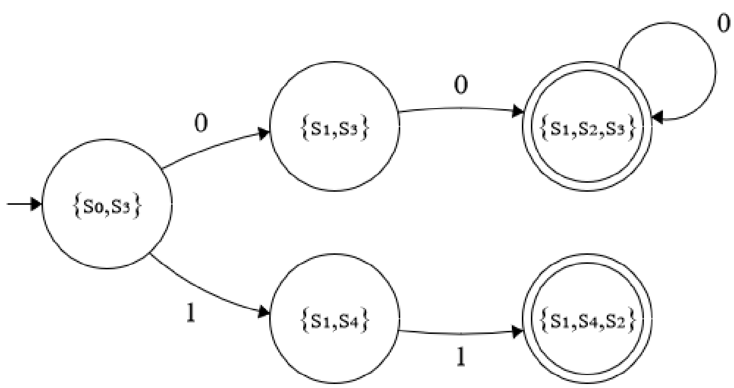
וזה מסיים את ההוכחה כי השפות של האוטומטים שוות. ■

דוגמה בחזרה לדוגמה למעלה (מצורף איור נוסף), נמצא DFA מתאים לזה (נבצע דטרמינטיזציה).



איור 17: NFA שראינו למעלה

ה-DFA המתאים הוא כבאיור, כאשר הוא לא שלם כי יש 2^5 מצבים. הרעיון בכל אופן הוא שבכל פעם אנחנו מסתכלים לאן כל אחד מהמצבים לוקח אותנו בהינתן האות הנוכחית ואוספים את כולם לכדי מצב (כמו ההגדרה של ρ), ושמצב הוא מקבל אם"ם הוא מכיל מצב שהיה מקבל ב-NFA.



איור 18: DFA חלקי שמתאים ל-NFA למעלה

תרגול

טענה לכל NFA $A=\langle Q,\Sigma,\delta,Q_0,F\rangle$ קיים NFA שקול B כך שב-B אין מעבר ϵ.

הוכחה: הרעיון הוא שנקבץ את כל המצבים שעוברים אליהם עם ϵ לאחד כל פעם ונראה שזה שקול. נגדיר

$$E\left(q\right)=\{s:\text{יש מסלול מ-}q\text{ ל-}S\text{ ב-}A\text{ רק עם מעברי }\epsilon\}$$

נשים לב כי תמיד $q \in E(q)$ ובפרט $E(q) \neq \varnothing$ (לא לצעוד מ-q זה כמו לצעוד אפסילון מ-q כי לא קראנו כלום).

נגדיר $B = \left\langle Q, \Sigma, \delta', \bigcup_{q \in Q_0} E(q), F \right\rangle$ כאשר הרעיון במצבים ההתחלתיים הוא כל המצבים שאפשר להגיע אליהם ממצב התחלתי כלשהו רק בצעדי אפסילון.

נגדיר $\delta'(q,\sigma) = \bigcup_{s \in \delta(q,\sigma)} E(s)$ כלומר כל מצב שאפשר להגיע אליו עם האות ומעברי אפסילון מ-q (בפרט זה כולל גם את מצבי $\delta(q,\sigma)$ המקוריים).

לא נוכיח נכונות אבל כן נסביר למה הבניה הזו היא פולינומיאלית: אפשר לחשב כל $E(q)$ בזמן יעיל באמצעות DFS כאשר קשת קיימת בגרף שלנו אם"ם היא מעבר אפסילון בין שני מצבים באוטומט. ■

טענה REG סגורה לאיחוד, כלומר אם $L_1, L_2 \in \mathrm{REG}$ אז $L_1 \cup L_2 \in \mathrm{REG}$.

הוכחה: יהיו $A_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle, A_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$ DFA-ים ל-L_1, L_2 בהתאמה. בה"כ $Q_1 \cap Q_2 = \varnothing$ (אפשר לשנות את השמות, זה לא מעניין). נבנה NFA B לשפה $L_1 \cup L_2$ כך ש-

$$B = \langle Q_1 \cup Q_2, \Sigma, \delta, \{q_1, q_2\}, F_1 \cup F_2 \rangle$$

ופ' המעבירים מוגדרת ע"י

$$\delta(q,\sigma) = \begin{cases} \delta(q,\sigma) & q \in Q_1 \\ \delta_2(q,\sigma) & q \in Q_2 \end{cases}$$

כך, מילים מ-L_1 יוכלו להתקבל מריצות שמתחילות ב-q_1 ומילים ב-L_2 מתקבלות על ריצות החל מ-q_2 (למעשה יש לנו שני אוטומטים זרים שכל ריצה יכולה לבחור איפה היא מתחילה).

נראה ש-$L(B) = L_1 \cup L_2$ באמצעות הכלה דו כיוונית.

$\underline{L_1 \cup L_2 \subseteq L(B)}$: תהי $w \in L_1 \cup L_2$ ובה"כ $w \in L_1$. היות ש-$w \in L_1$, הריצה של A_1 על w מקבלת ונסמנה $r_0, \ldots, r_{|w|}$ כאשר $r_0 = q_1$ ו-$r_{|w|} \in F_1$. נשים לב שהריצה $r_0, \ldots, r_{|w|}$ היא ריצה אפשרית של B על w כי $r_0 \in \{q_1, q_2\}$, פ' המעברים δ מוגדרת היטב במקרה ש-$q \in Q_1$ וזה מתקיים לכל אורך המסלול ובנוסף $r_{|w|} \in F_1 \subseteq F_1 \cup F_2$ ולכן הריצה גם מקבלת, כלומר $w \in L(B)$.

$\underline{L(B) \subseteq L_1 \cup L_2}$: תהי $w \in L(B)$, כלומר קיימת ריצה מקבלת של B על w שנסמנה $r_0, \ldots, r_{|w|}$. מהגדרת B, $r_0 \in \{q_1, q_2\}$ ונניח בה"כ כי $r_0 = q_1$. היות ש-$q_0 \in Q_1$, לכל $0 \le i \le |w| - 1$ מתקיים שהמעבר מ-r_i ל-r_{i+1} נעשה דרך הפ' δ_1 (δ_1 מוגדרת רק על מצבים מ-Q_1 ו-$Q_1 \cap Q_2 = \varnothing$) ולכן התמונה של δ_1 מוכל ב-Q_1. בנוסף, $r_{|w|} \in F_1 \cup F_2$ אבל $r_{|w|} \in Q_1$ ולכן $r_{|w|} \in F_1$. לכן, $r_0, \ldots, r_{|w|}$ היא גם ריצה מקבלת של A_1 על w ולכן $w \in L_1$. ■

טענה REG סגורה לשרשור, כלומר אם $L_1, L_2 \in \mathrm{REG}$ אז $L_1, L_2 \in \mathrm{REG}$.

הוכחה: הרעיון הוא שנאפשר קפיצה (בניחוש) מכל מצב מקבל ב-A_1 להתחלה של A_2 ואז כך נאפשר שרשור של מילים.

יהיו $A_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle, A_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$ DFA-ים ל-L_1, L_2 בהתאמה. בה"כ $Q_1 \cap Q_2 = \varnothing$. נגדיר NFA B לשפה $L_1 \cdot L_2$ ע"י $B = \langle Q_1 \cup Q_2, \Sigma, \delta, \{q_1\}, F_2 \rangle$ כאשר

$$\delta(q,\sigma) = \begin{cases} \delta_1(q,\sigma) & q \in Q_1, \sigma \in \Sigma \\ \delta_2(q,\sigma) & q \in Q_2, \sigma \in \Sigma \\ \{q_0\} & q \in F_1, \sigma = \epsilon \end{cases}$$

הוכחה: נוכיח הכלה דו כיוונית. $\underline{L_1 \cdot L_2 \subseteq L(B)}$: תהי $w \in L_1 \cdot L_2$ כלומר $w = x \cdot y$ כאשר $x \in L_1, y \in L_2$. ישנן ריצות מקבלות של A_1 על x ושל A_2 על y, בהתאמה נסמנן $r_0, \ldots, r_{|x|}$ ו-$r'_0, \ldots, r'_{|y|}$. נשים לב כי הריצה $r_0, \ldots, r_{|w|}, r'_0, \ldots, r'_{|y|}$ היא ריצה של B על $w = x \cdot y$. ■

$r_0 = q_0$ הוא אכן מצב התחלתי ב-B ועד $r_{|x|}$ הריצה של B על x ממשיכה כמו זו של A_1 ומסתיימת ב-$r_{|x|} \in F_1$.

מכאן יש מעבר $\delta(r_m, \epsilon) = \{q_2\}$ ומשם הריצה של B על ההמשך של w שהוא בדיוק y היא כמו של A_2 על y.

זו מסתיימת ב-$r_{|y|} \in F_2$ ובגלל שהמצבים המקבלים של B הם גם F_2, קיבלנו ריצה מקבלת.

$\underline{L(B) \subseteq L_1 \cup L_2}$: תהי $w \in L(B)$ ותהי $r_0, \ldots, r_{|w|}$ ריצה מקבלת (כלשהי) של B על w. מתקיים $r_0 = \{q_1\}$ ו-$r_{|w|} \in F_2$. מהגדרת B, כדי להגיע ל-F_2 חייב להיות קיים $k \in [|w|]$ כך שהמעבר $r_k \to r_{k+1}$ השתמש במעבר ϵ ממצב ב-F_1 ל-$\{q_2\}$.

נביט במילים $x = w_1, \ldots, w_k$ ו-$y = w_{k+1}, \ldots, w_{|w|}$. מהגדרת B, הריצה $r_0, \ldots, r_k$ היא ריצה של A_1 על x שמסתיימת ב-F_1 ולכן זו ריצה מקבלת של A_1 על x ולכן $x \in L(A_1)$.

באופן דומה, הריצה של B על y החל מ-r_{k+1} היא ריצה של A_2 על y שמסתיממת במצב מקבל ב-F_2 ולכן $y \in L(A_2)$ ולכן $w \in L(A_1) \cdot L(A_2)$. ■

טענה REG סגורה לפעולה Kleene-Star כלומר אם $L \in \text{REG}$ אז $L^* = \bigcup_{k \in \mathbb{N}_0} \underbrace{L \cdot \ldots \cdot L}_{k \text{ פעמים}} \in \text{REG}$.

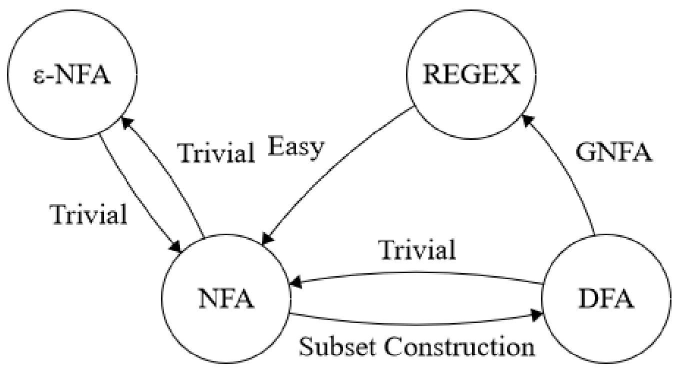
הוכחה: יהי $A = \langle Q, \Sigma, \delta, q_0, F \rangle$ DFA ל-L. לכאורה היינו יכולים לבנות NFA שהוא A פשוט עם חיבור מהמצבים הסופיים למצב ההתחלתי שוב עם צעד אפסילון. הבעיה היא שאם A לא מקבל את המילה הריקה, גם הבניה לא אבל $\epsilon \in L^*$. לכן נוסיף מצב נוסף q_{start} שהוא יהיה המצב ההתחלתי היחיד שיש ממנו צעד אפסילון למצב ההתחלתי של A.

נבנה NFA B לשפה L^* ע"י $B = \langle Q \cup \{q_{start}\}, \Sigma, \delta', \{q_{start}\}, \{q_{start}\} \rangle$ כאשר בה"כ $q_{start} \notin Q$. δ מוגדרת ע"י

$$\delta'(q,\sigma) = \begin{cases} \{\delta(q,\sigma)\} & q \in Q \\ \varnothing & q = q_{start} \\ \hline \varnothing & q = q_{start} \wedge \sigma = \epsilon \\ \{q_{start}\} & q \in F \wedge \sigma = \epsilon \\ \{q_0\} & q = q_{start} \wedge \sigma = \epsilon \end{cases}$$

■

הערה ראו איור של מצבנו מבחינת שקילות של אוטומטים, כאשר בקרוב נלמד על REGEX-ים,



איור 19 : מפת שקילות בין אוטומטים

שבוע III | שפות לא רגולריות ולמת הניפוח

הרצאה

חלק א' של ההרצאה

הערה בהרצאה הקודמת הראנו איך לעשות דטרמיניזציה ל-NFA וראינו שבהינתן NFA A' עם n מצבים, ל-DFA השקול לו יש לכל היותר 2^n מצבים (חסם עליון).

היום נראה שאין פולינום p שבהינתן (כל) NFA עם n מצבים, יש לו DFA שקול עם לכל היותר $p(n)$ מצבים (חסם תחתון).

מקרים פרטיים כמובן כן יכולים להיות חסומים ע"י פולינום בגדילה שלהם כשהם DFA, אבל שום בנייה לא תעבוד לכל NFA אפשרי.

הערה לא מספיק שנראה, לדוגמה, שפה L כך שיש ל-L NFA עם 10 מצבים, אבל כל DFA עבור L צריך 2^{10} מצבים.

זה לא מוכיח שום דבר כי זה לא סותר את הפולינום $p(n) = n^3 + 500$, שעבורו $p(10) > 2^{10}$ ולכאורה הוא מצליח לחסום NFA-ים כלשהם (כמובן שלא את כולם).

משפט לכל פולינום p, קיימת שפה L כך של-L קיים NFA עם n מצבים וה-DFA הקטן ביותר עבור L צריך יותר $p\left(n\right)$ מצבים.

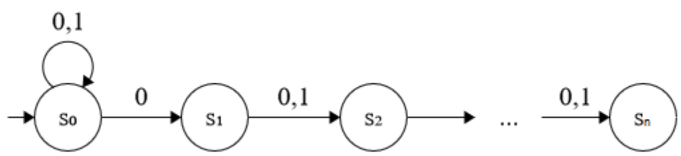
הוכחה: מספיק שנראה שלכל $n \geq 1$ קיימת L_n כך של-L_n קיים NFA עם $n+1$ מצבים אבל ה-DFA הקטן ביותר עבור L_n צריך לפחות 2^n מצבים.

כי אם בשלילה קיים פולינום כאמור, נתבונן ב-n_0 שמובטח שעבורו $2^{n_0} > p\left(n_0+1\right)$ ונתבונן ב-L_{n_0}. משם ה-DFA הקטן ביותר עבור L_{n_0} מכיל $2^{n_0} > p\left(n_0+1\right)$ מצבים כפי שנוכיח עכשיו בסתירה לקיום פולינום שמקיים את התנאים.

נבחר $\Sigma = \{0,1\}$ ונגדיר

$$L_n = \left(0+1\right)^* 0 \left(0+1\right)^{n-1} = \{w : \text{האות ה-}n\text{-ית מהסוף היא } 0\}$$

כאשר הביטוי משמאל נקרא ביטוי רגולרי - $0,1$ כמה פעמים שנרצה (רישא), 0, ואז $n-1$ 0 או 1-ים. ראו איור של NFA מתאים לשפה,



איור 20: NFA ל-L_n

נניח בשלילה שיש DFA D_n כך ש-$L\left(D_n\right) = L_n$ ויש ל-D_n פחות מ-2^n מצבים. ישנם 2^n וקטורים באורך n מעל $\{0,1\}$ ולכן 2^n מילים שונות באורך n מעל הא"ב $\{0,1\}$.

אם ב-D_n יש פחות מ-2^n מצבים, אז מעקרון שובך היונים יש שתי מילים $w_1 \neq w_2 \in \left(0+1\right)^n$ שעבורן D_n מגיע לאותו המצב בסוף קריאתן. ופורמלית, עבור $D_n = \langle \{0,1\}, Q, q_0, \delta, F \rangle$, קיימות $w_1 \neq w_2 \in \left(0+1\right)^n$ כך ש-

$$q = \delta^*\left(q_0, w_1\right) = \delta^*\left(q_0, w_2\right)$$

מהיות $w_1 \neq w_2$, הרי שקיים $i \in [n]$ כך ש-$w_1[i] \neq w_2[i]$ ובה"כ $w_1[i] = 0, w_2[i] = 1$. נוכיח שבהכרח האוטומט טועה כי נשרשר סיפא למילים כך ש-i יהיה האינדקס ה-n מהסוף ואז האוטומט מסווג את שתי המילים באותה הדרך בניגוד לכך שאחת הוא אמור לקבל והאחרת לדחות (מהגדרת השפה). נתבונן ב-$s = \delta^*\left(q, 1^{i-1}\right)$.

- אם $s \in F$ אז D_n מקבל את $w_2 \cdot 1^{i-1}$ בסתירה לנכונות D_n, שכן $w_2 \cdot 1^{i-1} \notin L$ (האות ה-n מהסוף היא $w_2[i-1]$).
- אם $s \notin F$ אז D_n דוחה את $w_1 \cdot 1^{i-1}$ (הוא DFA והריצה היחידה מגיעה ל-s) בסתירה לנכונות D_n, שכן $w_1 \cdot 1^{i-1} \in L$.

כלומר הגענו לסתירה בכל המקרים. ■

טענה אין DFA עבור $L = \{0^n 1^n : n \geq 0\}$.

הוכחה: נניח בשלילה כי $A=\left\langle Q,\Sigma,q_{)},\delta,F\right\rangle$ הוא DFA עם $L\left(A\right)=L$. יהי $|Q|=p$. נתבונן במילה $w=0^{p}1^{p}$. $w\in L$ ולכן הריצה של A על w, $r=q_{0}q_{1},\ldots,q_{2p}$, מקבלת, כלומר $q_{2p}\in F$.

ברישא $q_{0},\ldots,q_{p}$ יש מעגל, כלומר קיימים $0\le l<j\le p$ כך ש-$q_{l}=q_{j}$ (מעקרון שובך היונים). לכן יש ל-A ריצה מקבל גם על $0^{p-(j-1)}1^{p}\notin L$ (כי אפשר לגדום את המעגל מ-l ל-j ולהסתכל על הריצה $q_{0}\ldots q_{l}q_{j+1}\ldots q_{2p}$). ■

משפט (למת הניפוח לשפות רגולריות, pumping lemma) אם L רגולרית אז קיים $p\ge1$ (קבוע הנפוח) כך שלכל מילה $w\in L$, אם $|w|\ge p$ אז קיימת חלוקה $w=x\cdot y\cdot z$ כך ש:

1. $|x\cdot y|\le p$.
2. $|y|>0$ ($y\neq\epsilon$).
3. $\forall i\ge0$, המילה $xy^{i}z\in L$.

הערה אם L סופית אז אפשר לקחת $p=l+1$ עבור l אורך המילה הארוכה ביותר ב-L ואז הלמה מתקיימת באופן ריק.

דוגמה עבור $L=\left(0+1\right)^{*}0\left(0+1\right)$ (כל המילים שהאות הלפני אחרונה שלהם היא 0). ניקח $p=3$ ונתבונן במילה $w\in L$ עם $|w|\ge3$. נבחר $w=x\cdot y\cdot z$ כאשר $x=\epsilon,|y|=1,|z|=|w|-1$.

אכן $y\neq\epsilon$ וכמובן $|x\cdot y|=1\le3$ ולכל $i\ge0$, $xy^{i}z\in L$ כי $|z|\ge2$ ולכן האות הלפני האחרונה ב-$xy^{i}z$ נשארת האות הלפני האחרונה ב-z, הלא היא 0.

הוכחה: תהי L שפה רגולרית. יהי A DFA שמזהה את L ונבחר p להיות מספר המצבים ב-A. נתבונן במילה $w\in L$ עם $|w|\ge p$. בריצה של A על w, יש מצב שחוזר בקריאת p האותיות הראשונות, כלומר קיימים $0\le j<l\le p$ כך ש-$q_{l}=q_{j}$ (מעקרון שובך היונים). נבחר x,y,z ע"י

$$w=\underset{x}{\underline{w_{1}\ldots w_{j}}}\,\underset{y}{\underline{w_{j+1}\ldots w_{l}}}\,\underset{z}{\underline{w_{l+1}\ldots w_{n}}}$$

ונראה שהתנאים של הלמה מתקיימים. $j<l$ ולכן $|y|>0$, $|x\cdot y|\le p$ כי $l\le p$ ואכן $xy^{i}z\in L$ כי הריצה היא

$$q_{0},\ldots,q_{j},\left(q_{j+1}\ldots,q_{l}\right)^{i},q_{l+1},\ldots,q_{n}$$

כאשר זו ריצה חוקית כי יש מעבר מ-q_{l} ל-$q_{j+1}=q_{l+1}$. ■

חלק ב' של ההרצאה

הערה נוכל להשתמש בשלילת למת הניפוח כדי להוכיח ששפות הן לא רגולריות. אם למת הניפוח מספרת לנו ש-$L\in\mathrm{REG}\Rightarrow\alpha$, אז $\neg\alpha$ הוא שלכל $p\ge1$, קיימת מילה $w\in L$ עם $|w|\ge p$ כך שלכל חלוקה $w=x\cdot y\cdot z$, אם $|x\cdot y|\le p$ וגם $|y|>0$, קיים $i\ge0$ כך ש-$xy^{i}z\notin L$.

או במילים, לכל קבוע ניפוח קיימת מילה ארוכה מהקבוע כך שלא משנה איזו חלוקה נבחר עם $y \neq \epsilon$ ו-$|xy| \leq p$, אחד הניפוחים של y לא בשפה.

את הבחירה על השלילה של שלושת התנאים עשינו כי זה נוח אבל אפשר היה גם לעשות שאם $1, 3$ מתקיימים אז 2 לא מתקיים.

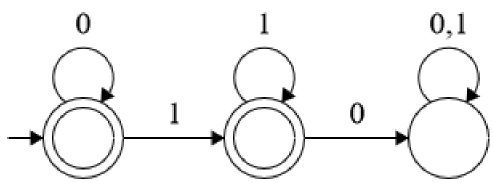
דוגמאות לשפות לא רגולריות

1. תהי $L_1 = \{0^n 1^n : n \geq 0\}$. זו שפה לא רגולרית (ראינו כבר אבל גם) כי לכל p, נוכל להתבונן במילה $0^p 1^p$. לכל חלוקה $xyz = 0^p 1^p$ כך ש-$|xy| \leq p$, מתקיים $y = 0^j$ עבור $1 \leq j$ (אחרת xy זולג ל-1-ים ויוצא שהוא ארוך מ-p). לכן, $xy^2 z = 0^{p+j} 1^p \notin L_1$.

2. $L_2 = \{w : \#_0 w = \#_1 w\}$ היא גם לא רגולרית. ההוכחה הנ"ל עובדת גם כן כי גם שם $0^p 1^p \in L$ ו-$|0^p 1^p| \geq p$ וכו' וכו'.

   יש דרכים אחרות בהינתן שידוע לנו ש-L_1 לא רגולרית להוכיח ש-L_2 לא רגולרית.

- ניסיון 1: $L_1 \subseteq L_2$ ו-L_1 לא רגולרית ולכן L_2 לא רגולרית - לא עובד! $L_1 \subseteq (0+1)^*$ אבל האחרונה כן רגולרית (DFA טריוויאלי).
- ניסיון 2: עבור $L_3 = 0^* 1^*$ קיים DFA שמזהה אותה (ראו איור). מתקיים $L_1 = L_2 \cap L_3$ ומסגירות שפות רגולריות לחיתוך, נובע ש-L_2 לא רגולרית (אחרת החיתוך שלה עם L_3 היה רגולרי בסתירה לכך ש-L_1 לא רגולרית).



איור 21: DFA ל-L_3

3. $L_4 = \{0^n 1^m : n > m\}$ לא רגולרית לפחות אינטואיטיבית. נוכיח זאת עם למת הניפוח. בהינתן p, נתבונן במילה $0^{p+1} 1^p$ ובחלוקה xyz כך ש-$|xy| \leq p$, $|y| > 0$, בהכרח $y = 0^j$ עבור $j \geq 1$. הניפוח עם $i = 0$ מוציא מהשפה (ניפוח מטה), כי

$$0^{p+1-j} 1^p = xy^0 z = xz$$

   אבל $p + 1 - j \leq p$ וזה לא בשפה.

4. $L_5 = \left\{w \cdot w : w \in (0+1)^*\right\}$ היא לא רגולרית (אינטואיטיבית) ונראה זאת עם למת הניפוח. בהינתן $p \geq 1$, נתבונן במילה $w = 0^p 1 0^p 1 \in L_5$ ואכן $|w| \geq p$. לכל חלוקה $w = xyz$ כך ש-$|xy| \leq p$ ו-$|y| > 0$ מתקיים $y = 0^j$ עבור $j \geq 1$ (כרגיל) ונתבונן ב-$i = 2$, שעבורו $xy^2 z = 0^{p+j} 1 0^p 1$ היא מילה לא בשפה (הצדדים שלה לא שווים).

5. $L_6 = \{a^p : p \text{ ראשוני}\}$ (כאשר $\Sigma = \{a\}$) היא לא רגולרית (כלומר גם אין אפיון עם מספר מצבים סופי של המספרים הראשוניים).

   בהינתן p, יהי q ראשוני עם $q > p$. נתבונן במילה $w = a^q$ ותהי חלוקה $w = xyz$ כך ש-$|xy| \leq p$ ו-$|y| > 0$. נסמן $|x| = n, |y| = m$ ולכן $|z| = q - (n+m)$.

$$\left|xy^i z\right| = n + mi + q - (n+m) = m(i-1) + q$$

ועבור $i = q+1$ מתקיים $q\left(m+1\right) = q + \left(1-\left(q+1\right)\right)m = \left|xy^iz\right|$ שזה כמובן לא בשפה כי זה פריק ($m > 0$ ולכן $m+1>1$).

6. $L_7 = \{w : w \text{ פלינדרום}\}$ עבור $\Sigma = \{0,1\}$. נתבונן ב-$w = 0^p10^p$ ואז אם $|xy| \leq p$ ו-$|y| > 0$ אז $xy^2z \notin L$ כי ה-1 לא באמצע.