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 אמ"ם דרגת כל הקודקודים זוגית, ולכן ניתן להכריע את הבעיה בזמן לינארית כי יש לבעיה אפיון מתמטי.

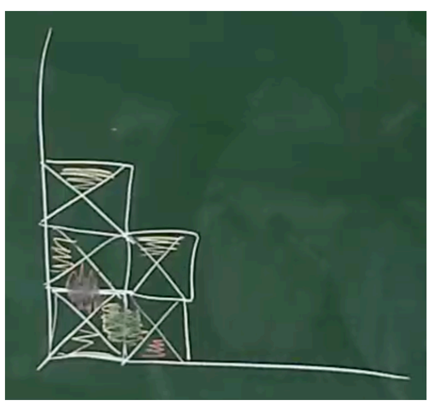
מעגל המילטון הוא מעגל שעובר בכל קודקוד בדיוק פעם אחת. לבעיה הזו אין אפיון מתמטי, והוכח שאין אלג' יותר טוב מאשר מעבר על כל האפשרויות, בסיבוכיות אקספוננציאלי.

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 $\{u_i\}, \{d_i\}, \{r_i\}, \{l_i\}$ (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.

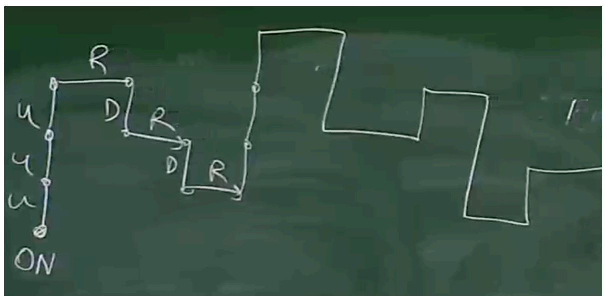
פלט: האם P עוצרת על x.

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

אוטומטים

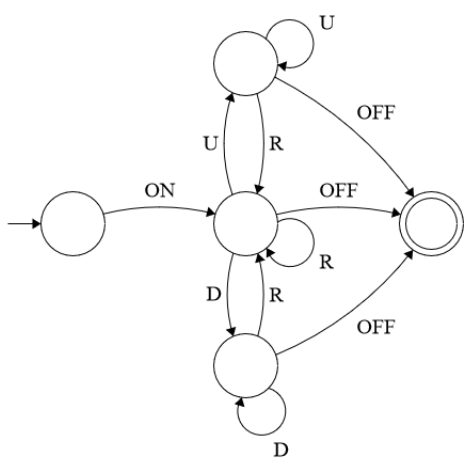
הגדרה <u>אוטומט</u> הוא מחשב עם זכרון מוגבל.

דוגמה נתון עט דיגיטלי שיכול לבצע אחת משש פקודות, 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 $w = w_1, \ldots, w_n$ סדרה סופית של אותיות, ו-ϵ היא המילה הריקה.
- שפה היא קבוצה של מילים, $L \subseteq \Sigma^*$ כאשר $\Sigma^* = \{w : \Sigma \text{ מילה סופית מעל הא"ב } w\}$.

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 $w = w_1 \ldots w_n$ מעל Σ היא סדרה של מצבים $r = r_0 \ldots r_n$ 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 $q_0 q_0 q_1 q_0$.

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

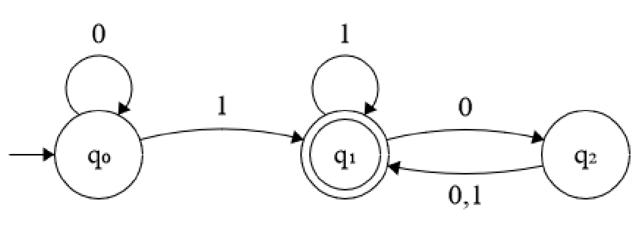
A מקבל את w אם הריצה של A על w היא מקבלת.

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

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

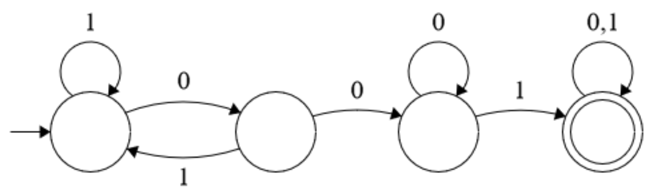
נסמן בצבע האם כמה מילים נבחרות הן בשפה או לא, 00000, 11, 1, 001110, 011, 010.

אם נחשוב עוד קצת, נגלה ש-

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

בתרגול נוכיח את זה באופן פורמלי.

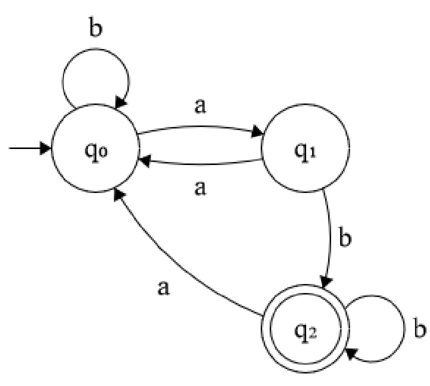
דוגמה בהינתן שפה, ננסה לחשב את האוטומט. השפה היא $L_3 = \{w : w$ מכילה את הרצף $001\}$.



איור 5 : אוטומט שנגזר מ-L_3

חלק ב' של ההרצאה

דוגמה $\Sigma = \{a, b\}$, $L = \{w :$ אי זוגי $\#_a w \wedge w_n = b\}$ (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 אינסופית (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

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

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

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

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

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

• $L=\{ww:w\in\Sigma^*\}$.

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

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

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

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

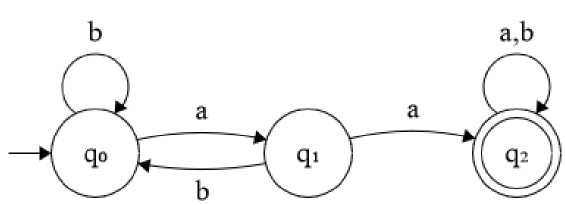
כמה שפות יש מעל Σ^*? $2^{|\Sigma^*|}=2^{\aleph_0}$.

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 $\mathbb{III}$ | 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 $A_2 = \langle Q_2, \Sigma, \delta_2, s_2, F_2 \rangle$, $A_1 = \langle Q_1, \Sigma, \delta_1, s_1, F_1 \rangle$, נבנה $A = \langle Q, \Sigma, \delta, s_0, F \rangle$ שעבורו $L(A) = L(A_1) \cup L(A_2)$.

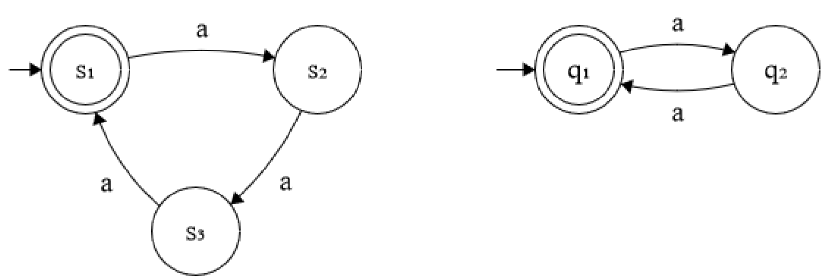
הרעיון הוא ש-A מסמלץ את A_1 ו-A_2 יחד, ואוטומט בבנייה כזו נקרא אוטומט המכפלה. נבחר $Q = Q_1 \times Q_2$, $s_0 = \langle s_1, s_2 \rangle$, ופ' מעברים

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

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

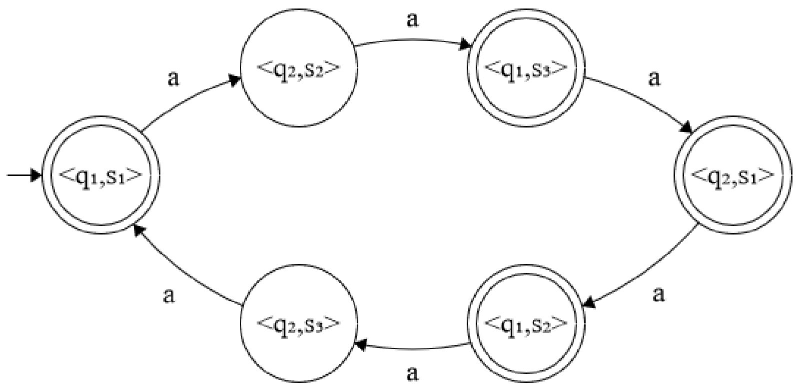
הערה אם $L \subseteq \{a\}^*$ אז היא מגדירה תת קבוצה של $\mathbb{N}$ - כל האורכים של מילים בשפה, כלומר $\{i : a^i \in L\}$.

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 $L\left(A\right)=\left\{ w:\left|w\right|\mod2=0\vee\left|w\right|\mod3=0\right\}$.

הערה מהדוגמה הנ"ל ניתן לראות שאם היינו רוצים לבנות אוטומט שהשפה שלו היא $L\left(A_{1}\right)\cap L\left(A_{2}\right)$ היינו בוחרים

$$F=\left\{ \left\langle q_{1},q_{2}\right\rangle :q_{1}\in F_{1}\wedge q_{2}\in F_{2}\right\}$$

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

הערה אם היינו רוצים A עם $L\left(A\right)=\Sigma^{*}\backslash L\left(A_{1}\right)$, מספיק שהיינו מגדירים $A=\left\langle Q_{1},\Sigma,\delta_{1},s_{1},Q_{1}\backslash F_{1}\right\rangle$ כי הריצה מגיעה ל-$Q_{1}\backslash F_{1}$ אם"ם A_{1} דוחה את w.

נוכיח כי $L\left(A\right)=L\left(A_{1}\right)\cup L\left(A_{2}\right)$. תהי $w=w_{1}w_{2}\ldots w_{n}$ מילה ב-Σ^{*} ותהי $r=r_{0}r_{1}\ldots r_{n}$ 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 $i\geq0$,

$$q_{1}^{i+1}=\delta_{1}\left(q_{1}^{i},w_{i}\right),q_{2}^{i+1}=\delta_{2}\left(q_{2}^{i},w_{i}\right)$$

ולכן $\rho_{1}=q_{1}^{0},q_{1}^{1},\ldots,q_{1}^{n}$ היא ריצה של A_{1} על w ובהתאמה $\rho_{2}=q_{2}^{0},q_{2}^{1},\ldots,q_{2}^{n}$ היא ריצה של A_{2} על w.

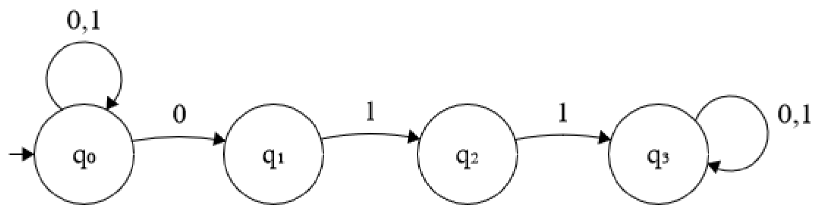
מכאן, r מקבלת אם"ם $\left\langle q_{1}^{n},q_{2}^{n}\right\rangle \in F$ אם"ם $q_{1}^{n}\in F_{1}$ או $q_{2}^{n}\in F_{2}$ אם"ם r_{1} מקבלת או r_{2} מקבלת אם"ם $w\in L\left(A_{1}\right)$ או $w\in L\left(A_{2}\right)$.

■

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

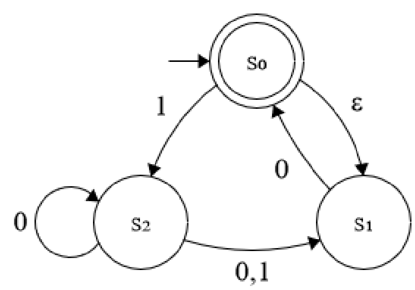
לכאורה פ' המעברים לא מוגדרת היטב עבור $q_0, 0$, אבל כאן הרעיון הוא שהאוטומט יכול לבחור מתוך כמה אפשרויות בעצמו לאיזה מצב הוא עובר, כאשר מילה מתקבלת ע"י האוטומט אם"ם קיימת ריצה עם ניחושים כלשהם שמקבלת, ובמקרה כזה נגדיר $\delta\left(q_0, 0\right) = \{q_0, q_1\}$.

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"

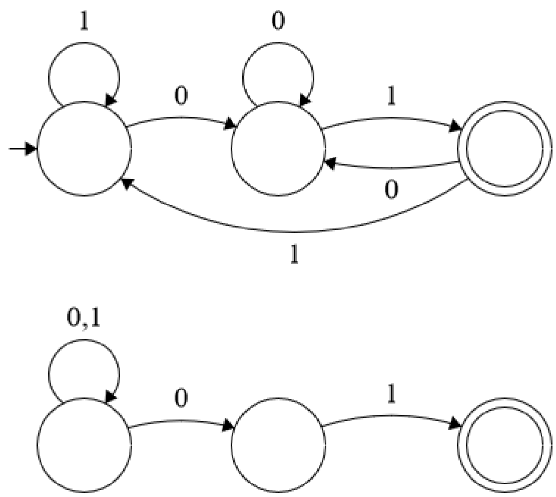
המילים הבאות מתקבלות : $\epsilon, 0, 00, 00110$ (כי נוכל להשתמש קודם בצד אפסילון במקום ליפול לבור דוחה מ-s_0) ואילו $001, 00111$ לא מתקבלות.

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 $r_m\in F$.

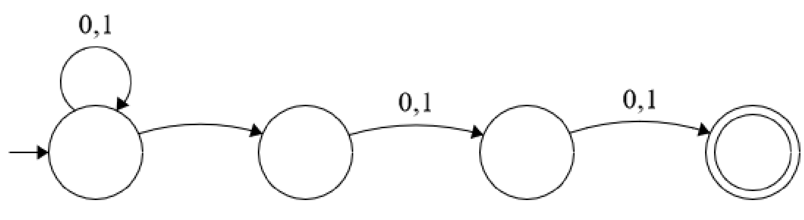
נאמר כי A מקבלת את w אם"ם קיימת ריצה של A על w שמקבלת.

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),



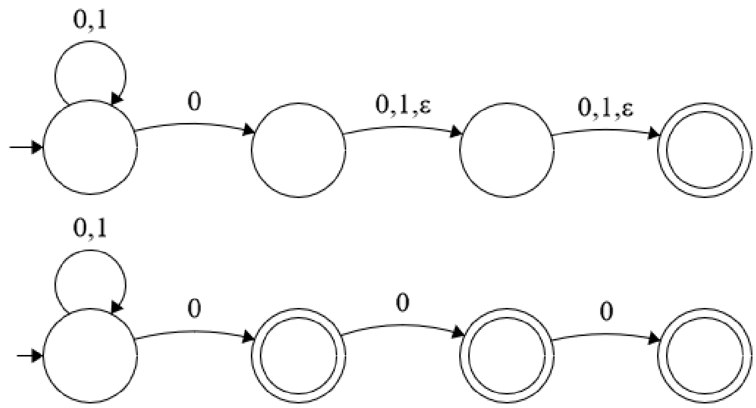
איור 12 : אוטומט דטרמיניסטי (למעלה) ואי-דטרמיניסטי (למטה) שמשרתים אותה המטרה

דוגמה עבור $L=\{w:0\,(0+1)\,(0+1)$ 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',



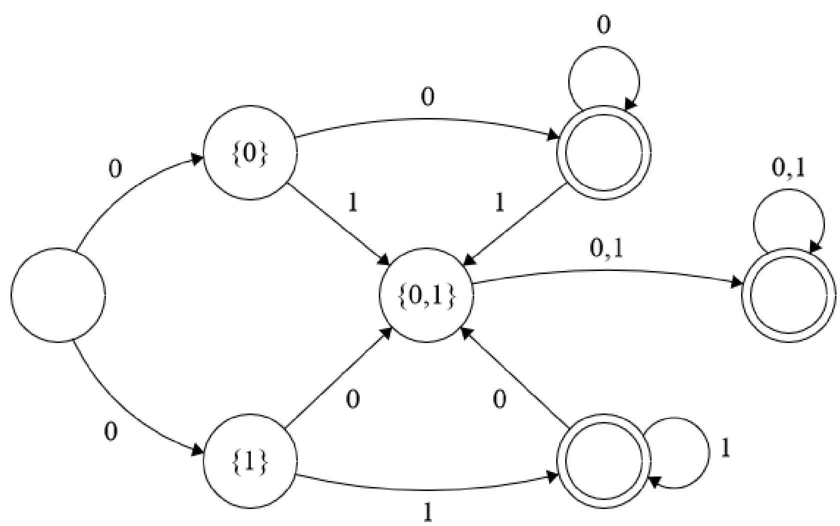
איור 14 : שני אוטומטים אי-דטרמיניסטיים ששפתם L'

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.

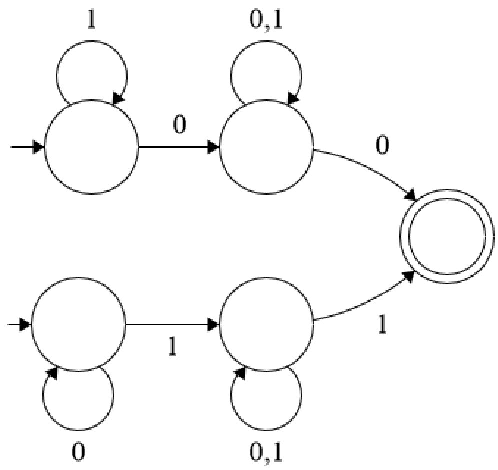
חלק ב' של ההרצאה

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 $\delta^*(s, \epsilon) = s$, $\delta^*(S, \sigma) = \bigcup_{s \in S} \delta(s, \sigma)$ 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 $(w = \epsilon)$: $\rho^*(q_0', \epsilon) = q_0' = Q_0 = \delta^*(Q_0, \epsilon)$.

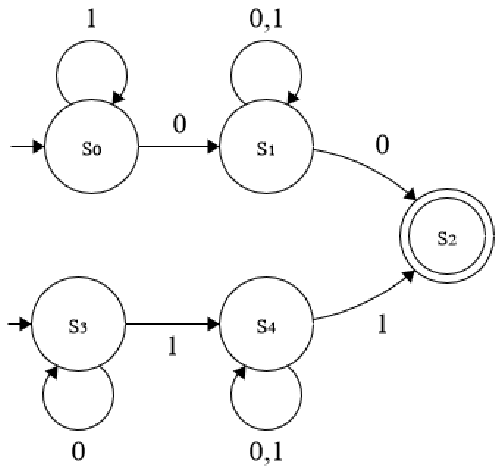
צעד $(|w| \to |w+1|)$:

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

■

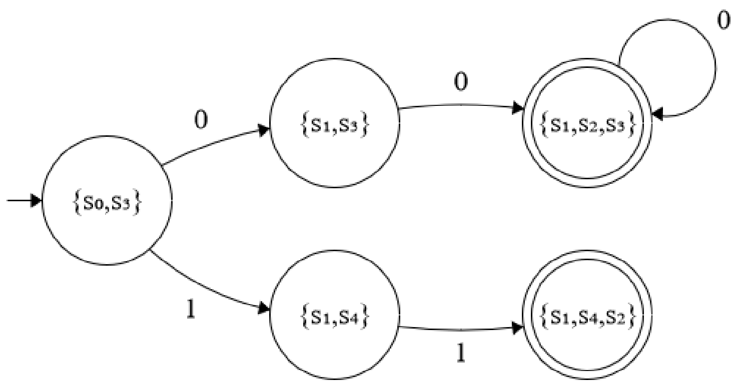
וזה מסיים את ההוכחה כי השפות של האוטומטים שוות. ■

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

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

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

נגדיר $B=\left\langle Q,\Sigma,\delta',\bigcup\limits_{q\in Q_{0}}E\left(q\right),F\right\rangle$ כאשר הרעיון במצבים ההתחלתיים הוא כל המצבים שאפשר להגיע אליהם ממצב התחלתי כלשהו רק בצעדי אפסילון.

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

לא נוכיח נכונות אבל כן נסביר למה הבניה הזו היא פולינומיאלית: אפשר לחשב כל $E\left(q\right)$ 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 $A_{1}=\left\langle Q_{1},\Sigma,\delta_{1},q_{1},F_{1}\right\rangle ,A_{2}=\left\langle Q_{2},\Sigma,\delta_{2},q_{2},F_{2}\right\rangle$ 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-

$$B=\left\langle Q_{1}\cup Q_{2},\Sigma,\delta,\left\{ q_{1},q_{2}\right\} ,F_{1}\cup F_{2}\right\rangle$$

ופ' המעבירים מוגדרת ע"י

$$\delta\left(q,\sigma\right)=\begin{cases}\delta\left(q,\sigma\right) & q\in Q_{1}\\ \\ \delta_{2}\left(q,\sigma\right) & q\in Q_{2}\end{cases}$$

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-$L\left(B\right)=L_{1}\cup L_{2}$ באמצעות הכלה דו כיוונית.

<u>$L_{1}\cup L_{2}\subseteq L\left(B\right)$</u>: 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 $r_{0}\in\left\{ q_{1,}q_{2}\right\}$, 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 $w\in L\left(B\right)$.

<u>$L\left(B\right)\subseteq L_{1}\cup L_{2}$</u>: תהי $w\in L\left(B\right)$, כלומר קיימת ריצה מקבלת של B על w שנסמנה $r_{0},\ldots,r_{|w|}$. מהגדרת B, $r_{0}\in\left\{ q_{1},q_{2}\right\}$ ונניח בה"כ כי $r_{0}=q_{1}$. היות ש-$q_{0}\in Q_{1}$, לכל $0\leq i\leq|w|-1$ 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 $r_0, \dots, r_{|x|}$ ו-$r'_0, \dots, r'_{|y|}$. נשים לב כי הריצה $r_0, \dots, r_{|w|}, r'_0, \dots, r'_{|y|}$ 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 $r_0, \dots, r_{|w|}$ 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 $x = w_1, \dots, w_k$ ו-$y = w_{k+1}, \dots, w_{|w|}$. מהגדרת B, הריצה $r_0, \dots, r_k$ 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 $L^* = \bigcup_{k \in \mathbb{N}_0} \underbrace{L \cdot \ldots \cdot L}_{k \text{ פעמים}} \in \text{REG}$.

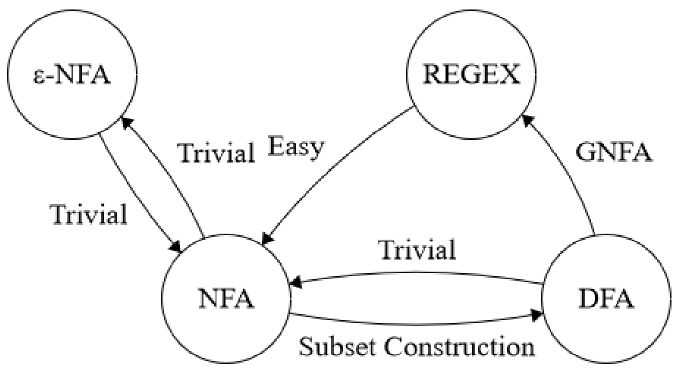
הוכחה: יהי $A = \langle Q, \Sigma, \delta, q_0, F \rangle$ DFA ל-L. לכאורה היינו יכולים לבנות NFA שהוא A פשוט עם חיבור מהמצבים הסופיים למצב ההתחלתי שוב עם צעד אפסילון. הבעיה היא שאם A לא מקבל את המילה הריקה, גם הבניה לא אבל $\epsilon \in L^*$. לכן נוסיף מצב נוסף q_{start} שהוא יהיה המצב ההתחלתי היחיד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

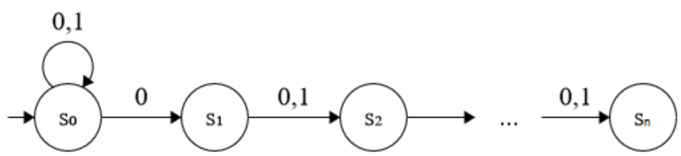
הוכחה: מספיק שנראה שלכל $n\geq1$ קיימת L_n כך של-L_n קיים NFA עם $n+1$ מצבים אבל ה-DFA הקטן ביותר עבור L_n צריך לפחות 2^n מצבים.

כי אם בשלילה קיים פולינום כאמור, נתבונן ב-n_0 שמובטח שעבורו $p\left(n_0+1\right)<2^{n_0}$ 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 $\Sigma=\left\{0,1\right\}$ ונגדיר

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

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 $\left\{0,1\right\}$ ולכן 2^n מילים שונות באורך n מעל הא"ב $\left\{0,1\right\}$.

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 $D_n=\left\langle \left\{0,1\right\},Q,q_0,\delta,F\right\rangle$, 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 $i\in\left[n\right]$ כך ש-$w_1\left[i\right]\neq w_2\left[i\right]$ ובה"כ $w_1\left[i\right]=0,w_2\left[i\right]=1$. 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 $w_2\cdot1^{i-1}$ בסתירה לנכונות D_n, שכן $w_2\cdot1^{i-1}\notin L$ (האות ה-n מהסוף היא $w_2\left[i-1\right]$).
- אם $s\notin F$ אז D_n דוחה את $w_1\cdot1^{i-1}$ (הוא DFA והריצה היחידה מגיעה ל-s) בסתירה לנכונות D_n, שכן $w_1\cdot1^{i-1}\in L$.

כלומר הגענו לסתירה בכל המקרים. ■

טענה אין DFA עבור $L=\left\{0^n1^n:n\geq0\right\}$.

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 $p\geq j<l\leq0$ 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 $p\geq1$ (קבוע הנפוח) כך שלכל מילה $w\in L$, אם $|w|\geq p$ אז קיימת חלוקה $w=x\cdot y\cdot z$ כך ש:

1. $|x\cdot y|\leq p$.
2. $|y|>0$ ($y\neq\epsilon$).
3. $\forall i\geq0$, 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 $|w|\geq3$.

נבחר $w=x\cdot y\cdot z$ כאשר $x=\epsilon,|y|=1,|z|=|w|-1$.

אכן $y\neq\epsilon$ וכמובן $|x\cdot y|=1\leq3$ ולכל $i\geq0$, $xy^{i}z\in L$ כי $|z|\geq2$ 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 $|w|\geq p$. בריצה של A על w, יש מצב שחוזר בקריאת p האותיות הראשונות, כלומר קיימים $p\geq l<j\leq0$ כך ש-$q_{l}=q_{j}$ (מעקרון שובך היונים). נבחר x,y,z ע"י

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

ונראה שהתנאים של הלמה מתקיימים. $j<l$ ולכן $|y|>0$, $|x\cdot y|\leq p$ כי $l\leq p$ 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-$q_{l+1}=q_{j+1}$. ■

חלק ב' של ההרצאה

הערה נוכל להשתמש בשלילת למת הניפוח כדי להוכיח ששפות הן לא רגולריות. אם למת הניפוח מספרת לנו ש-$L\in\text{REG}\Rightarrow\alpha$, אז $\neg\alpha$ הוא שלכל $p\geq1$, קיימת מילה $w\in L$ עם $|w|\geq p$ כך שלכל חלוקה $w=x\cdot y\cdot z$, אם $|x\cdot y|\leq p$ וגם $|y|>0$, קיים $i\geq0$ 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.

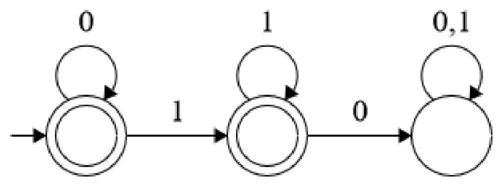
דוגמאות לשפות לא רגולריות

1. תהי $L_1 = \{0^n1^n : n \geq 0\}$. זו שפה לא רגולרית (ראינו כבר אבל גם) כי לכל p, נוכל להתבונן במילה 0^p1^p. לכל חלוקה $xyz = 0^p1^p$ 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, $xy^2z = 0^{p+j}1^p \notin L_1$.

2. $L_2 = \{w : \#_0 w = \#_1 w\}$ היא גם לא רגולרית. ההוכחה הנ"ל עובדת גם כן כי גם שם $0^p1^p \in L$ ו-$|0^p1^p| \geq p$ 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. $L_4 = \{0^n1^m : n > m\}$ 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

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

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 $w = 0^p10^p1 \in L_5$ 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 $xy^2z = 0^{p+j}10^p1$ 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 $|z| = q - (n+m)$.

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

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

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

תרגול

ביטויים רגולריים

הגדרה <u>ביטוי רגולרי</u> מעל א"ב Σ הוא אחד מהבאים:

- $\varnothing$.
- ϵ.
- $a \in \Sigma$.
- $t^*, t \cup s, t \cdot s$ כאשר t, s ביטויים רגולריים קצרים יותר.

הערה דרך נוספת לייצג ביטוי רגולרי מעל $\{a,b\}$ היא $r := \varnothing|\epsilon|a|b|r\cup s|r\cdot s|r^*$.

דוגמה נביט בביטוי מעל $\Sigma = \{a,b\}$, $(a\cup b)^*\,bb\,(a\cup b)^*$. השפה שלו היא כל המילים שמכילות את הרצף bb.

דוגמה הביטוי $00^*\left(1^*\cup 2^*\right)$ מייצג את כל המילים שמתחילות באחד או יותר אפסים ונגמרות ברצף כלשהו של 1-ים או של 2-ים.

הגדרה בהינתן ביטויים רגולריים r, s, t, נגדיר את השפה שלהם כך:

- אם $r = \varnothing$ אז $L(r) = \varnothing$.
- אם $r = \epsilon$ אז $L(r) = \{\epsilon\}$.
- אם $r = a \in \Sigma$ אז $L(r) = \{a\}$.
- אם $r = s \cdot t$ אז $L(r) = L(s)\cdot L(t)$.
- אם $r = s \cup t$ אז $L(r) = L(s)\cup L(t)$.

טענה $L \in \mathrm{REG}$ אם"ם קיים ביטוי רגולרי r כך ש-$L = L(r)$.

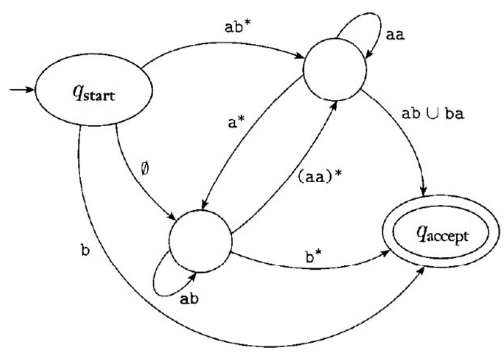
הוכחה: $\Rightarrow$: יהי r ביטוי רגולרי ונראה שקיים NFA A_r כך ש-$L(r) = L(A_r)$ באינדוקציה על אורך סדרת היצירה של r (מספר התווים בכתיבה של הביטוי הרגולרי, כך ϵ הוא באורך 1 לדוגמה).

- אם $r = \varnothing$ אז נבחר A_r להיות NFA ריקה (ששפתו ריקה).
- אם $r = \epsilon$ אז ניקח את A_r להיות NFA ששפתו היא $\{\epsilon\}$ (לדוגמה אוטומט שהמצב ההתחלתי שלו הוא מקבל וכל אות מובילה לבור דוחה).

- אם $r=a\in\Sigma$ אז נבחר A_r להיות NFA ששפתו היא $\{a\}$ (מצב התחלתי לא מקבל, מעבר ממנו למצב מקבל רק על a וכל השאר לבור דוחה).
- אם $r=s\cup t$ אז קיימים A_s,A_t מה"א ומסגירות לאיחוד קיים אוטומט ל-$L\left(A_s\right)\cup L\left(A_t\right)$.
- אם $r=s\cdot t$ אז קיימים A_s,A_t מה"א ומסגירות לשרשור, קיים אוטומט ל-$L\left(A_s\right)\cdot L\left(A_t\right)$.
- אם $r=t^*$ אז מה"א יש A_t ששפתו שווה לשל t ולכן מסגירות לפעולת הכוכב, קיים אוטומט ל-$L\left(A_t\right)^*$.

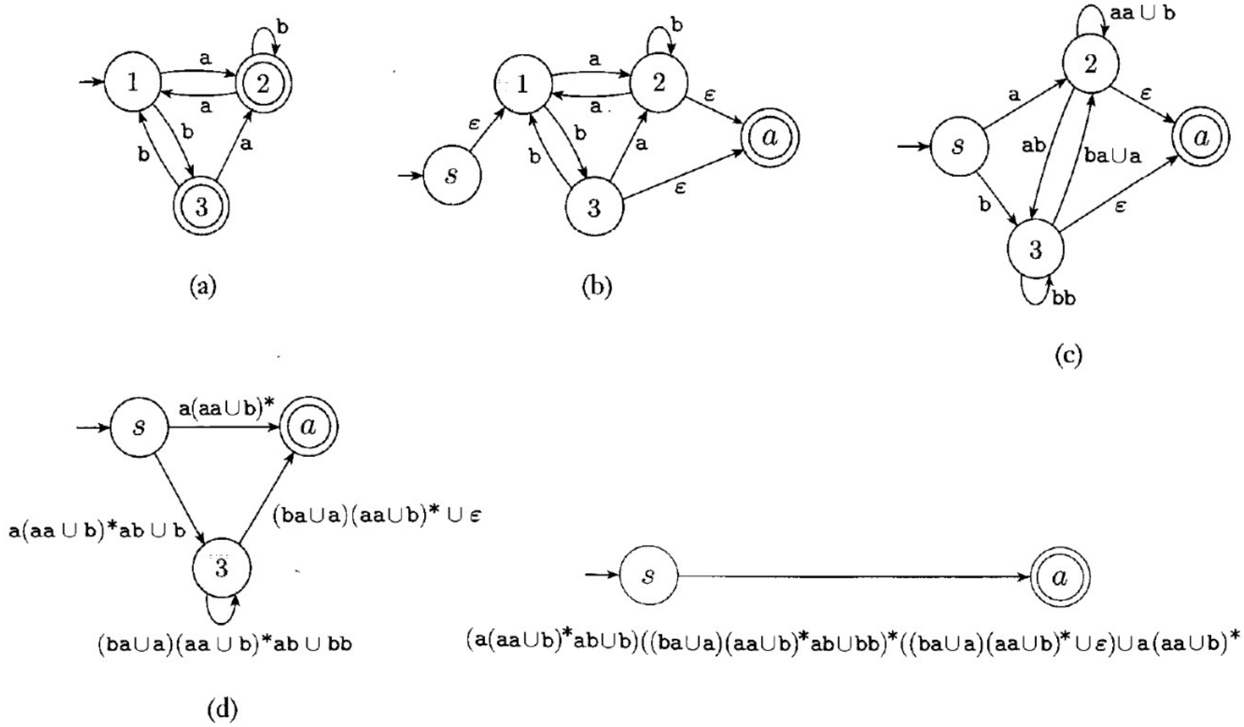
$\Leftarrow$: יהי A DFA ונוכיח שקיים לו ביטוי רגולרי r עם שפה שקולה. נוכיח בדוגמה של הרצת אלג' שמרדד DFA לביטוי רגולרי.

נניח שמותר לנו להשתמש ב-GNFA, שהוא NFA בעל קשתות עם ביטוים רגולריים במקום אותיות. בנוסף, נניח של-A (או ל-NFA המקביל לו) יש מצב התחלתי ומקבל יחיד (קל באמצעות צעדי אפסילון), וכן שהמצב ההתחלתי והמקבל זרים (גם קל עם צעדי אפסילון). ראו דוגמה ל-GNFA,



איור 22: GNFA לדוגמה, אפשר לעבור בין קשתות רק באמצעות מילה שעונה על הביטוי בקשת

עתה נעקוב אחר הדוגמה שלקוחה מהתרגול כי אני לא מזוכיסט, ראו איור ואחריו הנחיה בנוגע למה אנחנו רואים.



איור 23: GNFA לדוגמה, אפשר לעבור בין קשתות רק באמצעות מילה שעונה על הביטוי בקשת

במעבר הראשון אנחנו מוסיפים את המצב ההתחלתי והמקבל החדשים כדי לקיים את ההנחות שלנו.

במעברים הבאים אנחנו מוחקים מצבים (במקרה שלנו אחד כל פעם) ומחלצים מהם ביטוים רגולריים מתאימים עד שנישאר רק עם המצב ההתחלתי והמקבל החדשים. נציג נימוקים לכמה מהצמצומים האלה.

במעבר השני אנחנו מוחקים את 1:

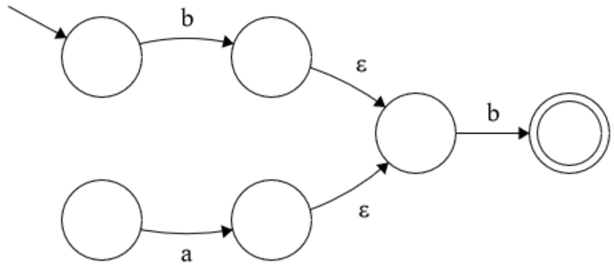
- ל-2 אפשר להגיע דרך 1 מ-s ולכן צמצמנו את צעד האפסילון;
- מ-s ל-3 צריך b ואז רצף כלשהו של bb, לכן יש לנו קשת b וחוג של 3 עם קשת bb;
- כדי להגיע מ-3 ל-2 אפשר או ללכת ישר באמצעות a, או לעבור דרך 1 באמצעות b ואז a, כלומר $ba \cup a$;
- בנוסף, אפשר להגיע ל-2 מ-2 באמצעות סיבוב דרך 3 ו-1 ולכן יש לו חוג סביב עצמו עם ערך $aa \cup b$ מנימוק דומה לנ"ל.

במעבר השני אנחנו מוחקים את 2:

- מ-s ל-a אפשר להגיע או דרך 2 באמצעות a ואיזושהי כמות של סיבובים סביב 2 באמצעות $aa \cup b$.
- מ-3 ל-a אפשר להגיע עם מספר כלשהו של bb וזהו, או דרך 2 עם $ba \cup a$ ואז כמה סיבובי $aa \cup b$, או ישר עם אפסילון.

הרידור האחרון לא מורכב מדי, הוא די ישיר מבחינת האיחודים כי אין יותר מדי אפשרויות, רק לכתוב את זה זה נורא. ■

דוגמה $(a\cup b)\cdot b$, נוכל להרכיב אוטומט ל-a, b, $a\cup b$ ואז $(a\cup b)\cdot b$, זהו כל אחת מהבניות באיור השלם (שימו לב שב-$a\cup b$ שני השניים משמאל היו מקבלים אבל זה הוסר לטובת המצב הסופי).



איור 24: NFA לביטוי הרגולרי הנ"ל

דוגמה תהי $L=\left\{1^{n^2}:n\in\mathbb{N}\right\}$. נראה ש-$L$ לא רגולרית. נניח בשלילה ש-L רגולרית, לכן קיים קבוע ניפוח p כך שלכל מילה $w\in L$ עם $|w|>p$ ניתן לכתוב $w=xyz$ כך ש-$|xy|\le p$, $|y|>0$ ו-$xy^iz\in L$ לכל $i\ge 0$.

נביט במילה $L\ni w=1^{p^2}$ אז $|w|>p$. נכתוב $w=xyz$ כאשר $x=1^j,y=1^k,z=1^l$ ונבחר אותם כך ש-$k>0$ ו-$k+j\le p$.

ננסה לנפח ב-$i=2$. $xy^2z=1^j1^{2k}1^l$ שאורכה $j+2k+l$. נשים לב כי

$$p^2\overset{k>0}{<}p^2+k\overset{k+j\le p}{\le}p^2+p<p^2+2p+1=(p+1)^2$$

כלומר $p^2<\left|xy^2z\right|<(p+1)^2$ ולכן $\left|xy^2z\right|$ אינו ריבוע שלם ולכן הניפוח ב-$i=2$ אינו ב-L, בסתירה לכך של-L רגולרית.

דוגמה $L=\left\{w\in\{0,1\}^*:\#_0w=\#_1w\right\}$. נראה כי L לא רגולרית. בהינתן p קבוע ניפוח, נבחר $w=0^p1^p$ ונכתוב $w=xyz$ כאשר $|xy|\le p$ ו-$|y|>0$ ולכן $x=0^j,y=0^k,z=0^l1^p$ כאשר $k>0,j+k<p$. עבור $i=2$, נקבל את הניפוח

$$xy^2z=0^{j+2k}0^l1^p$$

וברור שיש יותר אפסים מאחדים ולכן הניפוח לא בשפה סתירה.

שבוע $\mathbb{IV}$ | משפט מייהיל-נרוד

הרצאה

חלק א' של ההרצאה

הגדרה $\forall L\subseteq\Sigma^*$, נגדיר יחס $\sim_L\subseteq\Sigma^*\times\Sigma^*$ כך שלכל $x,y\in\Sigma^*$, מתקיים $x\sim_L y$ אם"ם $\forall z\in\Sigma^*$, $x\cdot z\in L\iff y\cdot z\in L$.

הערה מילולית, $x\sim_L y$ אם לא משנה איזו מילה נדביק לסוף של שתיהן, הן או שתיהן יהיו בשפה או שתיהן לא.

דוגמה $L=(0+1)^*0(0+1)$. במקרה כזה $1\nsim_L 0$ כי 0 זנב מפריד ($00\in L$ אבל $10\notin L$).

$\epsilon\sim_L 11\sim_L 1$ כי $\forall z\in\Sigma^*$, $11\cdot z\in L$ אם"ם $z\in L$ אם"ם $1\cdot z\in L$ (מילה היא בשפה אם האות הלפני אחרונה היא 0).

$10\nsim_L 01$ כי ϵ זנב מפריד (המילים עצמן מופרדות כבר).

טענה לכל שפה L, $\sim_L$ היא יחס שקילות.

הוכחה: רפלקסיביות: $\forall x$, $x \sim_L x$.

סימטרי: $\forall x_1, x_2 \in \Sigma^*$, $x_1 \sim_L x_2$ אם"ם $x_2 \sim_L x_1$ כי התנאי עצמו סימטרי.

טרנזיטיביות: $\forall x_1, x_2, x_3 \in \Sigma^*$ אם $x_1 \sim_L x_2$ וגם $x_2 \sim_L x_3$, מתקיים $x_1 \sim_L x_3$ כי אם בשלילה $x_1 \nsim_L x_3$, קיים $z \in \Sigma^*$ כך ש-$x_3 \cdot z \notin L \iff x_1 \cdot z \in L$ (בה"כ על המספור), אבל

$$x_3 \cdot z \notin L \iff x_1 \cdot z \in L \iff x_2 \cdot z \in L \iff x_3 \cdot z \in L$$

סתירה. ■

הערה נסמן $[w]$ מחלקת השקילות של המילה w.

דוגמה עבור L הנ"ל, נמצא את מחלקות השקילות של היחס $\sim_L$.

ϵ ו-0 לא מקיימים את היחס, והמילה 1 מפרידה ביניהם. מתקיים $1 \in [\epsilon]$. 00 מחלקה חדשה, ומפורדת מהשתיים הראשונות ע"י ϵ.
01 גם מחלקה חדשה, וסה"כ המחלקות הן

$$[0] = 0, \Sigma^* 10 \qquad [\epsilon] = \epsilon, 1, \Sigma^* 11 \qquad [00] = \Sigma^* 00 \qquad [01] = \Sigma^* 01$$

הערה נשים לב כי אם $x_1 \sim_L x_2$ וגם $x_3 \sim_L x_4$, ו-z מפריד בין x_1 ו-x_3, אז z מפריד בין x_2 ו-x_4.

ניתן לראות זאת בדוגמה הנ"ל עבור $10 \sim_L 0$ ו-101 $01 \sim_L$ ו-$z = \epsilon$, אכן מתקיים ש-$10 \nsim_L 01$ בין היתר בזכות ϵ.

משפט (מייהיל-נרוד) $\forall L \subseteq \Sigma^*$, אזי $L \in \text{REG}$ אם"ם יש ל-$\sim_L$ מספר סופי של מחלקות שקילות.

הוכחה: $\Rightarrow$: נניח של-$\sim_L$ יש מספר סופי של חלקות שקילות. נגדיר DFA $A = \langle \Sigma, Q, q_0, \delta, F \rangle$ שעבורו $L(A) = L$ נבחר

- Q מחלקות השקילות של $\sim_L$.
- $q_0 = [\epsilon]$.
- $\delta([w], \sigma) = [w \cdot \sigma]$.
- $F = \{[w] : w \in L\}$.

נשים לב שהגדרה של δ, F לא תלויה בבחירת הנציג (w) כי הרבה מאוד מצבים הם בעלי אותו נציג (אם $w \sim_L y$ אז $[w\sigma] = [y\sigma]$, $\forall z$ כי אחרת σz מפריד של y, w).

נוכיח שלכל $w \in \Sigma^*$, $\delta^*(q_0, w) = [w]$ ולכן מהגדרת F, $w \in L$ אם"ם $\delta^*(q_0, w) = F$ ונסיים. באינדוקציה על $|w|$.

בסיס ($w = \epsilon$): $w = \epsilon$ ואכן $\delta^*(q_0, \epsilon) = q_0 = [\epsilon]$.

צעד ($|w| \to |w| + 1$):

$$\begin{aligned}\delta^*(q_0, u \cdot \sigma) &= \delta(\delta^*(q_0, u), \sigma) \\ &\overset{\text{ה"א}}{=} \delta([u], \sigma) \\ &\overset{\text{הגדרה}}{=} [u\sigma]\end{aligned}$$

$\Leftarrow$: נניח ש-$A = \langle \Sigma, Q, q_0, \delta, F \rangle$ הוא DFA שמזז את L ונראה של-$\sim_L$ מספר סופי של מחלקות שקילות. נחסום את המספר הזה עם מספר המצבים ונסיים.

נגדיר יחס $\sim_A \subseteq \Sigma^* \times \Sigma^*$ ונאמר כי $x, y \in \Sigma^*$ מקיימות $x \sim_A y$ אם"ם $\delta^*(q_0, x) = \delta^*(q_0, y)$.

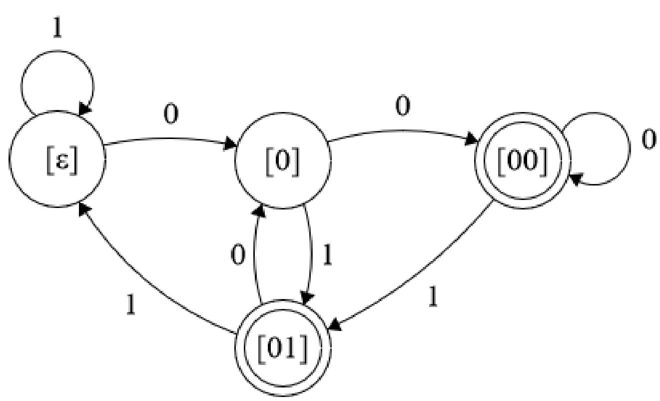
אם $x \sim_A y$ אז אין להן זנב מפריד כי xz, yz נפגשות אחרי x, y ומשם ממשיכות יחד בריצה על z ולכן תמיד יגיעו לאותו המקום, ולכן $x \sim_L y$, ופורמלית, אם $x \sim_A y$ אז $\forall z \in \Sigma^*$,

$$\delta^*(q_0, xz) = \delta^*(\delta^*(q_0, x), z) = \delta^*(\delta^*(q_0, y), z) = \delta^*(q_0, yz)$$

ולכן $yz \in L \iff xz \in L$ ולכן $x \sim_L y$.

מכאן שמספר מחלקות השקילות של $\sim_A$ חוסם את מספר מחלקות השקילות של $\sim_L$, והראשון חסום ע"י $|Q|$ ולכן גם האחרון ולכן הוא סופי. ■

דוגמה נפעיל את המשפט על הדוגמה הנ"ל ($L = (0+1)^* 0 (0+1)$),



איור 25 : אוטומט שמתאים לשפה L

כאשר בנינו כל קשת ע"י בדיקה של היכן נמצא הנציג יחד עם האות על הקשת, לדוגמה $[01]$ עם 0 הולך ל-0 כי 010 הוא במחלקת השקילות של 0, ושאר הקשתות בהתאם.

שימושים של משפט MN

1. סיווג ל-REG או לא REG.

דוגמה $L = \{0^n 1^n : n \geq 0\}$ אינה רגולרית כי $\forall i \neq j \geq 0$, $0^i \nsim 0^j$ כי 1^i זנב מפריד ($0^i 1^i \in L$ אבל $0^j 1^j$ לא) ולכן יש אינסוף מחלקות שקילות ל-$\sim_L$ וסיימנו.

דוגמה $L = \left\{0^i 1^j : \gcd(i,j) \neq 1\right\}$. נראה שעבור שני ראשוניים, $p_1 \neq p_2$, $0^{p_1} \nsim_L 0^{p_2}$ (כאן $j = 0$). נשים לב כי 1^{p_1} הוא זנב מפריד (כי $0^{p_1} 1^{p_1} \in L$ אבל $0^{p_2} 1^{p_1}$ לא). לכן ל-$\sim_L$ ∞ מח"ש.

2. צמצום/מזעור DFA-ים.

הרעיון הוא שאם לאוטומט יש יותר מצבים ממחלקות שקילות ל-$\sim_L$, אפשר לצמצם את ה-DFA עוד. נראה אלג' שבהנתן DFA $A = \langle \Sigma, Q, q_0, \delta, F \rangle$, נחזיר DFA A' שקול ל-A כך שלכל DFA A'', אם $L(A'') = L(A)$, אז $|A'| \leq |A''|$ (A' DFA מינימלי עבור $L(A)$). מעבר לכך, נראה שאוטומט זה הוא יחיד עד כדי שמות.

מזעור אוטומטים

נגדיר סדרה של יחסים $Q \times Q$ $\sim_i$, $\forall i \geq 0$. הרעיון הוא ש-$s_1 \sim_i s_2$ אם"ם $\forall z \in \Sigma^*$ עם $|z| \leq i$, $\delta^*(s_2, z) \in F \iff \delta^*(s_1, z) \in F$.

כלומר אינטואיטיבית $s_1 \sim_i s_2$ אם s_1, s_2 מסכימות על אילו מילים עד אורך i מתקבלות (כשהריצה מתחילה מהן).

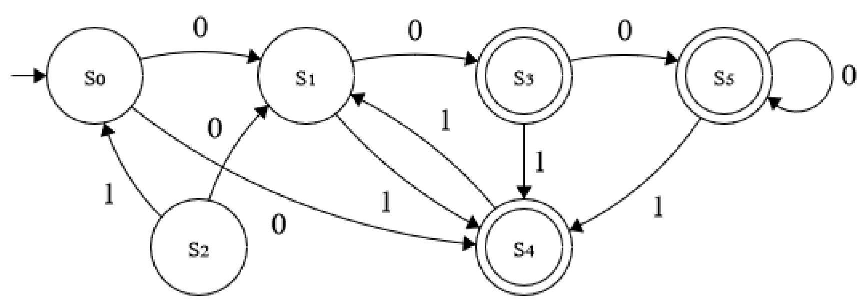
ככל ש-i יותר גדול, כך יש יותר מילים שצריך שהתנאי הזה יתקיים עליהן ולכן מחלקות השקילות שלו יגדלו (ומספרן יגדל). מתישהו נפסיק לעדן את מחלקות השקילות ומחלקות השקילות שנקבל יספקו לנו את המצבים ל-DFA המינימלי.

הגדרה נגדיר את הסדרה $\sim_i$ באופן אינדוקטיבי.

בסיס ($i = 0$): $s_1 \sim_0 s_2$ אם"ם $s_2 \in F \iff s_1 \in F$ (ויש לו שתי מחלקות שקילות, כל המקבלים וכל הלא מקבלים).

צעד ($i \to i+1$): נגדיר $s_1 \sim_{i+1} s_2$ אם"ם $s_1 \sim_i s_2$ וגם $\delta(s_1, \sigma) \sim_i \delta(s_2, \sigma)$, $\forall \sigma \in \Sigma^*$ (כלומר אם s_1, s_2 מסכימים על מילים באורך i וגם על כל הארכה באורך 1).

דוגמה נביט באוטומט הבא שמזהה את השפה $L = (0+1)^* 0 (0+1)$,



איור 26 : אוטומט שמתאים לשפה L

עבור $\sim_0$, מחלקות השקילות שלנו הן

$$\{\{s_0, s_1, s_2\}, \{s_3, s_4, s_5\}\}$$

עבור מילים באורך 1, נעדן את מחלקת השקילות. האם $s_0 \sim_1 s_1$? מתקיים $s_0 \sim_0 s_1$ אבל $s_3 = \delta(s_1, 0) \nsim_0 \delta(s_0, 0) = s_1$ ולכן התשובה היא לא. עם זאת $s_0 \sim_1 s_2$ כן מתקיים כי הפעלה של 0 ו-1 מובילות אותנו למצבים שהם באותה מחלקת שקילות בהתאמה. אחרי חישוב מקבלים שמחלקות השקילות ל-$\sim_1$ הן

$$\{\{s_0, s_1\}, \{s_2\}, \{s_3, s_5\}, \{s_4\}\}$$

ואז עבור $\sim_2$ מקבלים את אותה מחלקת שקילות ושם נעצור (הגענו לנקודת שבת) ואכן ארבעת המחלקות הללו נותנות לנו אוטומט מזערי.

חלק ב' של ההרצאה

נביט בסדרת היחסים שהגדרנו $\{\sim_i\}$ (שכל אחד מהם אוסף זוגות של מצבים). בהכרח שעבור i גדול מספיק, נקבל $\sim_i = \sim_{i+1}$ (שוויון בין קבוצות המוכלות ב-$Q \times Q$) כי אם $s_1 \sim_{i+1} s_2$ אז $s_1 \sim_i s_2$ ולכן $\sim_{i+1} \subseteq \sim_i$.

מכאן שאו שהגענו לנקודת שבת ונעצור, או שהורדנו לפחות זוג אחד מ-$\sim_i$, ולכן תוך לכל היותר $|Q|^2$ איטרציות נעצור.

בנוסף, המעבר מ-$\sim_i$ ל-$\sim_{i+1}$ מתבצע בזמן פולינומיאלי, שכן יש מספר פולינומיאלי של זוגות (לכל היותר $|Q|^2$) וחישוב האם זוג עובר ליחס הבא או לא דורש זמן קבוע.

טענה לכל $i \geq 0$ ו-$s_1, s_2 \in Q$, מתקיים $s_1 \sim_i s_2$ אם"ם לכל מילה w באורך $\leq i$, $\delta^*(s_1, w) \in F \iff \delta^*(s_2, w) \in F$.

הערה בתרגיל נוכיח שזה מספיק כדי להראות שמחלקות השקילות מהוות מצבים לאוטומט המזערי.

הוכחה: נראה באינדוקציה על i:

בסיס ($i = 0$): $w = \epsilon$. מההגדרה $(\delta^*(s_1, \epsilon) = s_1 \in F \iff \delta^*(s_2, \epsilon) = s_2 \in F) \iff s_1 \sim_0 s_2$.

צעד ($i \to i+1$):

$\Leftarrow$: נניח ש-$s_1 \sim_{i+1} s_2$ נוכיח שלכל מילה w, אם $|w| \leq i+1$, אז $\delta^*(s_1, w) = \delta^*(s_2, w) \in F$. תהי w כנ"ל.

- אם $|w| \leq i$, $s_1 \sim_{i+1} s_2$ ולכן $s_1 \sim_i s_2$ ולכן מה"א הטענה מתקיימת עבור w.
- אם $i = |w| + 1$ אז $w = \sigma y$ עבור $\sigma \in \Sigma, y \in \Sigma^*$ ומהגדרת $\sim_{i+1}$,

$$s_1' = \delta(s_1, \sigma) \sim_i \delta(s_2, \sigma) = s_2'$$

ולכן מה"א (עבור y שהיא באורך i)

$$\delta^*\left(s_1',y\right)\in F\iff\delta^*\left(s_2',y\right)\in F$$

ולכן

$$\delta^*\left(s_1,\sigma y\right)=\delta^*\left(\delta\left(s_1,\sigma\right),y\right)\in F\overset{\text{הביטוי הנ"ל}}{\iff}\delta^*\left(\delta\left(s_2,\sigma\right),y\right)\in F=\delta^*\left(s_2,\sigma y\right)$$

כלומר w מקיימת את התנאי.

$\Rightarrow$: נניח ש-s_1,s_2 מסכימים מילים עד לאורך $i+1$ ונוכיח ש-$s_1\sim_{i+1}s_2$.

נניח בשלילה ש-$s_1\nsim_{i+1}s_2$. לכן או ש-$s_1\nsim_i s_2$ או שקיימת $\sigma\in\Sigma$ כך ש-$\delta\left(s_1,\sigma\right)\nsim_i\delta\left(s_2,\sigma\right)$ (מההגדרה).

אם $s_1\nsim s_2$, קיימת מילה y באורך $\leq i$ כך ש-$\delta\left(s_1,y\right)\nsim_i\delta\left(s_2,y\right)$ כלומר s_1,s_2 לא מסכימים על מילה באורך i סתירה.

אם קיימת σ כך ש-$\delta\left(s_1,\sigma\right)\nsim_i\delta\left(s_2,\sigma\right)$, אז $\delta\left(s_1,\sigma\right),\delta\left(s_2,\sigma\right)$ הם מצבים לא ביחס $\sim_i$ ולכן מה"א הם לא מסכימים על השפה עד אורך $\leq i$.

כלומר, קיימת y עם $|y|\leq i$ כך ש-$\delta^*\left(\delta\left(s_1,\sigma\right),y\right)\in F$ אבל $\delta^*\left(\delta\left(s_2,\sigma\right),y\right)\notin F$ בסתירה לכך ש-s_1,s_2 מסכימים על מילים באורך $i+1$. ■