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.

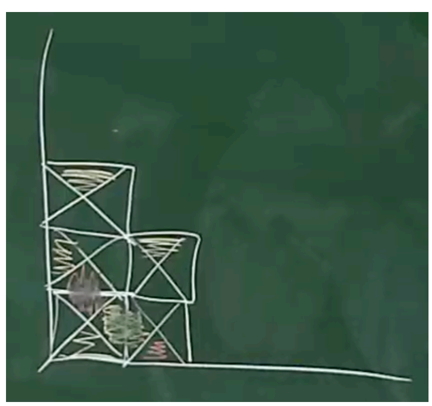
מעגל המילטון הוא מעגל שעובר בכל קודקוד בדיוק פעם אחת. לבעיה הזו אין אפיון מתמטי, והוכח שאין אלג' יותר טוב מאשר מעבר על כל האפשרויות, בסיבוכיות אקספוננציאלי.

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

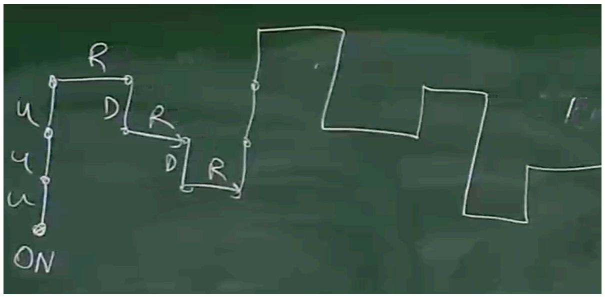
פלט: האם P עוצרת על x.

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

אוטומטים

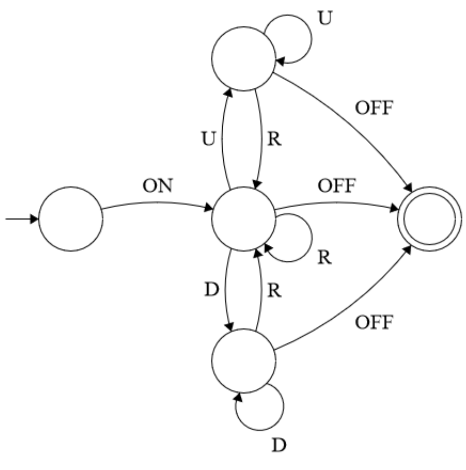
הגדרה אוטומט הוא מחשב עם זכרון מוגבל.

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 $\{0,1\}^4$, $\Sigma = \{0,1\}$ 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 $\Sigma^* = \{w : \Sigma$ 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).

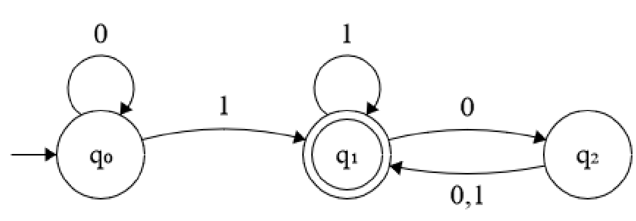
A מקבל את w אם הריצה של A על w היא מקבלת.

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

דוגמה עבור A_1, $L(A_1) = \{w :$ 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 $\Sigma \times Q$ 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

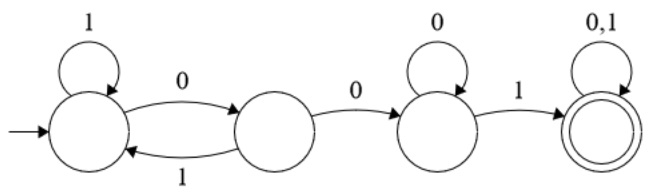
נסמן בצבע האם כמה מילים נבחרות הן בשפה או לא, 00000, 11, 1, 001110, 011, 010.

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.

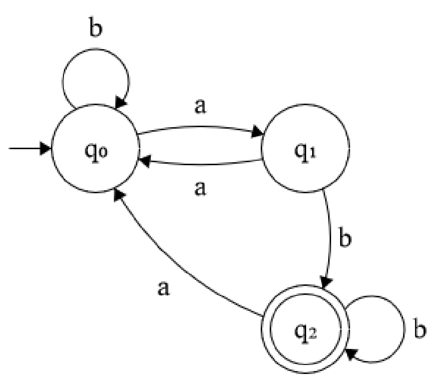
דוגמה בהינתן שפה, ננסה לחשב את האוטומט. השפה היא $L_3 = \{w : 001 \text{ מכילה את הרצף } w\}$.



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-$L(A) = L$.

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 <u>עוצמה</u> 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 $|B| \leq |A|$ אם יש העתקה חח"ע מ-A ל-B ו-$|B| < |A|$ אם בנוסף אין העתקה חח"ע מ-A על B.

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

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

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

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

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

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

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

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 $L\in P\left(\Sigma^*\right)$.

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

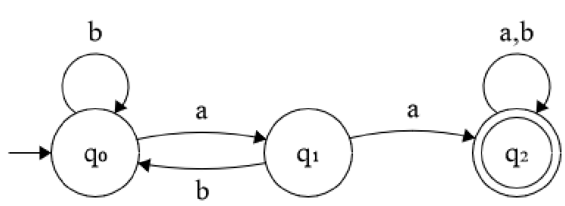
כמה שפות יש מעל Σ^*? $2^{|\Sigma^*|}=2^{\aleph_0}$.

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 $\delta^*\left(q,w\right)=\begin{cases} q & w=\epsilon\\ \delta\left(\delta^*\left(q,w'\right),\sigma\right) & w=w'\sigma,\sigma\in\Sigma\end{cases}$.

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 $x \in [0,\dots,9]^*$, $a \in \{0,\dots,9\}$ 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 $w \in \{0,\dots,9\}^*$ אז מטבענת העזר $\delta(q_0, w) = \langle S(w), 1\rangle \neq q_{acc}$.
- אם $w \in \{0,\dots,9\}^* \times \{\#\}$ 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 $L(A) = L(A_1) \cup L(A_2)$.

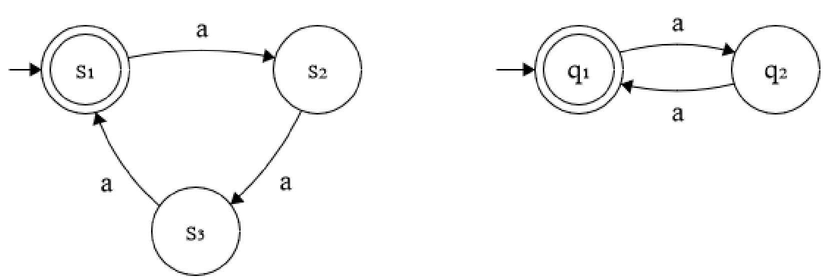
הרעיון הוא ש-A מסמלץ את A_1 ו-A_2 יחד, ואוטומט בבנייה כזו נקרא אוטומט המכפלה. נבחר $Q = Q_1 \times Q_2$, $s_0 = \langle s_1, s_2 \rangle$, ופ' מעברים

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

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

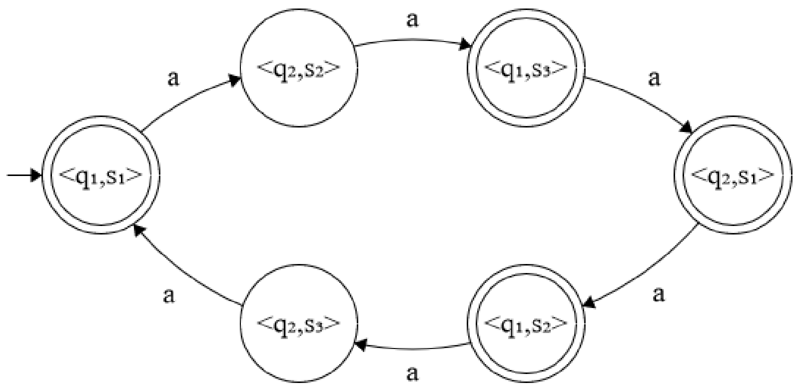
הערה אם $L \subseteq \{a\}^*$ אז היא מגדירה תת קבוצה של $\mathbb{N}$ - כל האורכים של מילים בשפה, כלומר $\{i : a^i \in L\}$.

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 $L(A)=\{w:|w| \mod 2=0 \vee |w| \mod 3=0\}$.

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 $r_i=\langle q_1^i,q_2^i\rangle$. 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.

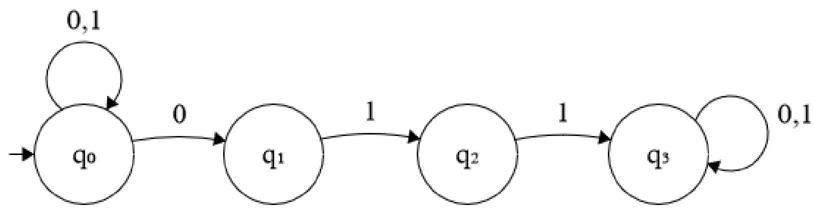
מכאן, r מקבלת אם"ם $\langle q_1^n,q_2^n\rangle\in F$ אם"ם $q_1^n\in F_1$ או $q_2^n\in F_2$ אם"ם r_1 מקבלת או r_2 מקבלת אם"ם $w\in L(A_1)$ או $w\in L(A_2)$.

■

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

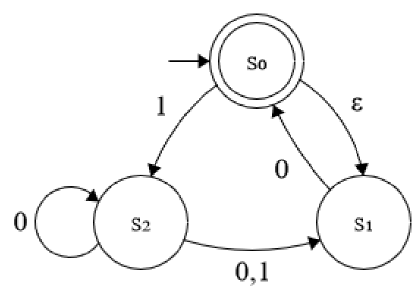
לכאורה פ' המעברים לא מוגדרת היטב עבור $q_0, 0$, אבל כאן הרעיון הוא שהאוטומט יכול לבחור מתוך כמה אפשרויות בעצמו לאיזה מצב הוא עובר, כאשר מילה מתקבלת ע"י האוטומט אם"ם קיימת ריצה עם ניחושים כלשהם שמקבלת, ובמקרה כזה נגדיר $\delta\left(q_0, 0\right) = \{q_0, q_1\}$.

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"

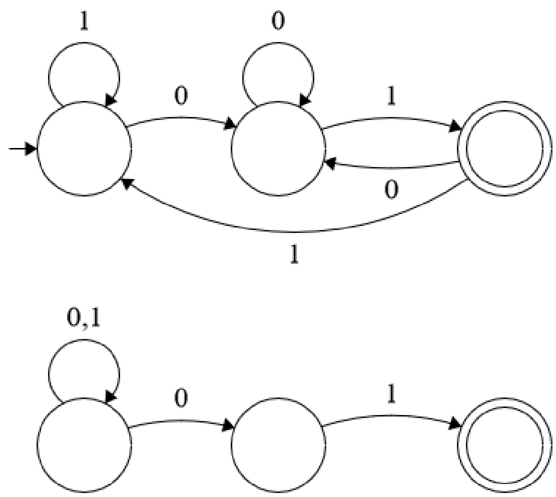
המילים הבאות מתקבלות: $\epsilon, 0, 00, 00110$ (כי נוכל להשתמש קודם בצד אפסילון במקום ליפול לבור דוחה מ-s_0) ואילו $001, 00111$ לא מתקבלות.

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 $r_m\in F$.

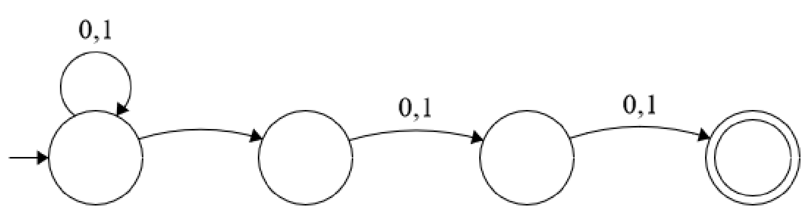
נאמר כי A מקבלת את w אם"ם קיימת ריצה של A על w שמקבלת.

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),



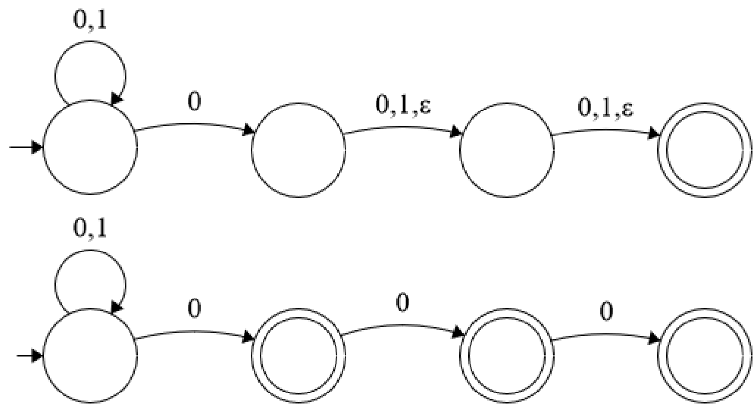
איור 12 : אוטומט דטרמיניסטי (למעלה) ואי-דטרמיניסטי (למטה) שמשרתים אותה המטרה

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',



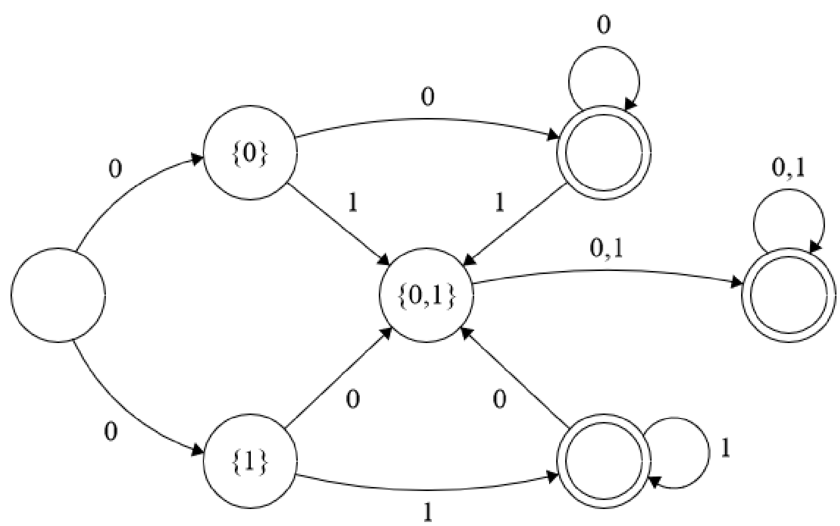
איור 14 : שני אוטומטים אי-דטרמיניסטיים ששפתם L'

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.

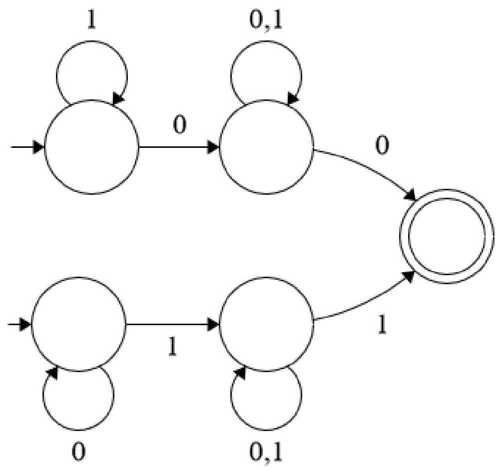
חלק ב' של ההרצאה

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

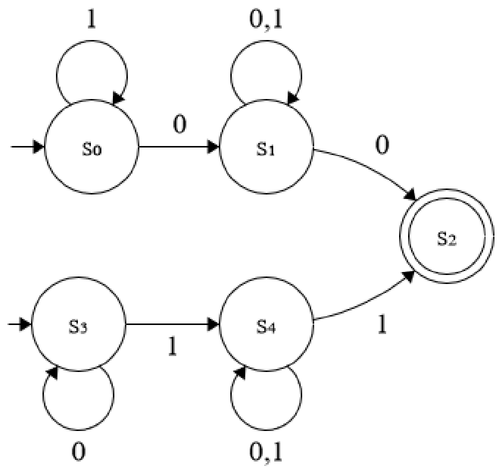
צעד $(|w| \to |w+1|)$:

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

■

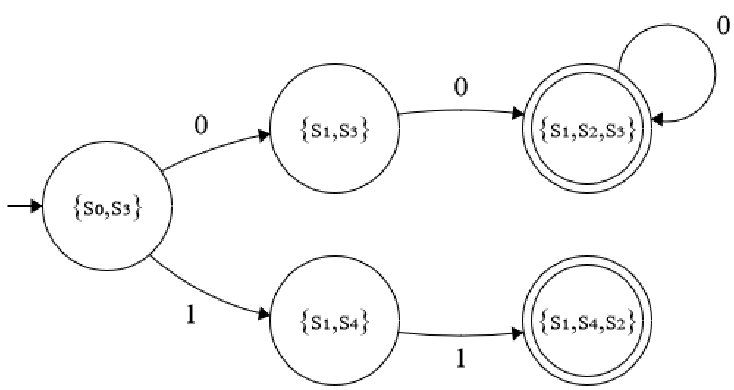
וזה מסיים את ההוכחה כי השפות של האוטומטים שוות. ■

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

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

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.

<u>$L_1 \cup L_2 \subseteq L(B)$</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 $r_0 \in \{q_1, q_2\}$, 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 $w \in L(B)$.

<u>$L(B) \subseteq L_1 \cup L_2$</u>: 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 $0 \leq i \leq |w| - 1$ 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 $r_0, \ldots, r_{|x|}$ 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 $L^* = \bigcup_{k \in \mathbb{N}_0} \underbrace{L \cdot \ldots \cdot L}_{k \text{ פעמים}} \in \text{REG}$.

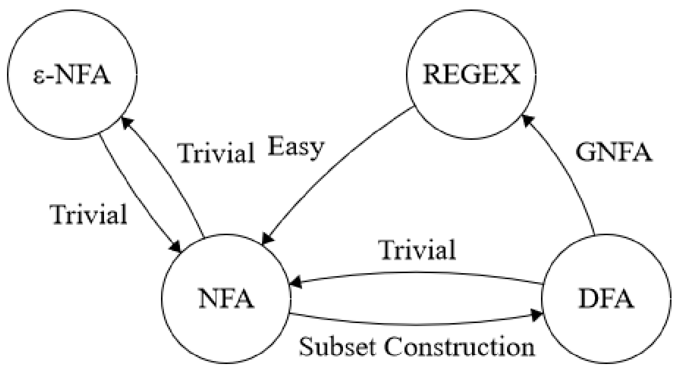
הוכחה: יהי $A = \langle Q, \Sigma, \delta, q_0, F \rangle$ DFA ל-L. לכאורה היינו יכולים לבנות NFA שהוא A פשוט עם חיבור מהמצבים הסופיים למצב ההתחלתי שוב עם צעד אפסילון. הבעיה היא שאם A לא מקבל את המילה הריקה, גם הבניה לא אבל $\epsilon \in L^*$. לכן נוסיף מצב נוסף q_{start} שהוא יהיה המצב ההתחלתי היחיד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

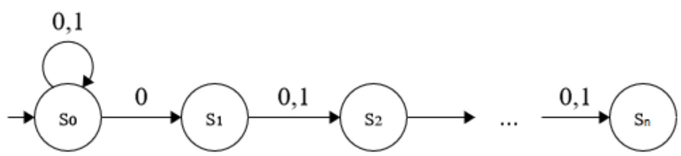
הוכחה: מספיק שנראה שלכל $n\geq1$ קיימת L_n כך של-L_n קיים NFA עם $n+1$ מצבים אבל ה-DFA הקטן ביותר עבור L_n צריך לפחות 2^n מצבים.

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

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

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 $w_2\cdot1^{i-1}$ בסתירה לנכונות D_n, שכן $w_2\cdot1^{i-1}\notin L$ (האות ה-n מהסוף היא $w_2[i-1]$).
- 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 $L=\{0^n1^n:n\geq0\}$.

הוכחה: נניח בשלילה כי $A=\left\langle Q,\Sigma,q_{)},\delta,F\right\rangle$ הוא DFA עם $L\left(A\right)=L$. יהי $\left|Q\right|=p$. 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 $0\leq l<j\leq p$ 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 $p\geq1$ (קבוע הנפוח) כך שלכל מילה $w\in L$, אם $\left|w\right|\geq p$ אז קיימת חלוקה $w=x\cdot y\cdot z$ כך ש:

1. $\left|x\cdot y\right|\leq p$.
2. $\left|y\right|>0$ ($y\neq\epsilon$).
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 $\left|w\right|\geq3$.
נבחר $w=x\cdot y\cdot z$ כאשר $x=\epsilon,\left|y\right|=1,\left|z\right|=\left|w\right|-1$.

אכן $y\neq\epsilon$ וכמובן $\left|x\cdot y\right|=1\leq3$ ולכל $i\geq0$, $xy^{i}z\in L$ כי $\left|z\right|\geq2$ 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 $\left|w\right|\geq p$. בריצה של A על w, יש מצב שחוזר בקריאת p האותיות הראשונות, כלומר קיימים $0\leq j<l\leq p$ 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 $\left|y\right|>0$, $\left|x\cdot y\right|\leq p$ 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-$\alpha\Leftarrow L\in\mathrm{REG}$, אז $\neg\alpha$ הוא שלכל $p\geq1$, קיימת מילה $w\in L$ עם $\left|w\right|\geq p$ כך שלכל חלוקה $w=x\cdot y\cdot z$, אם $\left|x\cdot y\right|\leq p$ וגם $\left|y\right|>0$, 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.

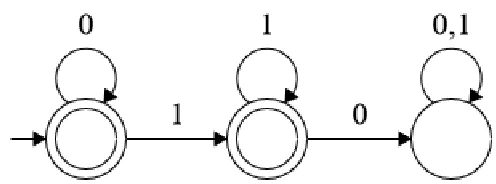
את הבחירה על השלילה של שלושת התנאים עשינו כי זה נוח אבל אפשר היה גם לעשות שאם $1, 3$ מתקיימים אז 2 לא מתקיים.

דוגמאות לשפות לא רגולריות

1. תהי $L_1 = \{0^n 1^n : n \geq 0\}$. 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. $L_6 = \{a^p : p$ 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 $\left|xy^iz\right| = m\left(\left(q+1\right)-1\right)+q = \left(m+1\right)q$ 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 $|xy| \leq p$ 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 $L\left(r\right) = \varnothing$.
- אם $r = \epsilon$ אז $L\left(r\right) = \{\epsilon\}$.
- אם $r = a \in \Sigma$ אז $L\left(r\right) = \{a\}$.
- אם $r = s \cdot t$ אז $L\left(r\right) = L\left(s\right) \cdot L\left(t\right)$.
- אם $r = s \cup t$ אז $L\left(r\right) = L\left(s\right) \cup L\left(t\right)$.

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

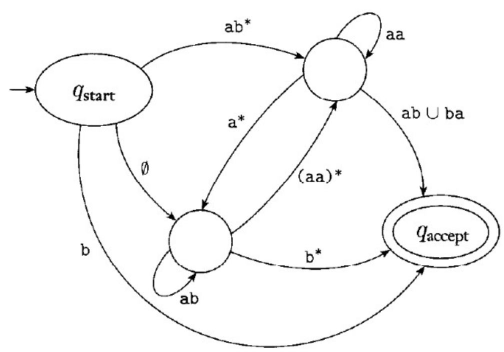
הוכחה: $\Rightarrow$: יהי r ביטוי רגולרי ונראה שקיים NFA A_r כך ש-$L\left(r\right) = L\left(A_r\right)$ באינדוקציה על אורך סדרת היצירה של r (מספר התווים בכתיבה של הביטוי הרגולרי, כך ϵ הוא באורך 1 לדוגמה).

- 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-$L\left(A_t\right)^*$.

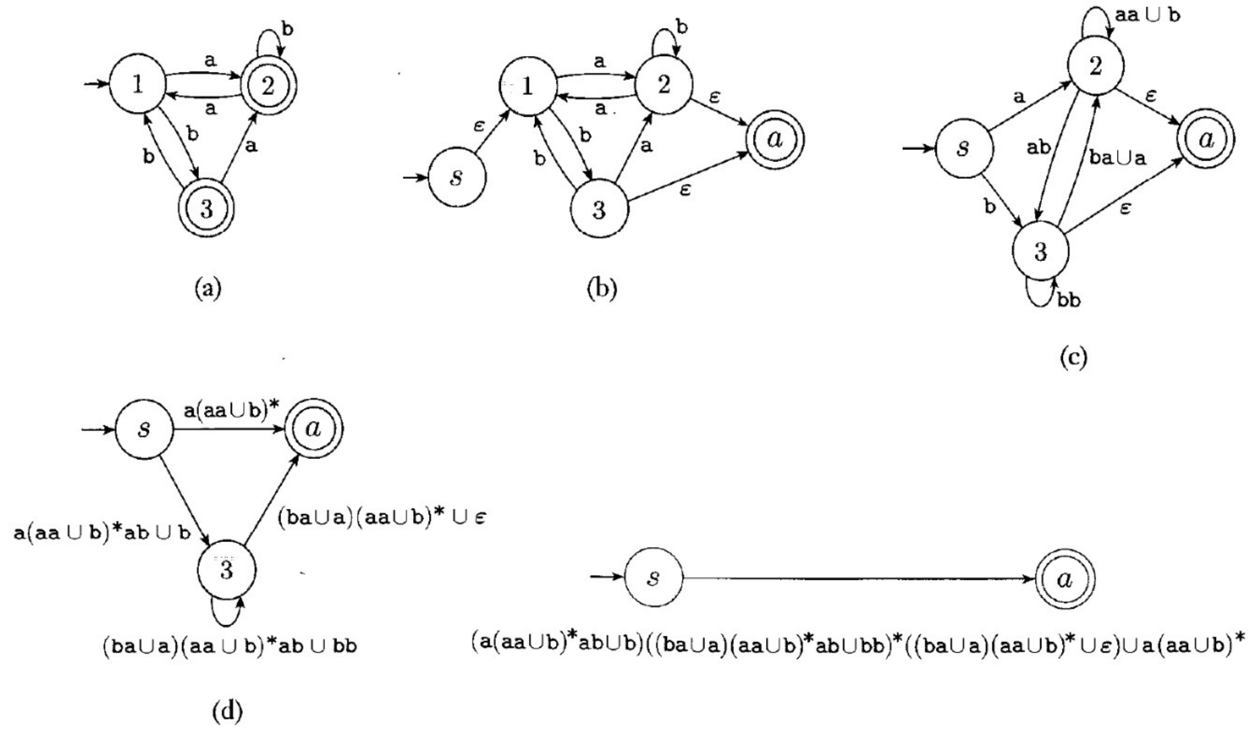
$\Leftarrow$: יהי A DFA ונוכיח שקיים לו ביטוי רגולרי r עם שפה שקולה. נוכיח בדוגמה של הרצת אלג' שמרדד DFA לביטוי רגולרי.

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 :

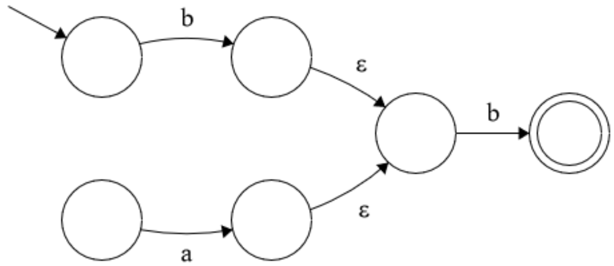
- ל-2 אפשר להגיע דרך 1 מ-s ולכן צמצמנו את צעד האפסילון ;
- מ-s ל-3 צריך b ואז רצף כלשהו של bb, לכן יש לנו קשת b וחוג של 3 עם קשת bb ;
- כדי להגיע מ-3 ל-2 אפשר או ללכת ישר באמצעות a, או לעבור דרך 1 באמצעות b ואז a, כלומר $ba \cup a$;
- בנוסף, אפשר להגיע ל-2 מ-2 באמצעות סיבוב דרך 3 ו-1 ולכן יש לו חוג סביב 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-$101 \sim_L 01$ ו-$z = \epsilon$, אכן מתקיים ש-$10 \nsim_L 01$ בין היתר בזכות ϵ.

משפט (מייהיל-נרוד) $\forall L \subseteq \Sigma^*$, אזי $L \in \mathrm{REG}$ 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 $\delta^*(q_0, x) = \delta^*(q_0, y)$.

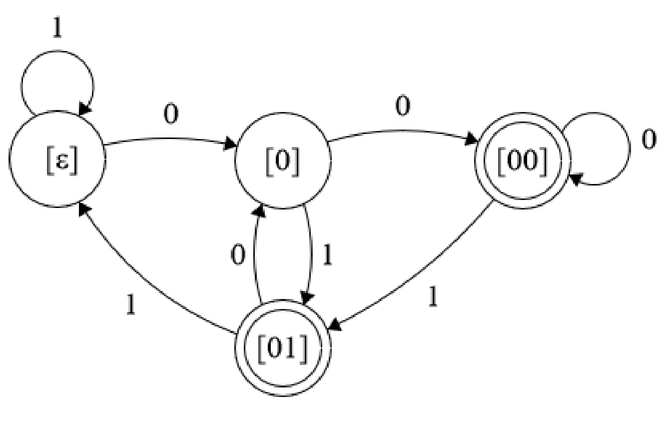
אם $x \sim_A y$ אז אין להן זנב מפריד כי xz, yz נפגשות אחרי x, y ומשם ממשיכות יחד בריצה על z ולכן תמיד יגיעו לאותו המקום, ולכן $x \sim_L y$, ופורמלית, אם $x \sim_A y$ אז $\forall z \in \Sigma^*$,

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

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).

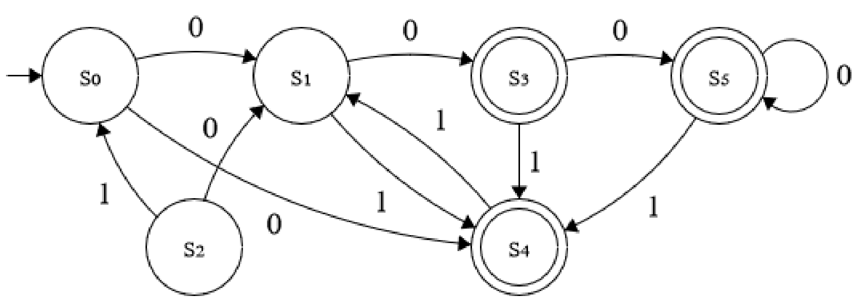
ככל ש-i יותר גדול, כך יש יותר מילים שצריך שהתנאי הזה יתקיים עליהן ולכן מחלקות השקילות שלו יגדלו (ומספרן יגדל). מתישהו נפסיק לעדן את מחלקות השקילות ומחלקות השקילות שנקבל יספקו לנו את המצבים ל-DFA המינימלי.

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 $s_1 = \delta(s_0, 0) \nsim_0 \delta(s_1, 0) = s_3$ 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 $\sim_i \subseteq \sim_{i+1}$.

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 $\geq i$, $\delta^*(s_2, w) \in F \iff \delta^*(s_1, w) \in F$.

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 $|w| \geq i+1$, אז $\delta^*(s_1, w) = \delta^*(s_2, w) \in F$. תהי w כנ"ל.

- אם $|w| \geq i$, $s_1 \sim_{i+1} s_2$ 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)

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

ולכן

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

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-$\delta(s_1,\sigma)\nsim_i\delta(s_2,\sigma)$ (מההגדרה).

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

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

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

תרגול

טענה תהי $f:\mathbb{N}\to\mathbb{N}$ מונוטונית עולה ממש כך ש-$f(n)$ היא $\omega(n)$, אזי השפה $L_f=\left\{a^{f(n)}:n\in\mathbb{N}\right\}$ לא רגולרית.

הוכחה: נשתמש בלמת הניפוח ע"י מציאה לכל n, מילה באורך בין $f(n)$ ל-$f(n+1)$, ונסיים.

טענת עזר תהי f כנ"ל. אזי $\forall K,N\in\mathbb{N}$, קיים $n>N$ כך ש-$f(n+1)-f(n)>K$ (כלומר נצליח לחסום ממתחת את ההפרשים בין האיברים, עבור מספרים מספיק גדולים).

הוכחה: (של טענת העזר) נניח בשלילה שלא קיים, לכן קיימים $K,N\in\mathbb{N}$ שעבורם $\forall n>N$, $f(n+1)-f(n)\le K$. בפרט, קיים $M\in\mathbb{N}$ כך ש-$f(n+1)-f(n)\le M$ (מקסימום ההפרשים עד N).

לכן מתקיים $f(2)-f(1)\le M$, ואז $f(3)\le f(2)+M\le f(1)+2M$ ובצעד ה-n-י, $f(n)\le(n-1)M+f(1)$ ולכן

$$\frac{f(n)}{n}\le\frac{n-1}{n}M+\frac{f(1)}{n}\underset{n\to\infty}{\longrightarrow}M+0$$

ולכן ממונוטוניות הגבול, $\lim\limits_{n\to\infty}\frac{f(n)}{n}\le M$ בסתירה לכך שהגבול הזה הוא ∞ מהגדרת ω. ■

נחזור לטענה. נניח בשלילה שלמת הניפוח מתקיימת ויהי $p>0$ קבוע הניפוח. נבחר $N=K=p$ ונביט במילה $a^{f(n)}$ עבור $n>p$ שמטענת העזר, מקיים $f(n+1)-f(n)>k$. נבחר $w=xyz=a^la^ma^s$ כאשר $l+m+s=f(n)$, $l+m\leq p$ ו-$m>0$.

נביט ב-xy^2z. $\left|xy^2z\right|=f(n)+m$ ומתקיים

$$f(n)<f(n)+m\leq f(n)+p<f(n+1)$$

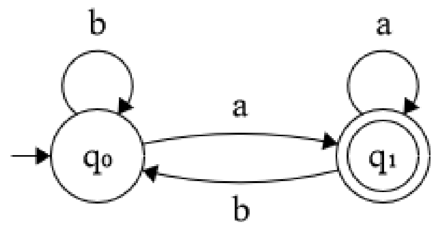
כאשר המעבר הראשון והשני נובעים מהתנאים של למת הניפוח על l,m והמעבר השלישי נובע מתטענת העזר ($p=K$). לכן $xy^2z\notin L$ בסתירה ללמת הניפוח.

למעשה המעבר המהותי הוא שניפחנו ב-m את המילה, אבל m קטן מאשר החסם התחתון שמצאנו להפרש ולכן הוא לא במילה. ■

הערה בכתיבה מתמטית נטו, יחס השקילות שמוגדר במייהיל-נרוד מוגדר באופן הבא,

$$\forall x,y\in\Sigma^*\left(x\sim_L y\iff(\forall z\in\Sigma^*,xz\in L\iff yz\in L)\right)$$

דוגמה נביט בשפה $L=\left\{w\in\Sigma\left\{a,b\right\}^*:w\text{ מסתיימת ב-}a\right\}$. היא רגולרית כי האוטומט הבא מזהה אותה.



איור 27: אוטומט שמתאים לשפה L

נוכיח זאת עם MN. נסתכל על המילים בשפה באופן שיטתי.

- אם $x,y\in\Sigma^*$ מסתיימות ב-a: $xz\in L$ אם"ם $z=\epsilon$ או ש-z עצמה מסתיימת ב-a (וזה אותו התנאי על y) ולכן $x\sim_L y$ וזו מחלקת שקילות אחת.
- אם $x,y\in\Sigma^*$ לא מסתימות ב-a: $xz\in L$ אם"ם z מסתיימת ב-a (באותו האופן על y) ולכן $x\sim_L y$ וזו עוד קבוצה במחלקת שקילות, עדיין לא ידוע אם שונה מהקודמת.
- אם x לא מסתיימת ב-a ו-y מסתיימת ב-a: $x\nsim_L y$ כי $z=\epsilon$ זנב מפריד, ולכן שתי מחלקות השקילות הנ"ל שונות ומיפינו את כל המרחב לשתי מחלקות שקילות.

דוגמה נביט בשפה $L=\{w:2\text{ מאורך שאינו חזקה של }w\}$. מעל $\Sigma=\{a\}$. ראינו שהמשלימה של השפה הזו היא לא רגולרית ולכן נצפה שגם זו תהיה (אחרת נוכל לבנות אוטומט עם מצבים מקבלים הפוכים).

נראה ש-L לא רגולרית ע"י מציאת אינסוף מח"ש ל-$\sim_L$. יהיו $m > n \in \mathbb{N}$. נביט במילים $x = a^{2^n}, y = a^{2^m}$, שתיהן ב-Σ^* (ולא ב-L אבל זה לא מעניין). נשים לב שעבור $z = a^{2^n}$ נקבל ש-$xz = a^{2^{m+1}} \in L$ אבל $yz = a^{2^n\left(2^{m-n}+1\right)} \notin L$ ולכן $x \nsim_L y$.

כלומר, לכל $m > n$, x, y כנ"ל מצאות במח"ש שונות ויש אינסוף זוגות מספרים כאלה ולכן יש ∞ מח"ש ל-$\sim_L$.

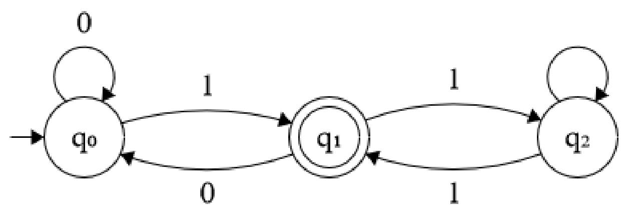
תרגיל יהי $A = \langle Q, \{0,1\}, q_0, \delta, F\rangle$ DFA עם $|Q| = r$. נתון ש-$0^r1^r \in L(A)$. מה מהבאים נכון בהכרח?

1. $0^*1^* \subseteq L(A)$.
2. $L(A) \subseteq 0^*1^*$.
3. (1) לא בהכרח נכון אבל לכל $i \geq 1$ מתקיים $0^{ir}1^{ir} \in L(A)$.
4. (1) לא בהכרח נכון אבל קיים $k \geq 1$ שעבורו לכל $i \geq 1$, $0^{r+ik}1^{r+k} \in L(A)$.

פתרון (1) לא נכון כי אוטומט עם שני מצבים לשפה שמכילה את כל המילים עם מספר זוגי של אפסים. אוטומט כזה יקבל את 0011 אבל לא את 00111.

(2) לא נכון כי עבור האוטומט הנ"ל, $010 \in L(A)$ (מספר זוגי של אפסים) אבל $010 \notin 0^*1^*$.

(3) לא נכון כי עבור האוטומט באיור, שעבורו $r = 3$, מתקיים $0^31^3 \in L(A)$ אבל 0^61^6. זה משום 0^31^3 יגיע עד ל-q_2 ויחזור ל-q_1, ואילו 0^61^6 יגיע עד ל-q_2 וילך הלוך ושוב ויסיים ב-q_2 ולא יקבל.

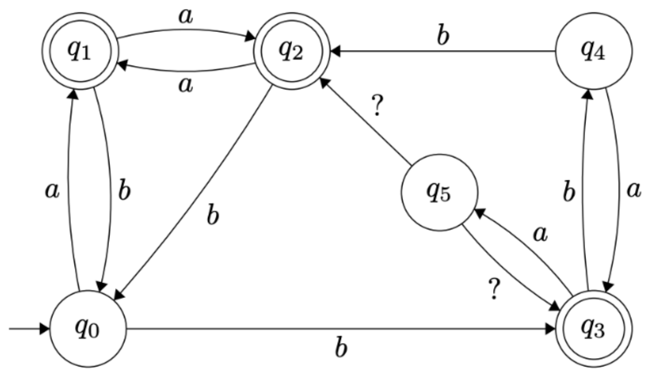


איור 28: אוטומט שמפריך את (3)

(4) כן נכון, נוכיח עם למת הניפוח. בריצות על המילים 0^r ו-1^r, יש מצב שחוזר על עצמו (לפחות אחד) ולכן בריצה על 0^r יש מעגל באורך k_1 ובריצה על 1^n יש מעגל באורך k_2.

את המעגלים האלה נוכל לשכפל עוד ועוד ולהגיע לאותו המצב. נביט בריצה של A הדומה לזו על 0^r1^r אבל רצה על המעגל של 0^r ik_2 פעמים ועל המעגל של 1^r ik_1 פעמים. נסמן $k = k_1k_2$ ואז הטענה מתקבלת (הוספנו ל-0^r ik אפסים וגם ל-1^r ik אחדות ונשארנו בשפה).

תרגיל נתון ה-DFA כבאיור, A,



איור 29: האוטומט A לתרגיל

נתון כי ל-$L(A)$ יש 4 מח"ש MN. מה אמור להיות במקום סימני השאלה באיור?

1. $\delta(q_5, a) = q_2, \delta(q_5, b) = q_3$.
2. $\delta(q_5, a) = q_5, \delta(q_5, b) = q_2$.
3. (1) ו-(2) נכונות.
4. כל התשובות לא נכונות.

פתרון נשים לב שמכך של-A 4 מח"ש MN, האלג' המצמצם אמור לאחד מצבים עד שנגיע ל-4.

- הצעד הראשון באלג' יגיע למח"ש (לפי F) $\{q_0, q_4, q_5\}, \{q_1, q_2, q_3\}$.
- השלב השני יפריד עם זנב a לפחות ל-$\{q_3\}, \{q_1, q_2\}$ ו-$\{q_0, q_4, q_5\}$ עבור תשובות $(2), (1)$.
- בשלב השלישי, ab לא יפריד לנו שום דבר. עבור זנב aa, נקבל $\{q_4\}, \{q_0, q_5\}, \{q_3\}, \{q_1, q_2\}$ כי q_4 מגיע למצב לא מקבל ו-q_0, q_5 למקבל (בשתי התשובות).

כאן נעצור כי הגענו ל-4 מחלקות שקילות ובגלל שתשובות $(2), (1)$ מקיימות את המח"ש האלה, אלה התשובות הנכונות ולכן (3) היא התשובה הנכונה.

הערה נשים לב שאם היינו בוחרים זנבות אחרים, היינו יכולים להגיע למחלקות שקילות אחרות אבל עדיין מספר מחלקות שקילות שווה.

שבוע $\mathbb{V}$ | שפות חסרות הקשר

הרצאה

חלק א' של ההרצאה

הערה בהרצאה הקודמת ראינו איך למזער אוטומט דטרמיניסטי. כיצד נוכל למזער NFA? אם אנחנו יודעים להכריע האם קיים NFA שקול עם k מצבים, נוכל לעבור על כל $k \in \mathbb{N}$ עד שנענה כן וזה יהיה NFA מינימלי.

בעיית הריקנות

- בעיית הריקנות שואלת, בהינתן אוטומט A, האם אם $L\left(A\right)=\varnothing$?

אפשר להכריע ע"י חיפוש בגרף (DFS/BFS) החל מ-Q_0, ואם מגיעים לקודקוד כלשהו והוא מקבל נחזיר "שקר" ואחרת אם כל הקודקודים הישיגים לא מקבלים, נחזיר "אמת".

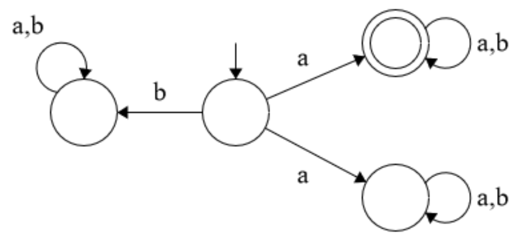
- הבעיה הדואלית לבעיית הריקנות, בעיית האוניברסליות, שואלת, בהינתן אוטומט A, האם $L\left(A\right)=\Sigma^*$?

מתקיים $L\left(A\right)=\Sigma^*$ אם"ם $\overline{L\left(A\right)}=\varnothing$ אם"ם $L\left(\overline{A}\right)=\varnothing$ (כאשר $\overline{A}$ הוא המשלים של A, נגדיר אותו עוד רגע). לכן מספיק שנייצר את $\overline{A}$ ונבדוק האם $L\left(\overline{A}\right)=\varnothing$.

בניית המשלים של A

- עבור A DFA : $\overline{A}$ הוא אותו אוטומט עם מצבים מקבלים הכל חוץ מהמצבים המקבלים של A ($F'=Q\backslash F$).

- עבור A NFA : החלפת המצבים המקבלים לא מספיקה, לדוגמה באיור הבא, נקבל גם במקורי וגם בבנייה החדשה שמילים שמתחילות ב-a מתקבלות. הבעיה היא שכאן הבנייה מקבלת את כל המילים שקיימת להן ריצה לא מקבלת, ולא כזו שכל ריצה שלהן היא לא מקבלת.



איור 30 : אוטומט שסותר את הבניה המקורית למשלים

מה שכן יעבוד, הוא לעשות דטרמיניזציה ל-DFA שקול A', דואליזציה למשלים $\overline{A'}$ ובדיקת ריקנות ל-$\overline{A'}$.

הסיבוכיות של אלג' זה היא אקספוננציאלית כי A' במקרה הגרוע הוא בעל מספר מצבים אקספוננציאלי ב-n גודל ה-NFA.

משפט אין פולינום p כך שבהינתן (כל) A NFA, ניתן לייצר $\overline{A}$ עם $\left|\overline{A}\right|\leq p\left(|A|\right)$.

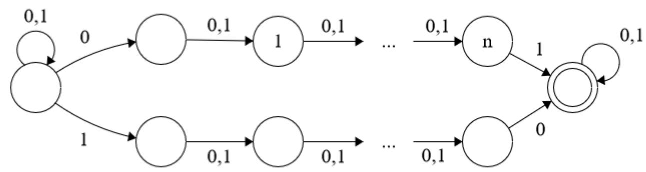
מסקנה האלג' שהראנו למעלה הוא הכי טוב שאפשר ואין אחד עם סיבוכיות קטנה יותר, כי זה בכל מקרה אקספוננציאלי.

הוכחה: נראה משפחה של שפות $\{L_n\}_{n=1}^{\infty}$ כך שלכל n קיים A_n NFA עבור L_n עם $\mathcal{O}\left(n^2\right)$ מצבים ולכל $\overline{A}_n$ NFA עבור $\overline{L_n}$ דורש לפחות 2^n מצבים.

נבחר $\overline{L_n}=\left\{ww:w\in\{0+1\}^n\right\}$. כך שלדוגמה $\overline{L_2}=\{0000,0101,1010,1111\}$ (ו-L_2 כל השאר המילים).

נראה שקיים NFA עם $\mathcal{O}\left(n^2\right)$ מצבים ל-$L_n=\overline{\left(\overline{L_n}\right)}$.

נשים לב כי $w \in L_n$ אם $|w| \neq 2n$ או שקיים אינדקס $i \in [n]$ כך ש-$w_i \neq w_{n+i}$. לכן האוטומט הבא יזהה נכון את $\overline{L_n}$, כי הוא יכול לנחש כל אינדקס לא נכון (נניח שניחש שזה 0 בהתחלה ו-1 בסוף אז אחרי n צעדים במסלול העליון הוא יקבל).



איור 31 : אוטומט שמזהה את L_n

זהו אוטומט עם $\mathcal{O}(n)$ מצבים.

נראה שכל NFA ל-$\overline{L_n}$ צריך לפחות 2^n מצבים. נניח בשלילה שקיים NFA $\overline{A_n}$ המזהה את $\overline{L_n}$ עם פחות מ-2^n מצבים.

לכל מילה $u \in (0+1)^n$, נתבונן בקבוצת המצבים

$$good(u) = \left\{s : \text{יש ריצה מקבלת של } \overline{A_n} \text{ על } uu \text{ שמבקרת ב-} s \text{ אחרי קריאת } u\right\} \subseteq Q$$

כלומר אוסף המצבים שבהם בדיוק באמצע ריצה מקבלת על uu הגענו אליהם.

מהיות מספר המצבים של $\overline{A_n}$ פחות מ-2^n מצבים, ולכן מעקרון שובך היונים קיימים $u_1 \neq u_2 \in (0+1)^n$ כך ש-$good(u_1) \cap good(u_2) \neq \varnothing$ ולכן אם s בחיתוך הזה, מתקיים

$$s \in \delta^*(Q_0, u_1), \quad \delta^*(s, u_2) \cap F \neq \varnothing \quad \Rightarrow \quad \delta^*(Q_0, u_1u_2) \cap F \neq \varnothing$$

כלומר $\overline{A_n}$ קיבל את u_1u_2 בסתירה לכך שברור ש-$u_1u_2 \in \overline{L_n}$ (L_n היא השפה עם כל המילים שאינן חזרה על מילה). ■

שפות חסר הקשר

שפות חסרות הקשר מוגדרות ע"י דקדוק חסר הקשר.

דוגמה נביט בדקדוק הבא,

$$A \to 0A1$$

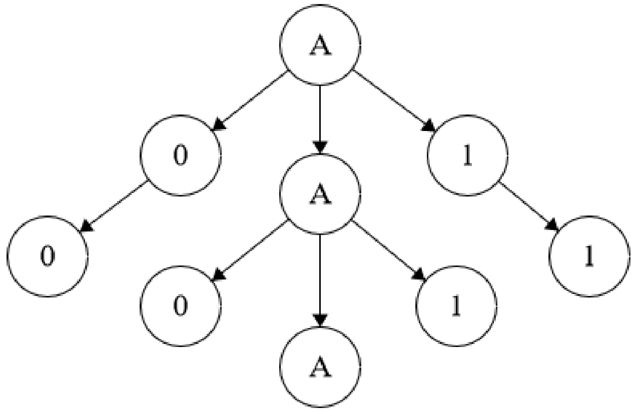
$$A \to B$$

$$B \to \#$$

נשים לב שיש לנו משתנים A, B, טרמינלים (א"ב) $0, 1, \#$, חוקים (המשוואות) ומשתנה התחלתי.

במקרה כזה שרשרת פעולות הגזירה הבאה מייצרת לנו מילה, $A \to 0A1 \to 00A11 \to 00B11 \to 00\#11$, כאשר נשים לב שהשפה שהדקדוק מגדיר אינה רגולרית, ובפרט היא $L(G) = \{0^n\#1^n\}$.

נוכל בנוסף לצייר את עץ הגזירה של הריצה הנ"ל, כאשר העלים של העץ משמאל לימין מייצרים לנו את המילה הסופית שקיבלנו בשרשרת הגזירה



איור 32 : עץ הגזירה של שרשרת הגזירות הנ"ל

הערה דקדוק חסר הקשר התחיל מעיבוד שפות טבעיות, שם נוכל לאפיין תארים ושמות עצם על ידי גזירה, לדוגמה $N \rightarrow AN$ מאפשר הוספת שם תואר לשם עצם באנגלית.

הגדרה דקדוק חסר הקשר הוא $G = \langle V, \Sigma, R, S\rangle$ כאשר :

- V קבוצה סופית של משתנים.
- Σ קבוצה סופית של אותיות.
- R קבוצה של חוקי גזירה מהצורה $V \rightarrow (V \cup \Sigma)^*$.
- $S \in V$ משתנה התחלתי.

הערה הדקדוק נקרא חסר הקשר כי יש בצד שמאל רק משתנה והוא יחיד.

הגדרה אם $w, u, v \in (V, \cup\Sigma)^*$ ו-$A \rightarrow w$ הוא חוק בדקדוק, אז <u>יצירה/גזירה</u> היא המעבר $vAu \Rightarrow vwu$.

אם $u, w \in (V \cup \Sigma)^*$ אז $u \Rightarrow^* w$ אם קיים $k \geq 1$ ו-$u_1, \ldots, u_k$ כך ש-$(V \cup \Sigma)^*$ כך ש-$u = u_1 \Rightarrow \ldots \Rightarrow u_k = w$ (ניתן לגזור מ-u ולהגיע ל-w).

הגדרה עבור G דקדוק ח"ה, נגדיר את <u>השפה</u> שלו להיות $L(G) = \{w : w \in \Sigma^* \land S \Rightarrow^* w\}$. שפה L היא שפה ח"ה (ונסמן $L \in \mathrm{CFL}$) אם יש CFG G כך ש-$L(G) = L$.

דוגמאות

1. $G = \langle \{S, A\}, \{0, 1\}, R, S\rangle$ כאשר החוקים הם

$$S \rightarrow A1A$$

$$A \rightarrow \epsilon|0A|1A$$

כל תהליך גזירה יתחיל ב-$S\to A1A$. לכן $\epsilon\notin L(G)$ אבל $1\in L(G)$. קל לראות ש-$L(G)=(0+1)^{*}1(0+1)^{*}$.

.2

$$S\to 0S1|SS|\epsilon$$

מגדיר את שפת הסוגריים המקוננים חוקית כאשר 0 הוא) ו-1 הוא (. נצטרך שבכל רישא לא יהיו יותר 1-ים מ-0-ים, ובסוף יהיו לנו מספר שווה של 0-ים ו-1-ים.

נשים לב כי $L(G)\cap\{0^*1^*\}=\{0^n1^n:n\geq 0\}$ ולכן $L(G)$ לא רגולרית.

משפט $\text{REG}\subseteq\text{CFL}$.

הוכחה: בהינתן DFA $A=\langle Q,\Sigma,q_0,\delta,F\rangle$, נבנה $G=\langle V,\Sigma,R,S\rangle$ כך ש-$L(G)=L(A)$. נבחר

- $V=\{V_q:q\in Q\}$.
- $S=V_{q_0}$.
- לכל מצב $q\in Q$ ו-$\sigma\in\Sigma$, נסמן $s=\delta(q,\sigma)$, נוסיף חוק $V_q\to\sigma V_s$. אם $q\in F$, נוסיף (מעבר לנ"ל) $V_q\to\epsilon$.

הרעיון כאן הוא שגזירה של מילה מ-V_q תסתיים בדיוק על כל המילים שמתקבלות מ-q.

נראה שלכל מצב $q\in Q$ ומילה w, $\delta^*(q,w)\in F \iff V_q\Rightarrow^* w$. נסמן $w=\sigma_1,\ldots,\sigma_k$ ולכן $\delta^*(q,w)\in F$ אם"ם יש ריצה $r_0,\ldots,r_k$ של A על w כך ש-$r_0=q$ ולכל $0\leq i\leq k$, $r_{i+1}=\delta(r_i,\sigma_{i+1})$ אם"ם

$$V_{r_0}\Rightarrow\sigma_1V_{r_1}\Rightarrow\ldots\Rightarrow\sigma_1\ldots\sigma_kV_{\sigma_k}\Rightarrow\sigma_1\ldots\sigma_k\epsilon=w$$

■

חלק ב' של ההרצאה

דוגמה הדקדוק $S\to aSa|bSb|\epsilon$ מייצר פולינדרומים באורך זוגי (באינדוקציה הוא מוסיף בכל צד אות). אם נרצה כל אורך, נוסיף $a|b$ לחוק היחיד שלנו.

משפט (למת הניפוח ל-CFL) תהי $L\in\text{CFL}$ אזי קיים $p\geq 0$ קבוע הניפוח כך שלכל מילה $w\in L$ עם $|w|\geq p$, ניתן לכתוב $w=uvxyz$ כאשר מתקיים

1. $|vxy|\leq p$.
2. $|vy|>0$.
3. לכל $i\in\mathbb{N}_0$, מתקיים $uv^ixy^iz\in L$.

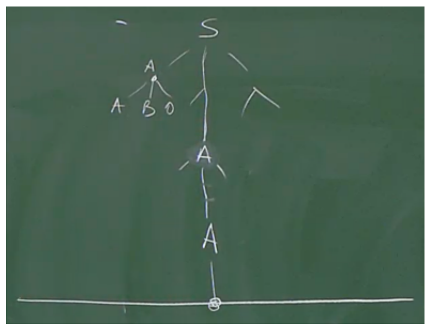
דוגמה שפת הפלינדרומים מקיימת את למת הניפוח. נבחר $p=3$, ואז אם $w\in L$ ו-$w\geq 3$:

- אם $|w|$ אי זוגי, נבחר x להיות האות האמצעית, v,y שכנותיה ו-u,z הרישא והסיפא בהתאמה.
- אם $|w|$ זוגי נבחר x להיות ϵ וכל השאר כנ"ל (v,y שמאל לאמצע וימין לאמצע בהתאמה).

רק כך המילה המנופחת תהיה מספיק גדולה גם ב-$i=0$, בחלוקות אחרות לא היו לנו מספיק אותיות בניפוח $i=0$.

הוכחה: בלמת הניפוח ל-REG מצאנו מעגל במצבים (כאשר $|Q|>p$) וחזרנו עליו i פעמים. יהי $b\geq 2$ האורך של צד ימין ארוך ביותר בדקדוק של L (כלומר ב-$(2)\rightarrow(1)$ מדובר במספר המשתנים/טרמינלים ב-(2)).

עתה נבחר p שיבטיח שבעץ הגזירה של מילים באורך גדול מ-p, יש מסלול עם משתנה שחוזר לפחות פעמיים (כבאיור, A יכול לחזור אין ספור פעמים, לא תמיד מיד אחרי עצמו).



איור 33: עץ הגזירה עם חזרה של משתנה

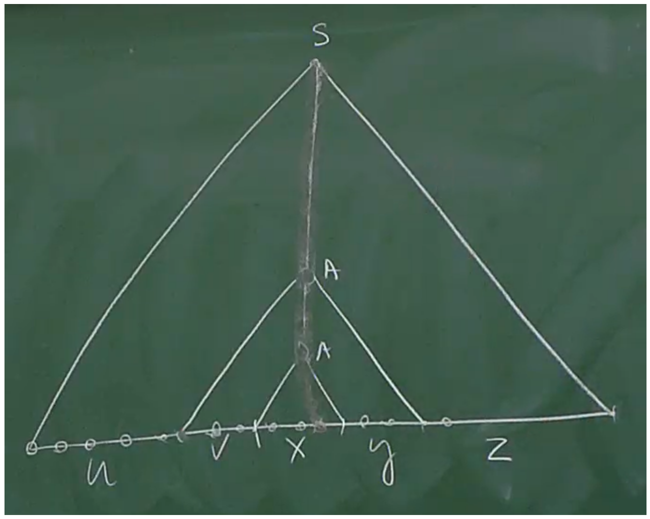
מתקיים שדרגת הפיצול של העץ (מספר הבנים של קודקוד כלשהו) $\leq b$ כי כל פיצול מתאים לחוק. נטען שהמילה מספיק ארוכה כדי שמשתנה יחזור פעמיים ועליו נוכל לחזור שוב ושוב.

נזכור כי אם מספר העלים $\leq b^{|V|+1}$ אז הגובה $\leq |V|+1$ (ממבני נתונים).

נבחר $p=b^{|V|+1}$ ותהי $w\in L$ עם $|w|\geq b^{|V|+1}$. נתבונן בעץ הגזירה הקטן ביותר של w (יש כמה דרכים אולי לגזור ולהגיע ל-w). בהכרח מתקיים שגובה העץ $\leq |V|+1$ מההבחנה הנ"ל.

יש $|V|$ משתנים ויש עלה עם עומק $\leq |V|+1$ (מהגדרת הגובה) שמכיל רק משתנים (כי אם היה טרמינל היינו עוצרים ולא ממשיכים הלאה).

לכן יש משתנה (שמופיע כ-A באיור הבא) שחוזר על עצמו באחת מ-$|V|+1$ הרמות הקרובות לעלים מעקרון שובך היונים.



איור 34 : חלוקה של המילה על פני עץ הגזירה, משולש מגדיר תת-עץ גזירה

נבחר חלוקה כבאיור הנ"ל (מספיק פורמלי). נראה שמתקיימים התנאים.

1. $|vxy| \leq b^{|V|+1}$ כי בחרנו את החזרה הכי נמוכה של A בעץ, שהיא בגובה (ביחס לעלים) לכל היותר $|V|+1$ ומהיות דרגת הפיצול לכל היותר b הרי שהמילה שנוצרת מהעלים היא באורך לכל היותר $b^{|V|+1}$.
2. $|vy| > 0$ כי בחרנו את עץ הגזירה המינימלי ואם גם v וגם y היו ריקים, זה לא עץ גזירה מינימלי (הייתה לנו תת-גזירה $A \Rightarrow^* A$ כשיכלנו לדלג עליה, הביטו באיור לאינטואיציה).
3. $ux^iyv^iz \in L$ לכל $i \in \mathbb{N}_0$ כי אנחנו יודעים שניתן לגזור $S \Rightarrow^* uAz$ וגם $A \Rightarrow^* vAy$ ו-$A \Rightarrow^* x$ ולכן נוכל גם לבצע $A \Rightarrow^* v^iAy^i$ ולכן גם $S \Rightarrow^* uv^ixy^iz$.

■

תרגול

דוגמאות

1. נביט בדקדוק הבא

$$A \to 0A1|B$$

$$B \to \#$$

במקרה כזה נוכל לגזור

$$A \to 0A1 \to 00A11 \to 00B11 \to 00\#11$$

וכמו שראינו בהרצאה, השפה היא כל המילים מהצורה $0^n\#1^n$.

2. נמצא דקדוק לשפה $L=\left\{a^nb^{2n}:n\geq 0\right\}$.מספיק החוק $S\to aSbb|\epsilon$, כאשר כדי להגיע ל-$aabbbb$ נגזור

$$S\to aSbb\to aaSbbbb\to aabbbb$$

3. $L=\left\{a^ib^j:j\geq i\right\}$. כאן נגדיר $S\to aSb|Sb|\epsilon$ ואז נוכל להוסיף כמה b-ים שנרצה מעבר ל-a-ים.

4. $L=\left\{a^ib^jc^jd^i:i,j\in\mathbb{N}_0\right\}$. כאן נגדיר

$$S\to aSd|T|\epsilon$$

$$T\to bTc|\epsilon$$

וזה יספיק כדיר להגדיר לנו (המשתנה הנוסף כאן אינו הכרחי למעשה).

טענה CFL סגורה לאיחוד.

הוכחה: תהיינה $L_1,L_2\in\mathrm{CFL}$ ו-G_1,G_2 CFG-ים המתאימים להן. נוכיח כי $L_1\cup L_2\in\mathrm{CFL}$. נניח בה"כ כי $V_1\cap V_2=\varnothing$ (שינוי שמות).

נגדיר

$$G=\left\langle V_1\cup V_2\cup\left\{S\right\},\Sigma,R_1\cup R_2\left\{S\to S_1|S_2\right\},S\right\rangle$$

כאשר $S\notin V_1\cup V_2$. קל לראות מכאן שמילה מתקבלת ע"י $S\to S_1\to\ldots$ כאשר היא יכולה להמשיך מ-S_1 בגזירה המקורית שלה (ומ-S_2 בדומה). ■

טענה CFL סגורה לשרשור.

הוכחה: תהיינה $L_1,L_2\in\mathrm{CFL}$ ו-G_1,G_2 CFG-ים המתאימים להן. נוכיח כי $L_1\cdot L_2\in\mathrm{CFL}$. נניח בה"כ כי $V_1\cap V_2=\varnothing$ (שינוי שמות).

נגדיר

$$G=\left\langle V_1\cup V_2\cup\left\{S\right\},\Sigma,R_1\cup R_2\left\{S\to S_1\cdot S_2\right\},S\right\rangle$$

כאשר $S\notin V_1\cup V_2$. קל לראות שכל השרשורים מתקבלים כאן, וכל מה שאינו שרשור לא מתקבל. ■

משפט (למת הניפוח ל-CFL) תהי $L \in \text{CFL}$ אזי קיים $p \geq 0$ קבוע הניפוח כך שלכל מילה $w \in L$ עם $|w| \geq p$, ניתן לכתוב $w = uvxyz$ כאשר מתקיים

1. $|vxy| \leq p$.
2. $|vy| > 0$.
3. לכל $i \in \mathbb{N}_0$, מתקיים $uv^ixy^iz \in L$.

הערה למה זו דומה מאוד ללמת הניפוח המקורית רק שעכשיו יש לנו שני סגמנטים שונים לנפח (ורק אחד מהם יכול להיות ריק), והחלק שהוא לכל היותר p לא חייב להיות רישא של המילה.

דוגמה $L = \{a^nb^na^n : n \in \mathbb{N}\}$. נראה ש-$L \notin \text{CFL}$. נניח בשלילה ש-$L \in \text{CFL}$. יהי $p \geq 0$ קבוע ניפוח ונבחר $w = a^pb^pa^p$ ותהי $w = uvxyz$ חלוקה של w שמקיימת את התנאים.

- $vxy \subseteq a^p$ אז עבור $i = 0$, v^ixy^i מכיל פחות a-ים מ-vxy כי $|vy| > 0$ ולכן $uv^ixy^iz \notin L$ סתירה.
- $vxy \subseteq b^p$ אז אותו הדבר כנ"ל עובד רק עם b-ים.
- $vxy \subseteq a^p$ אז כנ"ל.
- $vxy \subseteq a^pb^p$ כאשר אנחנו מכילים לפחות a אחד או לפחות b אחד, אז בהכרח שבניפוח עם $i = 0$ נקטין את מספר ה-a-ים או ה-b-ים וכך נצא מהשפה סתירה.
- $vxy \subseteq b^pa^p$ כאשר אנחנו מכילים לפחות b אחד או לפחות a אחד, אותו טיעון כנ"ל עובד.

דוגמה ננסה להבין האם CFL סגורה לחיתוך. $L_1 = \{a^nb^na^m : n, m \geq 0\}$ היא כן ב-CFL עם הדקדוק

$$S \to XA$$
$$X \to aXb|\epsilon$$
$$A \to Aa|\epsilon$$

וגם $L_2 = \{a^nb^ma^m : n, m \geq 0\}$ היא גם ב-CFL עם הדקדוק

$$S \to Ax$$
$$X \to bXa|\epsilon$$
$$A \to Aa|\epsilon$$

אבל $L = L_1 \cap L_2$ כאשר L היא מהדוגמה הנ"ל וראינו שהיא לא ב-CFL לכן CFL לא סגורה לחיתוך.

הערה CFL בנוסף אינה סגורה להשלמה כי אחרת מדה-מורגן $L_1 \cap L_2 = \overline{\overline{L_1} \cup \overline{L_2}}$ ואז CFL הייתה סגורה לחיתוך והיא לא.

דוגמה $L=\left\{ ww:w\in\left\{ a,b\right\} ^{*}\right\}$. האם L ב-CFL? לא! נשתמש בלמת הניפוח ל-CFL.

תהי $p>0$, נבחר את המילה $w=a^{p}b^{p}a^{p}b^{p}\in L$, ותהי חלוקה $w=uvxyz$ שמקיימת את התנאים.

- אם $vxy\subseteq a^{p}$ או $vxy\subseteq b^{p}$ במופעם הראשון או a^{p} או b^{p} במופעם השני, אז מהיות $|vy|>0$, ניפוח ב-$i=0$ נקבל שב-$uv^{i}xy^{i}z$ יש פחות a-ים (או b-ים) מאשר בצד השני ולכן יצאנו מהשפה סתירה.
- אם $vxy\subseteq a^{p}b^{p}$ במופעו הראשון או השני כאשר vxy מכיל לפחות a אם v לא ריק ולפחות b אחד אם y לא ריק. אז כשננפח עם $i=0$ נקבל פחות a-ים או b-ים מאשר בצד השני סתירה.
- אם $vxy\subseteq b^{p}a^{p}$ אז או ש-v לא ריק ואז הוא מכיל b או ש-y לא ריק והוא מכיל a ואז ננפח עם $i=0$ ונקבל שאחד הצדדים קטן מהאחר קטן מהאחר ונצא מהשפה סתירה.

נביט ב-$\overline{L}$, זו השפה $\underbrace{\left\{ uv:|u|=|v|,u\neq v\right\} }_{L_{1}}\cup\underbrace{\left\{ w:|w|\equiv1\mod2\right\} }_{L_{2}}$ (כל המילים האי זוגיות או זוגיות עם חצאים שונים). נוכיח כי $\overline{L}\in\text{CFL}$. L_{2} רגולרית (אוטומט שבודק זוגיות של אורך המילה) ולכן ב-CFL. נותר להוכיח כי $L_{1}\in\text{CFL}$ (למרות שהראנו כבר בהרצאה שהיא רגולרית) ונסיים מסגירות לאיחוד.

תהי $w\in L_{1}$, לכן $|w|=2n$ עבור $n\geq0$ וקיים אינדקס $i\in[n]$ כך ש-$w_{i}=a$ ו-$w_{n+i}=b$ (בה"כ).

לכן ניתן לכתוב $w=xaybz$ כאשר $|x|=i-1,|y|=n-1,|z|=n-i$. נגדיר את L_{1} מחדש בתור

$$\left\{ xaybz,xbyaz:x,y,z\in\left\{ a,b\right\} ^{*},|y|=|x|+|z|\right\}$$

נמצא דקדוק ל-L_{1}.

$$S\rightarrow AB|BA$$

$$A\rightarrow aAa|aAb|bAa|bAb|a$$

$$B\rightarrow aBa|aBb|bBa|bBb|b$$

מזהה את L_{1} כאשר הרעיון כאן הוא שהגזירה מ-S מחלקת אותנו להאם יש לנו a קודם ואז b או b קודם ואז a, וכדי לשמור על דרישת האורך, בכל פעם שנוסיף טרמינל ל-x או z נוסיף גם אות ל-y כדי לשמור על שוויון בין האגפים.

שבוע $\mathbb{VII}$ | מכונות טיורינג

הרצאה

חלק א' של ההרצאה

דוגמה עבור $L=\left\{ w\#w:w\in(0+1)^{*}\right\}$, קל מאוד לכתוב תכנית שמכריעה את השפה (האם קלט הוא בשפה או לא), אבל CFL ו-REG לא עזרו לנו למדל את הפתרון. מכונות טיורינג כן יכולות למדל אלג' כאלה.

אינטואיטיבית, מכונת טיורינג (מ"ט) היא סרט אינסופי שאליו אפשר לכתוב ולקרוא ובהתחלה כתובות עליו אותיות מילת הקלט (וכל השאר רווחים). הראש (הקורא/כותב) יכול לנוע שמאלה וימינה, כל עוד לא הגענו למצב סיום (קבלה/דחייה).

דוגמה נתאר מ"ט לא פורמלית עבור L הנ"ל.

1. סרוק את הקלט ונוודא שיש לפחות # אחת, אם אין, דחה. אם יש #, חזור לתא הראשון.
2. זגזג בין מיקומים מתאימים משאל ומימין ל-# וודא שמסומנים באותה האות. אם לא, דחה. אם הסתיימה הבדיקה ואין אותיות נוספות מימין ל-#, קבל.

הגדרה מכונת טיורינג היא שביעייה $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} \rangle$ כאשר:

- Q היא קבוצה סופית של מצבים.
- Σ היא א"ב הקלט ($\_ \notin \Sigma$).
- Γ היא א"ב העבודה, $\Sigma \subseteq \Gamma$ ו-$\_ \in \Gamma$ (אותיות שאפשר לכתוב על הסרט).
- $q_0 \in Q$ מצב התחלתי.
- $q_{acc} \in Q$ מצב מקבל.
- $q_{rej} \in Q$ מצב דוחה.
- δ היא פ' המעברים המוגדרת לפי $Q \times \Gamma \mapsto Q \times \Gamma \times \{L, R\}$ כאשר אם לדוגמה $\delta(q, a) = (q', b, R)$ אז כאשר נהיה במצב q ונקרא את האות a, נעבור למצב q', נכתוב b בתא הנוכחי ונזוז ימינה.

  הגרסה האי-דטרמיניסטית שבה נשתמש היא עם הגדרה זהה לנ"ל רק שעתה הפ' δ מעתיקה $Q \times \Gamma$ ל-$2^{Q \times \Gamma \times \{L,R\}}$.

הערה DFA הוא מ"ט כאשר $\delta(q, a) = \langle \delta'(q, a), a, R \rangle$ עבור δ' פ' המעברים של ה-DFA. בנוסף צריך לבצע התאמות למצבים המקבלים וכו'.

הגדרה פעילות מ"ט כלשהי מוגדרת באופן הבא:

1. מילת הקלט כתובה על סרט העבודה, מרופדת ב-_-ים. אם $w = \sigma_1 \ldots, \sigma_n$, הקונפיגורציה ההתחלתית תראה כבסרט הבא

σ_1	σ_2	$\ldots$	σ_n	_	_	$\ldots$

2. המכונה מתקדמת לפי פונקציית המעברים.
   - קונפ' שניתן לעבור ביניהן באמצעות פ' המעברים נקראות קופנ' מעברים.
   - ריצה היא סדרה של קונפיגורציות עוקבות, החל מהקונפ' ההתחלתית.

- שלושה גורלות לריצה:
  1. מגיעה למצב מקבל $\leftarrow$ עוצרת ומקבל.
  2. מגיעה למצב דוחה $\leftarrow$ עוצרת ודוחה.
  3. לא עוצרת ודוחה את מילת הקלט.

הגדרה קופנ' של מ"ט מגדירה ע"י המצב הנוכחי, תוכן הסרט ומיקום הראש. קופנ' מתוארת ע"י מילה ב-$\Gamma^* \cdot Q \cdot \Gamma^*$. כאשר הקונפ' uqv אומרת לנו שאנחנו במצב q, שהראש מצביע לאות הראשון של v ושתוכן הסרט הוא uv ולאחר מכן _ (הרעיון הוא ש-q הוא על הסרט, בין u ל-v).

הקונפ' ההתחלתית היא $q_0 w$ כאשר w מילת הקלט.

הגדרה יהיו $a, b, c \in \Gamma$, $u, v \in \Gamma^*$ ו-$q \in Q$. אזי הקונפ' העוקבת של $uaqbv$ היא (ראו הדגמה, הקו כאן והדגמות הבאות הוא תקלה טכנית בלתי פתירה):

		q	
u	a	b	v

- $uq'acv$ אם $\delta\left(q,b\right)=\left(q',c,L\right)$.

	q'		
u	a	c	v

- $uacq'v$ אם $\delta\left(q,b\right)=\left(q',c,R\right)$.

			q'
u	a	c	v

- אם $u=\epsilon$ (אנחנו בקצה השמאלי) ו-$\delta\left(q,b\right)=\langle q',c,L\rangle$ אז הקונפ' העוקבת תהיה $q'cv$ (מונעים מעבר שמאלה).

הגדרה ריצה של M על מילה $w\in\Sigma^*$ היא סדרה $c_0, c_1, \ldots$ של קונפ' כך ש:

1. c_0 היא הקונפ' ההתחלתית של M על w.
2. c_{i+1} עוקבת ל-c_i לכל i.
3. הסדרה סופית ומסתיימת בקונפ' עוצרת (קונפ' מקבלת אם המצב שלה הוא q_{acc} ודוחה אם המצב שלה הוא q_{rej}), או שאינה סופית.

M מקבלת את w אם יש ריצה של M על w שמגיעה לקונפ' מקבלת. אחרת (כל הריצות מגיעות לקונפ' דוחה או לא עוצרות).

נגדיר את השפה של M להיות $L\left(M\right)=\left\{w: w \text{ על } M \text{ יש ריצה מקבלת של}\right\}$.

הגדרה נאמר כי מ"ט M מזהה שפה L אם $L\left(M\right)=L$. מחלקת השפות RE (recursively enumerable) היא כל השפות הניתנות לזיהוי ע"י מ"ט.

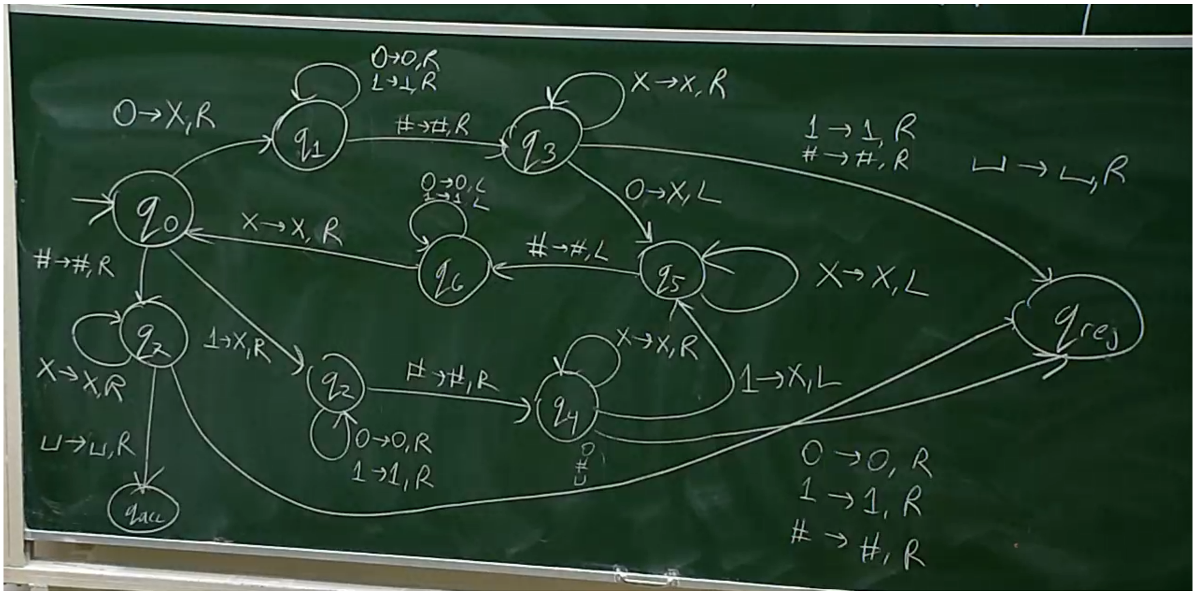
נאמר כי M מכריעה שפה L אם M מזהה את L ובנוסף M עוצרת על כל קלט. מחלקת השפות R (recursive) היא כל שהפות הניתנות להכרעה ע"י מ"ט.

הערה מההגדרה $\mathrm{R}\subseteq\mathrm{RE}$, אבל האם $\mathrm{R}\subsetneq\mathrm{RE}$? כן! נוכיח בהמשך ש-$\mathrm{R}\neq\mathrm{RE}$.

דוגמה נסתכל על $L=\left\{w\#w: w\in\left(0+1\right)^*\right\}$ ונבנה מכונה שמזהה אותה.

נבחר $\Sigma=\left\{0,1,\#\right\}$, $\Gamma=\left\{0,1,\#,\times,\_\right\}$ כאשר $\times$ מסמן שאישרנו כבר תווים.

נקבל את גרף המצב הבא ($a \to b, \Delta$ אומר שאם קראנו a, נכתוב b ונזוז $\Delta \in \{R, L\}$).



איור 35: מ"ט שמזהה את L

אינטואיציה:

1. אם התא הנוכחי מסומן ב-#, בדוק האם יש תאים לא מחוקים מימינו.

אם מ-q_0 מצאנו #, נלך ימינה על $\times$ ונחזור כל פעם ל-q_2 עד שנקרא לתו אחר. אם קראנו רווח הצלחנו (q_{acc}), אחרת יש יותר תווים מימין מאשר משמאל ונדחה (q_{acc}).

(א) אם התא הנוכחי מסומן ב-0, מחק אותו, לך ימנה עד ל-# ואז ימינה עד לתא הלא מחוק הראשון. אם מסומן ב-_, 1, #, דחה. אחרת, עבור ל-(4).

אם מ-q_0 מצאנו 0, מחק אותו ועבור ל-q_1. קרא דברים וחזור כל פעם ל-q_1 עד לסולמית. קרא $\times$-ים וחזור כל פעם ל-q_3 עד שנגיע למשהו שהוא לא $\times$. אם קראנו אחד מהתווים האסורים, דוחים,

(ב) אם התא הנוכחי מסומן ב-1, בצע את המקרה הדואלי ל-2.

המצבים שממשים את ההתנהגות הדואלים הם q_2, q_4.

(ג) לך שמאלה (על מחוקים) עד ל-# ואז לך שמאלה עד למחוק המיני ביותר, ועוד אחד, ואז חזור ל-1.

אנחנו ב-q_5, זזים שמאלה כל עוד מחוק, ואז ב-# עוברים ל-q_6 שעליו זזים כל עוד אנחנו ב-$0, 1$ ואז כשמגיעים למחוק זזים עוד פעם אחת ל-q_0.

חלק ב' של ההרצאה

נתונה M מ"ט ומחליפים בין q_{acc} ו-q_{rej}. האם מקבלים מכונה עם $\Sigma^* \backslash L(M)$? לא! אם M לא עצרה על מילה w אז $w \notin L(M)$ וגם $w \notin L(\overline{M})$.

אם M מכריעה את L אז ההחלפה כן הייתה משלימה את השפה.

מסקנה R סגורה למשלים.

הגדרה $L \in \text{co-RE}$ אם"ם $\overline{L} \in \text{RE}$. co-RE היא מחלקת כל השפות שקיימת מ"ט שמזהה את המשלים שלהן.

משפט $\text{R} = \text{RE} \cap \text{co-RE}$ כלומר ניתן להכריע שפה אם"ם ניתן לזהות אותה ואת המשלים שלה.

הוכחה: נוכיח הכלה דו-כיוונית.

<u>$\text{R} \subseteq \text{RE} \cap \text{co-RE}$</u>: מההגדרה מתקיים $\text{R} \subseteq \text{RE}$ (אם מכריעים גם מזהים). תהי $L \in \text{R}$. מהיות $L \in \text{R}$, הרי ש-$\overline{L} \in \text{R}$ (החלפת q_{acc}, q_{rej}), ולכן $\overline{L} \in \text{R} \subseteq \text{RE}$ כלומר $L \in \text{co-RE}$.

<u>$\text{RE} \cap \text{co-RE} \subseteq \text{R}$</u>: תהי $L \in \text{RE} \cap \text{co-RE}$. לכן קיימת מ"ט M שמזהה את L ו-$\overline{M}$ שמזהה את L. נבנה מכונה M' שמכריעה את L.

נבנה מכונה שמריצה את שתי המכונות בו זמנית, ואז בטוח אחת מהן תעצור מתישהו ולכן תמיד נעצור בעצמנו (ונחזיר תשובה בהתאמה לתוצאה שהתקבלה משתי המכונות). באופן מעט יותר פורמלי, עבור $i = 1, 2, \ldots$:

1. הרץ את M על w i צעדים. אם M קיבלה את w, עצור וקבל.
2. הרץ את $\overline{M}$ על w i צעדים. אם $\overline{M}$ קיבלה את w, עצור ודחה.

טענה M' עוצרת על כל קלט w.

הוכחה: זאת משם שאם $w \in L$ אז לריצה המקבלת r של M על w יש מספר $1 \leq j < \infty$ של צעדים ואז M' תעצור באיטרציה ה-j.

אחרת, לריצה $\overline{M}$ על w יש מספר $1 \leq k < \infty$ שעבורה M' תעצור ותדחה באיטרציה ה-k. ■

טענה $L(M') = L(M)$.

הוכחה: אם $w \in L(M')$ אז w התקבלה בעקבות ריצה מקבלת של M על w כלומר $w \in L(M)$. אם $w \in L(M)$ אז M' תעצור בגלל זה ותקבל. ■

■

הערה כיצד נריץ דברים במקביל? בכל איטרציה נשכפל את המילה על הסרט ונפריד אותה עם איזשהו סימן מפריד וערך של מונה שעולה בכל פעם. לא כל כך חשוב להבין איך זה עובד, ונראה בקרוב שאפשר להניח שיש לנו כמה סרטים שאנחנו רצים עליהם במקביל ושזה שקול.

תרגול

הערה בהגדרה של מכונת טיורינג אין לנו זיכרון, אבל הוא מגולם בתוך פ' המעברים והמצבים שמאפשרים לנו לכתוב דברים שנשמרים על הסרט.

הערה אינטואטיבית, קופנ' מוגדרת כמידע המינימלי שנצטרך כדי שאם נכבה את המחשב, נוכל לשחזר את המצב שהיינו בו לפני שכיבינו את המחשב.

הגדרה תהיינה מילה w ומ"ט M. נאמר כי $c_1, \ldots, c_k$ היא ריצה חלקית של M על w אם $c_1 = q_0 w$ ולכל $i \in [k-1]$, c_i גוררת את c_{i+1} לפי δ.

הגדרה תהיינה $f : \mathbb{N} \to \mathbb{N}$ ו-M מ"ט. נאמר כי מ"ט מחשבת את f אם בתחילת הריצה של M כתוב את w על הסרט ובסוף הריצה (המכונה אכן עוצרת) הסרט מכיל רק את $f(w)$.

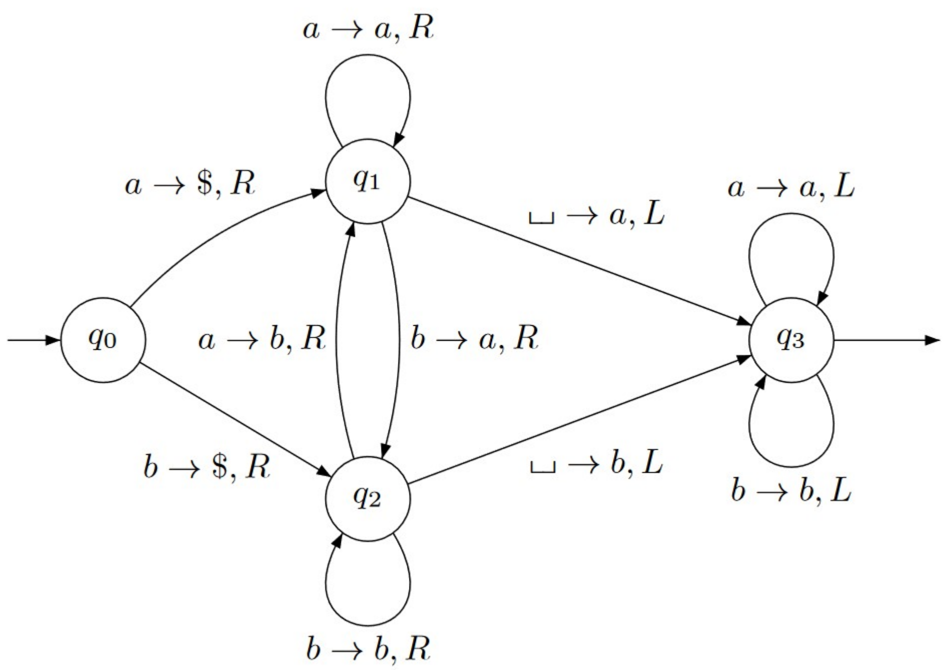
דוגמה נתאר מ"ט שמחשבת את הפ' $f(n) = n + 1$ בייצוג הבינארי. המכונה שלנו תתחיל בסימון התו הראשון בסרט ב-\$ ותזיז את הקלט תו אחד ימינה. מכאן, אינטואטיבית נחליף את רצף ה-1-ים הראשון מימין (LSB) ב-1 עם הרבה אפסים ($111\ldots$ הופך ל-$1000\ldots$).

משם, במצב q_0 ותסרוק את הסרט ימינה עד שתגיע ל-_ ואז תעבור ל-q_1. ב-q_1, אם M קוראת 1 היא משנה אותו ל-0 וממשיכה שמאלה. אם היא רואה 0, היא משנה אותו ל-1 ועוצרת.

אם M קוראת \$, הקלט היה $1\ldots1$ (כי היינו עוצרים אם ראינו 0) ובמקרה כזה היא תשנה את התו הראשון ל-1 ותזיז את כל הסרט אחד ימינה ותכתוב \$ בהתחלה (ככה יש לנו 1 והרבה אפסים).

התיאור הזה מספיק, חוץ מהעובדה שלא הסברנו איך להזיז את כל הסרט ימינה. באיור ניתן לראות מ"ט שהרעיון שלה הוא ש-q_1 הוא המצב שזוכר שהתו הקודם שקראנו הוא a ו-q_2 זוכר שעכשיו קראנו b.

כך, מ-q_1 לא משנה מה קוראים, נכתוב a ומ-q_2 נכתוב b. אם נקרא רווח נדע שסיימנו



ש

איור 36 : מ"ט שמזיזה ימינה את הסרט

מודלים שקולים למ"ט

- מ"ט שסרטה לא חסום משמאל.
- מ"ט עם k סרטים.
- מ"ט שיכולה להישאר במקום בנוסף לבחירה ימינה/שמאלה (Stay-TM).
- מ"ט שבמקום סרט יש לה גריד דו ממדי אינסופי.
- מ"ט אי-דטרמיניסטית.

הגדרה נאמר כי שתי מכונות חישוב M, N הן שקולות אם לכל $w \in \Sigma^*$:

- M מקבלת את w אם"ם N מקבלת את w.
- M דוחה את w אם"ם N דוחה את w.
- M לא עוצרת על w אם"ם N לא עוצרת על w.

הגדרה שני מודלים חישוביים $\mathcal{X}, \mathcal{Y}$ הם שקולים אם לכל מכונה מסוג $\mathcal{Y}$ יש מכונה שקולה מסוג $\mathcal{X}$ ולהפך.

הגדרה מ"ט עם שני סרטים היא מכונה רגילה, עם שני סרטים אינסופיים מימין, שני ראשים קוראים ופ' מעברים המוגדרת ע"י $\delta : Q \times \Gamma^2 \rightarrow Q \times \Gamma^2 \times \{L, R\}^2$.

הערה משמעות פ' המעברים כאן היא שאנחנו קוראים בכל פעם את התווים משני הראשים הקוראי, ויחד עם המצב החדש קובעים לאיזה צד הולכים בכל סרט בנפרד.

משפט מ"ט עם שני סרטים היא מודל חישובי שקול למ"ט קלאסי.

הוכחה: ברור שלמ"ט קלאסי יש מכונה עם שני סרטים שקולה (פשוט מנוונים את הסרט השני). נוכיח את הכיוון השני.

תהי מ"ט עם שני סרטים $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} \rangle$הרעיון הוא שנמיר את שני הסרטים לסרט אחד שבו א"ב הסרט (העבודה) הוא מתוך $\Gamma^2 \times \{0,1\}^2$ שייצג את האות בכל סרט והאם כל ראש קורא נמצא כרגע על התו ההוא.

נגדיר $M' = \langle Q', \Sigma', \Gamma', \delta', q_0', q_{acc}', q_{rej}' \rangle$ כאשר $\Gamma' = (\Gamma \times \Gamma \times \{0,1\} \times \{0,1\}) \cup \{\_\}$. M' פועלת כך:

1. מתחילה עם סרט שעליו כתובה $w = \sigma_1 \dots \sigma_n$ ומחליפה לפי הסדר את σ_i ב-$(\sigma_i, \_, 0, 0)$, לכל i, עד שמגיעה לסוף המילה ואז חוזרת לתחילת הסרט ומחליפה את התו הראשון ב-$(\sigma_1, \_, 1, 1)$.
2. M' תסרוק את הסרט שלה עד שתמצא את המיקום של הראש הקורא הראשון בריצה של M על w (תזהה $(*, *, 1, *)$).

משם תעבור למצב שמקודד את זה שנמצא הראש הראשון ונקראה אות כלשהי σ במקום הזה בסרט הראשון של M.

משם היא תחזור לראש הסרט ותתחיל לחפש באופן דומה את הראש השני ותזכור במצבים איזו אות נקרא.

משם, M' תביט בפ' המעברים של M ותתחיל לעדכן את הסרט שלה בהתאם - נסרוק שוב את הסרט כשנחפש את הראש הקורא הראשון, תעדכן את האות במיקום הזה וגם את סמני הקוראים המדומים, תחזור לתחילת הסרט, ותעשה את אותו הדבר עבור הראש הקורא השני.

■

טענה R סגורה לאיחוד.

הוכחה: נריץ את המכונה שמכריעה שפה אחת, אם היא תקבל נקבל ואם לא נריץ את המכונה השנייה (נאפס את הסרט וכו') ונקבל/נדחה בהתאם לה. המזל כאן הוא ששתי המכונות תמיד עוצרות ולכן זה עובד. ■

הערה גם RE סגורה לאיחוד, אבל שם צריך להריץ את שתי המכונות במקביל וזה קצת יותר מורכב.

שבוע $\mathbb{VIII}$ | אנמורציה ואי-כריעות

הרצאה

חלק א' של ההרצאה

הגדרה ספרן (Enumerator) E הוא מ"ט שלא מקבלת קלט ומדפיסה מילים (עם "אנטרים" ביניהן), ושפתה היא

$$L\left(E\right)=\left\{ w:w\text{ בסופו של דבר מדפיסה את } E\right\}$$

משפט $\forall L\subseteq\Sigma^{*}$, $L\in\mathrm{RE}$ יש ספרן E כך ש-$L\left(E\right)=L$.

הוכחה: $\Rightarrow$: נניח שיש ספרן E כך ש-$L\left(E\right)=L$. נייצר M שמזהה את L.

בהינתן מילה, M תריץ את E ובכל פעם שידפיס מילה y, M בודקת האם $w=y$. אם כן, עוצרת ומקבלת. אם לא, ממשיכה להריץ את E.

M אכן מזהה את L כי אם $w\in L$ אז E ידפיס את w בסוף של דבר ולכן נעצור ואז M תעצור ותקבל. אם $w\notin L$ אז E לא ידפיס את w ואז M תרוץ לנצח ולא תקבל את w (או שתעצור ותדחה אם E עוצר).

$\Leftarrow$: נתונה M מ"ט שמזהה את L ונייצר ספרן E כך ש-$L\left(E\right)=L$. נזכר ש-Σ^{*} בת מניה, ולכן יש סידור $w_{1},w_{2},\ldots$ של Σ^{*} (עבור $\Sigma=\left\{ 0,1\right\}$ הסידור $\epsilon,0,1,00,01,...$ עובד).

לא נוכל להריץ את M על המילים אחד אחרי השני כי M מזהה ולא מכריעה ולכן ייתכן שלא נעצור ולא נגיע למילים אחרות.

נריץ את כל המילים במקביל ע"י הרצה למשך i צעדים של $w_{1},\ldots,w_{i}$ לכל i באופן איטרטיבי. אם M מקבלת את w_{j} עבור $j\in\left[i\right]$ במהלך הריצה, נדפיס את w_{j}.

אם $w\in L$ אז w תודפס בסופו של דבר כי קיים i כך ש-$w=w_{i}$ ואז קיים t כך ש-M מקבלת את w תוך t צעדים. לכן w תדפיס בכל איטרציה $k\geq\max\left\{ i,t\right\}$.

אם $w\notin L$ אז E לא תדפיס את w מהגדרתה. ■

הבעיה העשירית של הילברט היא הבעיה הבאה: תאר אלג', שבהינתן פולינום במספר משתנים, יכריע האם יש לו שורש שלם.

ב-1970 הוכח שאין אלג' שיכריע את הבעיה במספר צעדים קבוע (כלומר לא ב-R). עם זאת, $H = \{\langle p\rangle :$ יש ל-p שורש שלם $\} \in \mathrm{RE}$ כי אפשר לסדר את $\mathbb{Z}^n$ כאשר n מספר המשתנים ולבדוק האם כל אחד מה-n-יות היא שורש של האלג'.

שלוש רמות לתיאור אלג'

1. ע"י מ"ט, כאשר ניווכח שכל עצם קלט A ניתן לקודד כמילה $\langle A\rangle$.

דוגמה $G = \langle V, E\rangle$ אפשר לקודד כרשימה של קודקודים (עם מפריד #) ואז רשימה של קשתות בין קודקודים (עם מפריד $).

2. תיאור פעולות של מ"ט (בסגנון "זוז עם הראש הקורס שמאלה").

3. שפה עילית (pseudo-code).

התזה של צ'רץ' וטיורינג קובעת שהכרעה ע"י מ"ט שקולה לאלג', כלומר כל תיאור ברמה 3 שקול לתיאור ברמה 1.

הערה לא נוכיח שהתזה נכונה, אבל נעשה כמה דוגמאות שישכנעו אותנו.

דוגמה מ"ט שמכריעה את $CG = \{\langle G\rangle :$ גרף לא מכוון קשיר $G\}$.

1. כיצד נתון גרף: נניח ש-G נתון ע"י רשימת קודקודים (מספרים בבסיס 2) מופרדים ב-# ורשימת קשתות מופרדות ב-$.

2. אלג': (BFS) נחזיק $C = \varnothing, T = \{v_0\}$ ואז:

   כל עוד $T \neq \varnothing$, נוציא v מ-T, נוסיף אותו ל-V, ולכל $u \in V \setminus (C \cup T)$, אם $E(u, v)$, נוסיף את u ל-T.

   אם $C = V$ נקבל אחרת נדחה.

3. תיאור האלג' ע"י מ"ט: נבחר $\Sigma = \{0, 1, \#, \$\}$, $\Gamma = \Sigma \cup \{\_\} \cup \{0, 1\} \times \{C, T, A\}$.

   המכונה יכולה לסמן קודקודים T-לסמן קודקודים ע"י הפיכת התו הראשון בקידוד שלהם לתו ב-0_T או 1_T (וכך גם C, A-תסמן).

   (א) T-סמן את הקודקוד הראשון.

   (ב) חזור כל עוד יש קודקודים T מסומנים:

   i. A-סמן קודקוד T-מסומן (הוצא מ-T קודקוד כלשהו).

   ii. עבור על רשימת הקודקודים, אם יש קודקוד לא מסומן (בשום דבר), בדוק האם יש קשת בינו ובין הקודקוד ה-A-מסומן.

   אם יש, T-סמן את הקודקוד הנבדק.

   iii. C-נסמן את הקודקוד ה-A-מסומן.

   (ג) אם כל הקודקודים C-מסומנים נקבל, אחרת נדחה.

דוגמה $A_{DFA} = \{\langle A, w\rangle : w \in L(A)$ ו- DFA הוא $A\}$. נקודד את הקלט כרצף אותיות, #, רצף מצבים, דולר, מצב התחלתי, מצבים מקבלים וכו' מופרדים.

המ"ט תסמלץ ריצה של A על w. נשמור את המצב הנוכחי ואינדקס במילה, ובכל איטרציה נעדכן מצב ונגדיל אינדקס. נבדוק בכל פעם מה δ אומרת ואם נקבל בסוף נקבל ואחרת נדחה.

אם היה מדובר ב-A_{NFA}, פשוט נריץ את ה-NFA כאשר נשמור את קבוצת המצבים שאליהם אפשר להגיע בריצה כלשהי (כלומר subset construction פונקציונאלי).

אי כריעות

משפט יש שפה L כך ש-$L \notin R$.

הוכחה: משיקולי ספירה: עבור א"ב כלשהו, יש $2^{\aleph_0}$ שפות ב-Σ^*. עם זאת, יש רק $\aleph_0$ מ"ט, כי כל מ"ט ניתן לקודד באמצעות מספר סופי של תווים.

לחלופין, כל תכנית בפייתון מגדירה מ"ט, ויש $\aleph_0$ תכניות פייתון סופיות שמגדירות מ"ט.

ממשפט קנטור, $2^{\aleph_0} > \aleph_0$ ולכן יש שפה L כך שאין מ"ט שמכריעה אותה. ■

חלק ב' של ההרצאה

הוכחה: נבנה קונסטרוקטיבית: נצביע על שפה $L \notin \mathrm{R}$. $A_{TM} = \{\langle M, w\rangle : w \in L(M) \text{ ו- } M \text{ מ"ט}\}$. נוכיח כי $A_{TM} \notin \mathrm{R}$.

ראשית $A_{TM} \in \mathrm{RE}$ כי מ"ט אוניברסלית מזהה את A_{TM} - בהינתן M ו-w היא מריצה את M על w ועונה כמותה. אם M מקבלת את w אז תקבל גם. יתכן שהיא תתקע וזה בסדר כי זה יקרה רק אם M לא עוצרת.

נניח בשלילה כי קיימת מ"ט H מכריעה כך ש-$L(H) = A_{TM}$, כלומר $H(\langle M\rangle, w)$ מקבלת אם M מקבלת על w ודוחה אם M דוחה על w או לא עוצרת על w.

נבנה מ"ט $D(\langle M\rangle) = H(\langle M\rangle, \langle M\rangle)$ כלומר D מקבלת אם M מקבלת על $\langle M\rangle$ (המילה שמקודדת את M) ודוחה אחרת.

נבנה מ"ט $\widetilde{D}$ שמחליפה בין q_{acc} ו-q_{rej} של D, כלומר $\widetilde{D}$ מקבלת אם M דוחה או לא עוצרת על $\langle M\rangle$ ודוחה אם היא מקבלת על $\langle M\rangle$.

עתה מהו $\widetilde{D}\left(\left\langle \widetilde{D}\right\rangle\right)$? מההגדרה, היא תריץ את $\widetilde{D}$ על $\left\langle \widetilde{D}\right\rangle$ ותקבל אם $\widetilde{D}$ דוחה את $\widetilde{D}$ ותדחה אחרת, סתירה! ■

הערה נשים לב שהנ"ל היא סוג של הוכחה בלכסון! $2^{\aleph_0} > \aleph_0$ הוכחנו ע"י הנחה בשלילה האם יש סידור בן מנייה של $2^{\mathbb{N}}$ לקבוצות $S_1, S_2, \ldots$. נסדר אותם בטבלה ואז נסתכל על קבוצה שמוגדרת הפוך מהאלכסון, כלומר $i \in S$ אם"ם $i \notin s_i$. ואז S לא בטבלה.

עתה נוכל לכל מ"ט לסדר את $\langle M_i\rangle$ לפי האם היא מקבלת או לא, ואז D היא האלכסון ו-$\widetilde{D}$ היא הדואלי לאלכסון.

דוגמה $HALT_{TM} = \{\langle M, w\rangle : w \text{ עוצרת על } M\}$. לו הייתה מכונה M_2 שמכריעה את $HALT_{TM}$, היינו יכולים לבנות מכונה M_1 שמכריעה את A_{TM} סתירה.

נעשה זאת ע"י הרצת M_2. M_2 עוצרת ולכן אם היא עצרה ודחתה, נעצור, אם היא עצרה וקיבלה, נריץ את M_1 על w ללא חשש שנתקע, ונחזיר מה ש-M מחזירה.

הערה מתקיים $A_{TM} \subseteq HALT_{TM}$.

הגדרה $REG_{TM} = \{\langle M\rangle : L\left(M \in \text{REG}\right)\}$.

טענה $REG_{TM} \notin \text{R}$.

תרגול

טענה אם $L_1, L_2 \in \text{RE}$, אז $L_1 \cdot L_2 \in \text{RE}$.

הוכחה: ראשית נתאר מ"ט M_3 שמזהה את השפה $\{u\#v : u \in L, v \in L_2\}$. M_3 תסמלץ את ריצת M_1 על u, אם M_1 מקבלת את u, תסמלץ את M_2 על v. אם M_2 מקבלת אז M_3 תקבל.

עתה נשתמש ב-M_3 כדי לבנות מ"ט M שמזהה את $L_1 \cdot L_2$. נשים לב כי אם $w \in L_1 \cdot L_2$ אז קיימת חלוקה $w = uv$ כך ש-$u \in L_1, v \in L_2$ ובה"כ החלוקה היא באינדקס i ואז M_3 תקבל את המילה $u\#v$ אחרי מספר סופי k של צעדים.

M תפעל כך: תשמור את w במקום שמור בסרט, ואחריו 3 קאונטרים i, j, k (כמה צעדים לרוץ, באיזו חלוקה אנחנו, כמה צעדים רצנו עד כה, בהתאמה). בכל שלב בריצה, M תסמלץ את M_3 על החלוקה הנוכחית במשך i צעדים (תוך שימוש בקאונטר j). אם M_3 מקבלת תקבל, אחרת תמשיך הלאה עד מיצוי כל החלוקה במשך j צעדים. לאחר מכן נגדיל את j ב-1 ונאפס את מונה החלוקות ל-0 וכן $k = 0$.

אם קיימת חלוקה של w ל-uv כך ש-$u \in L_1, v \in L_2$ אז נקבל מתישהו, אחרת M_1 לא תעצור או תדחה או ש-M_2 לא תעצור או תדחה ולכן אנחנו לא נעצור או נדחה. ■

הגדרה <u>מכונת טיורינג אוניברסלית</u> היא מ"ט שמקבלת כקלט מ"ט M ומילה w ומתנהגת בדיוק כמו M על w, כלומר היא מסמלצת את M על w כאשר היא מקבלת/דוחה/לא עוצרת בהתאם ומסמלצת את תוכן הסרט.

הגדרה קידוד של מ"ט הוא $w_M \in \{0, 1, \#\}^*$.

- נקודד את המצבים ב-Q באמצעות מס' בינאריים בסדר עולה, מופרדים ע"י # (...0#1#00#), לבסוף נוסיף ###.
- נקודד את Γ (וכך גם את $\Sigma \subseteq \Gamma$). נעשה זאת באמצעות קידוד בינארי, שהוא באורך $\lceil \log_2 |\Gamma| \rceil$, ולבסוף ###.
- נקודד את פ' המעברים δ ע"י ## $\langle q\rangle$ # $\langle \sigma\rangle$ # $\langle q'\rangle$ # $\langle \sigma'\rangle$ # $\langle L/R\rangle$ ## לכל מעבר $\delta\left(q, \sigma\right) = \left(q', \sigma', L/R\right)$ ($\langle\cdot\rangle$ זה הקידוד של אובייקט כלשהו), כאשר $\langle L\rangle = 0, \langle L\rangle = R$. לבסוף נוסיף ###
- נקודד את המצבים המיוחדים ע"י $\langle q_{rej}\rangle$ # $\langle q_{acc}\rangle$ # $\langle q_0\rangle$.

נבנה מ"ט אוניברסילת U שמקבלת כקלט $\langle M, w\rangle$. U תהיה מכונה עם 3 סרטים. בסרט הראשון יהיה שמור תיאור של M, בסרט השני תתבצע סימולציה של הסרט של M, והסרט השלישי ישמור את המצב הנוכחי שבו M נמצאת וישמש לחישובים.

U תפעל כך:

1. תסרוק את סרט 1 ותמצא את w.
2. תעתיק את w לסרט 2 ותחזיר את הראש הקורא השני לתחילת סרט 2 ואת הראש הראשון לתחילת הסרט הראשון.
3. תסרוק את סרט 1, תמצא את q_0 ותעתיק לסרט 3 ושוב תחזיר את ראש 1 להתחלה.
4. בכל איטרציה:

- תשווה את המצב בסרט 3 ל-q_{acc}, q_{rej} ותקבל/תדחה לפי הצורך.
- תסרוק את סרט 1 ותמצא את תחילת התיאור של δ.
- תשווה את המצב בסרט 3 והאות מתחת לראש בסרט 2 לכל המעברים עד שתמצא את המעבר המתאים.
- תחליף את האות מתחת לראש בסרט 2 בהתאם למעבר שנמצא ותעביר את ראש 2 ימינה/שמאלה בהתאם.
- תחליף את המצב בסרט 3 לפי המעבר שנמצא.

הגדרה מכונת טיורינג א"ד (NTM) היא מ"ט עם $\delta : Q\backslash\{q_{acc}, q_{rej}\} \times \Gamma \to 2^{Q\times\Gamma\times\{L,R\}}\backslash\{\varnothing\}$. ויתקיים $w \in L(N)$ אס"ם קיימת ריצה מקבלת של N על w.

בהינתן מילה $w \in L^*$, עץ הריצה של מ"ט א"ד N על w הוא $T_{N,w} = \langle V, E\rangle$ המוגדר כך: תהי C קבוצה כל הקונפ' האפשריותת בריצה כלשהי של N על w.

- $V \subseteq C \times (\mathbb{N} \cup \{0\})$ כלומר כל קודקוד מגדיר קונפ' ומיקום בריצה.
- שורש העץ הוא $\langle q_0 w, 0\rangle$.
- $E \subseteq \bigcup\limits_{i\geq 0} (C \times \{i\}) \times (C \times \{i+1\})$ כאשר $E(\langle c, i\rangle, \langle d, i+1\rangle)$ אס"ם d היא קונפ' עוקבת של c.

טענה לכל מ"ט א"ד N קיימת מ"ט דטרמיניסטית M ששקולה לה.

הוכחה: M תפעל כך: בהינתן $w \in \Sigma^*$, M תבנה במהלך הריצה את עץ הריצה של N על w שלב אחר שלב, תוך שהיא מבצעת חיפוש BFS על הקודקודים ומחפשת מצב מקבל.

אם נמצא מצב מקבל, M מקבלת את w. אם כל הענפים עצרו במצב דוחה, M דוחה את w. אחרת, M תמשיך לרוץ ולא תעצור על w.

קל לראות ש-M מקבלת/דוחה/לא עוצרת אס"ם N מקבלת/דוחה/לא עוצרת. ■

הערה הבנייה הנ"ל מתרגמת ב-$\mathcal{O}\left(|Q|^{|w|}\right)$ את הריצה של N על w. לא ידוע האם אפשר לעשות זאת בזמן קצר יותר.

שבוע $\mathbb{VIII}$ | רדוקציה

הרצאה

חלק א' של ההרצאה

הגדרה $f:\Sigma^{*}\to\Sigma^{*}$ היא <u>פונקציה ניתנת לחישוב</u> אם קיימת מ"ט M_f שבהינתן קלט x, עוצרת עם $f\left(x\right)$ על הסרט.

דוגמה $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ המוגדרת ע"י $f\left(x,y\right)=x+y$. נניח ש-x,y מקודדים באונרית, ואז נניח שקיבלנו את x,y בהפרדה של #, כל שנצטרך לעשות הוא להסיר את ה-# ולהזיז את y אחד שמאלה.

דוגמה מ"ט $\to$ מ"ט : f המוגדרת ע"י $f\left(\left\langle M\right\rangle \right)=\left\langle M'\right\rangle$ כך ש-$L\left(M'\right)=L\left(M\right)$ ו-M' לא עוצרת על קלטים שאינם ב-$L\left(M\right)$. נצטרך לקבל קידוד של מכונה, ואז לקודד מצב חדש q_{loop} עם חוג עצמי ולשנות את המעברים שהולכים ל-q_{rej} ל-q_{loop}.

הגדרה עבור שתי שפות $A,B\subseteq\Sigma^{*}$, נאמר כי A ניתנת לרדוקצית מיפוי ל-B ונסמן $A\leq_{m}B$ אם קיימת פ' ניתן לחישוב $f:\Sigma^{*}\to\Sigma^{*}$ כך שלכל $w\in\Sigma^{*}$ מתקיים $w\in A\iff f\left(w\right)\in B$.

הערה אם $A\leq_{m}B$ אז נוכל במקום לשאול שאלות שייכות ל-A נוכל לשאול לשייכות ב-B.

דוגמה $A=\left\{ x:\left|x\right|\leq5\right\} ,B=\left\{ x:\left|x\right|\leq10\right\}$. נניח שקשה לנו לחשב האם $w\in A$, נוכל להגדיר $f\left(y\right)=2y$ ועם הפ' הזו יתקיים $A\leq_{m}B$ ונוכל להיעזר בשייכות ל-B כדי להגיד דברים על A.

משפט (הרדוקציה) לכל A,B, $A\leq_{m}B$ ו-$B\in R$ אז $A\in R$.

הוכחה: יהיו מ"ט M_B שמכריעה את B ומ"ט M_f שמחשבת את הרדוקציה מ-A ל-B. נבנה M_A שמכריעה את A.

בהינתן $w\in\Sigma^{*}$, M_A מריצה את M_f על w ואז מריצה את M_B על $f\left(w\right)$ ועונה כמוה.

נשים לב ש-M_A עוצרת על כל קלט והיא נכונה כי $f\left(w\right)\in L\left(M_{B}\right)\iff f\left(w\right)\in B\iff w\in A$. ■

מסקנה אם $A\leq_{m}B$ אז A "קלה" מ-B.

הערה נשתמש הרבה במשפט הרדוקציה כי אם $A\leq_{m}B$ ו-$A\notin R$ אז $B\notin R$.

דוגמה נראה שוב ש-$HALT_{TM}\notin R$ עם משפט הרדוקציה. ידוע לנו ש-$A_{TM}\notin R$. נראה ש-$A_{TM}\leq_{m}HALT_{TM}$ ונסיים.

נצטרך גדיר פ' $f:\left\{ A_{TM}\text{-קלטים ל}\right\} \to\left\{ HALT_{TM}\text{-קלטים ל}\right\}$ כך ש-$f\left(\left\langle M\right\rangle ,w\right)=\left\langle M'\right\rangle ,w'$ כך ש-M מקבלת את w אם"ם M' עוצרת על w'.

בהינתן $\left\langle M\right\rangle ,w$ הפ' f תחזיר $w'=w$ ו-M' מכונה שעוצרת רק כשהיא מקבלת ואחרת מתבדרת (כמו שראינו בדוגמה למעלה עם q_{loop}).

f אכן ניתן לחישוב. וכן מתקיים $\left(\left\langle M'\right\rangle ,w'\right)\in HALT_{TM}\iff\left(\left\langle M\right\rangle ,w\right)\in A_{TM}$ כי:

- אם $\left\langle M\right\rangle ,w\in A_{TM}$ אז M' עוצרת על w.
- אם $\left\langle M\right\rangle ,w\notin A_{TM}$ אז אם M לא עצרה על w, M' לא עוצרת על w'.

כלומר אם M דחתה את w, אז M' תגיע ל-q_{loop} ותתקע על w'.

דוגמה $\{M\}$ עוצרת על ϵ, $HALT^{\epsilon}_{TM} = \{\langle M\rangle$. זו שפה ב-RE כי אפשר פשוט להריץ ולקבל אם עוצרים (ואם נתקעים אז זה בסדר). נוכיח כי $HALT^{\epsilon}_{TM} \notin R$ ע"י הוכחת $HALT^{\epsilon}_{TM} \leq_m HALT^{\epsilon}_{TM}$.

נגדיר $\{HALT^{\epsilon}_{TM}$-קלטים ל$\} \rightarrow \{HALT_{TM}$-קלטים ל$\} : f$ ע"י $f(\langle M\rangle, w) = \langle M'\rangle$ כאשר M' היא מכונה שמוחקת את מילת הקלט ומריצה את M על w (לא משנה מה הקלט, בפרט אם הוא ϵ).

אכן f ניתן לחישוב כי כל מה שצריך לעשות זה למחוק כמה אותיות, להוסיף מילה קבועה וללכת למצב ההתחלתי של M.

M עוצרת על w אם"ם M' עוצרת על ϵ כי M' מסמלצת ריצה של M על w בהינתן כל קלט.

דוגמה $\mathrm{REG}_{TM} = \{\langle M\rangle : L(M) \in \mathrm{REG}\}$. נוכיח כי $\mathrm{REG}_{TM} \notin \mathrm{RE}$ וגם לא $\mathrm{REG}_{TM} \notin \text{co-RE}$. ראשית נראה כי $\mathrm{REG}_{TM} \notin R$.

נראה כי $A_{TM} \leq_m \mathrm{REG}_{TM}$, כלומר, נראה שיש פ' f שבהינתן $\langle M\rangle, w$ (קלט למ"ט ב-A_{TM}), מחזירה $\langle M'\rangle$ (קלט למ"ט ב-REG_{TM}) כך ש-M מקבלת את w אם"ם $L(M')$ רגולרית (w לא ממש משנה כאן).

בהינתן $\langle M\rangle, w$ נגדיר M' שמקבלת $x \in (0+1)^*$ כך:

1. אם $x \in \{0^n1^n : n \geq 0\}$ אז M' מקבלת את x.
2. אחרת M' מריצה את M על w ועונה כמוה.

הרדוקציה נכונה, כלומר $\langle M, w\rangle \in A_{TM}$ אם"ם $\langle M'\rangle \in \mathrm{REG}_{TM}$ כי:

1. אם M מקבלת את w אז נחזיר M' שמקבלת כל $x \in (0+1)^*$ (או שנקבל בשלב הראשון או שבטוח מקבלת בשלב השני) כלומר $L(M') = (0+1)^*$ שזה אכן רגולרי.
2. אם M לא מקבלת את w אז נחזיר M' שמקבלת את $x \in (0+1)^*$ אם"ם $x \in \{0^n1^n : n \geq 0\}$ ואז $L(M') = \{0^n1^n : n \geq 0\}$ שזה אכן לא רגולרי.

נשים לב שלא בנינו כאן מבחין לשפות רגולריות, אלא רק התאמה בין השאלה (ה"קלה") האם M מקבלת את w לשאלה (ה"קשה") האם שפה של מ"ט היא רגולרית.

$L(M')$ היא אחת מבין שתי אפשרויות: $(0+1)^*$ שהיא רגולרית ומייצגת קבלה של M על w ו-$\{0^n1^n\}$ שמייצגת אי קבלה של M על w (שפות הדמה הן proxy לשאלה הקבלה של M).

לכן $A_{TM} \leq_m \mathrm{REG}_{TM}$ וידוע כי $A_{TM} \notin R$ ולכן $\mathrm{REG}_{TM} \notin R$.

משפט (הרדוקציה, גרסת RE) אם $A \leq_m B$ ו-$B \in \mathrm{RE}$ אז $A \in \mathrm{RE}$ ואם $B \in \text{co-RE}$ אז $A \in \text{co-RE}$.

הערה $A \leq_m B$ אם"ם $\overline{A} \leq_m \overline{B}$ (באמצעות אותה פ' ניתנת לחישוב).

דוגמה נמשיך עם REG_{TM}. ידוע כי $A_{TM} \in \mathrm{RE}\backslash\mathrm{R}$ ולכן בהכרח $A_{TM} \notin \text{co-RE}$ (אחרת $A_{TM} \in \mathrm{RE} \cap \text{co-RE} = R$).

לכן מהיות $A_{TM} \leq_m \mathrm{REG}_{TM}$ (הוכחנו למעלה) הרי ש-$\mathrm{REG}_{TM} \notin \text{co-RE}$.

בהמשך לנימוק הנ"ל, $\overline{A_{TM}} \notin \mathrm{RE}$ ומספיק שנראה $\overline{A_{TM}} \leq_m \mathrm{REG}_{TM}$ ואז מהיות $\overline{A_{TM}} \notin \mathrm{RE}$ נקבל $\mathrm{REG}_{TM} \notin \mathrm{RE}$.

לשם כך מספיק שנוכיח כי $A_{TM} \leq_m \overline{\mathrm{REG}_{TM}}$ ואז מההערה הנ"ל נקבל את הנדרש.

נמצא פ' ניתנת לחישוב שעבור $f(M,w)=M'$ מתקיים ש-M מקבלת את w אם"ם $L(M')$ לא רגולרית.

על קלט $x\in(0+1)^*$ המכונה M' תפעל כך:

1. אם $x\in\{0^n1^n:n\geq 0\}$ אז M' מריצה את M על w ועונה כמוה.
2. אחרת תדחה את x.

הרדוקציה נכונה, כלומר M מקבלת על w אם"ם $L(M)\notin\text{REG}$ כי:

- אם M מקבלת את w אז $L(M')=\{0^n1^n:n\geq 0\}\notin\text{REG}$.
- אם M לא מקבלת את w אז נדחה ב-1 תמיד וגם ב-2 ולכן $L(M')=\varnothing\in\text{REG}$.

חלק ב' של ההרצאה

דוגמה $A=(00)^*, B=A_{TM}$. מתקיים $(00)^*\leq_m A_{TM}$ (אינטואיטיבית $(00)^*$ מאוד קלה). נוכיח זאת.

נגדיר $f(x)=\begin{cases}\langle M_1\rangle,\epsilon & x\in(00)^*\\ \langle M_2\rangle,\epsilon & x\notin(00)^*\end{cases}$ כאשר M_1 תמיד עוצרת (קל לבנות) ו-M_2 נתקעת תמיד.

לא מתקיים כמובן $A_{TM}\leq_m(00)^*$ כי $(00)^*\in\text{R}$ אבל כמובן ש-$A_{TM}\notin\text{R}$.

דוגמה בבעיית הריצוף יש לנו אריחים עם ארבעה צבעים בכל כיוון ואנחנו רוצים לרצף "יפה". פורמלית,

$$TILE=\{\langle T,H,V,t_0\rangle:1\leq n\text{ לכל }n\times n\text{ יש ריצוף חוקי}\}$$

כאשר:

- $T=\{t_0,\ldots t_k\}$ קבוצה סופית של אריחים.
- $H\subseteq T\times T$ תנאי שכנות במאוזן ($(t,t')\in H$ אם"ם אפשר לשים את t משמאל ל-t').
- $V\subseteq T\times T$ תנאי שכנות במאונך.
- t_0 אריח התחלתי.

וריצוף חוקי הוא $f:[n]\times[n]\to T$ כך ש-$f(1,1)=t_0$ ומתקיים $H(f(i,j),f(i+1,j))$ לכל $i\in[n-1],j\in[n]$ ו-$V(f(i,j),(i,j+1))$ לכל $i\in[n],j\in[n-1]$.

נוכיח כי $TILE\in\text{co-RE}$, כלומר $\overline{TILE}\in\text{RE}$, כלומר שקיימת מכונה שמזהה האם קיים $n\geq 1$ כך שאין ריצוף חוקי $n\times n$. המכונה פשוט תבדוק את כל $|T|^{n^2}$ הריצופים $n\times n$ ואם אין עבור n כלשהו, מקבלת, אחרת תמשיך ל-n הבא.

נוכיח ש-$TILE\notin\text{R}$ (ומכוח כך גם $TILE\notin\text{RE}$). נשים לב שהגדרה שקולה של $TILE$ היא

$$TILE=\{\langle T,H,V,t_0\rangle:\text{יש ריצוף חוקי של רבע מישור}\}$$

כאשר ריצוף חוקי על רבע מישור משמעו שקיימת $f:\mathbb{N}\times\mathbb{N}\to T$ כך שמתקיימים יחסי שכנות חוקיים לכל $i,j\in\mathbb{N}$.

נראה את שקילות ההגדרות באמצעות הלמה של קניג, לפיה בעץ מכוון אינסופי עם דרגת פיצול סופית, יש מסלול אינסופי. נגדיר עץ באופן הבא:

השורש יהיה ריצוף 1×1 והילדים שלו יהיו כל הריצופים החוקיים 2×2 שמכילים את הריצוף, והילדים שלהם יהיו כל הריצופים 3×3 שמכילים את ההורים שלהם וכו'. מהלמה של קניג, יש כאן מסלול אינסופי ולכן יש שייכות ל-$TILE$ (נרד בעץ כמה שצריך עד שנגיע לריצוף שמכיל את i,j כדי לראות שהשכנות חוקית).

נחזור להוכחה ש-$TILE\notin\mathrm{R}$. נראה ש-$\overline{HALT_{TM}^{\epsilon}}$ (כל המ"ט שלא עוצרות על ϵ) ניתנת לרדוקציית מיפוי ל-$TILE$.

קונפ' של M היא מילה ב-$\Gamma^{*}\cdot(Q\times\Gamma)\cdot\Gamma^{*}$. נגרום לכל קונפ' להיות שורה של אריחים ברבע מישור ונגדיר שכנות חוקית רק אם קונפ' הן עוקבות בריצה של M על ϵ. לבסוף יהיה ריצוף חוקי אינסופי אם"ם M לא עוצרת אף פעם על ϵ כלומר $\langle M\rangle\in\overline{HALT_{TM}^{\epsilon}}$.

נגדיר את האריחים שיממשו את הרעיון:

1. מרצפות השורה הראשונה: t_0 הוא $\_\,\overset{(q_0,\_)}{\underset{*}{}}\,*$ והשאר הם $\_\,\overset{\_}{\underset{*}{}}\,\_$.
2. מרצפות שמתאימות לתזוזה של הראש.
3. ריפוד: לכל $c\in\Gamma$, נוסיף את המרצפת $*\,\overset{c}{\underset{c}{}}\,*$.

תרגול

משפט (הרדוקציה ל-RE) יהיו L_1,L_2 שפות כך ש-$L_1\le_m L_2$.

1. אם $L_2\in\mathrm{RE}$ אז גם $L_1\in\mathrm{RE}$.
2. אם $L_1\in\text{co-RE}$ אז גם $L_2\in\text{co-RE}$.

הוכחה: קיימת מ"ט M שמזהה את L_2 ופ' ניתנת לחישוב $f:\Sigma^{*}\to\Sigma^{*}$ כך ש-$f(x)\in L_2\iff x\in L_1$ ולכן קיימת M_f מ"ט שמחשבת את f. נגדיר N שמזהה את L_1: N תחשב את $f(X)$ ותסמלץ את ריצת M על $f(x)$.

נשים לב כי N מקבלת את x אם"ם M מקבלת את $f(x)$ אם"ם $f(x)\in L_2$ אם"ם $x\in L_1$. לכן N מזהה את L_1 כלומר $L_1\in\mathrm{RE}$. ■

הערה כדי להוכיח רדוקציית מיפוי נבצע שלושה שלבים:

1. נזהה את הצורה של הרדוקציה ונבחר פ' מיפוי.
2. נוכיח שהפ' ניתן לחישוב.
3. נוכיח נכונות של הרדוקציה.

סיווג שפות

1. $ALL_{TM} = \{\langle M\rangle : L(M) = \Sigma^*\}$. נוכיח כי $ALL_{TM} \notin \overline{\text{RE} \cup \text{co-RE}}$. מספיק שנוכיח כי $A_{TM} \le_m ALL_{TM}$ (ואז $ALL_{TM} \notin \text{co-RE}$ כי $A_{TM} \notin \text{co-RE}$) וגם $\overline{A_{TM}} \le_m ALL_{TM}$.

(א) נראה ש-$ALL_{TM} \notin \text{co-RE}$. נמצא פ' ניתנת לחישוב f שמקיימת $f(x) \in ALL_{TM} \iff x \in A_{TM}$, כלומר

$$\langle M, w\rangle \in A_{TM} \iff f(\langle M, w\rangle) = \langle M'\rangle \in ALL_{TM}$$

נגדיר את f כך: f תמפה את $\langle M, w\rangle$ ל-M' שפועלת כך: בהינתן $x \in \Sigma^*$, M' מתעלמת מ-x ומסמלצת את M על w ומקבלת את (כל) x אם"ם M מקבלת את w.

נשים לב כי f ניתן לחישוב כי ניתן בזמן סופי לייצר את M' שמסמלצת את M על w.

אם $\langle M, w\rangle \in A_{TM}$ אז M מקבלת את w (מההגדרה) ולכן $\forall x \in \Sigma^*$, M' תקבל את x ואז $L(M') = \Sigma^*$.

אם $\langle M, w\rangle \in A_{TM}$ אז M לא מקבל את w ואז M' לא תקבל אף מילה כלומר $L(M') = \varnothing$ ובפרט $L(M') \neq \Sigma^*$.

לכן סה"כ קיבלנו $\langle M, w\rangle \in A_{TM}$ אם"ם $\langle M'\rangle \in ALL_{TM}$ כלומר הוכחנו נכונות של הרדיקוציה.

(ב) נראה ש-$ALL_{TM} \notin \text{RE}$ ע"י רדוקציה מ-$\overline{A_{TM}}$. נגדיר f שבהינתן $\langle M, w\rangle$, ממפה למ"ט M' שפועלת כך: בהינתן x, נסמלץ את M על w למשך $|x|$ צעדים ונדחה אם"ם M קיבלה.

f ניתן לחישוב כי חישוב מילה אפשר לעשות בזמן סופי, ולהחזיר מ"ט שמסמלצת את הנ"ל גם קורה בזמן סופי.

אם $\langle M, w\rangle \in \overline{A_{TM}}$ אז M לא מקבלת על w ולכן M' תמיד תקבל (כי M אף פעם לא תקבל את w לא משנה כמה צעדים נריץ אותה) כלומר $L(M') = \Sigma^*$.

אם $\langle M, w\rangle \notin \overline{A_{TM}}$ אז M מקבלת את w ולכן M' תדחה מתישהו כי עבור קלט מספיק ארוך נסמלץ את M על w מספיק צעדים כך שתקבל ואז נדחה. לכן $L(M') \neq \Sigma^*$.

לכן סה"כ קיבלנו $\langle M, w\rangle \in \overline{A_{TM}}$ אם"ם $\langle M'\rangle \in ALL_{TM}$ כלומר הוכחנו נכונות של הרדיקוציה.

2.

$$U = USELESS = \{\langle M\rangle : \text{יש מצד ב-}M\text{ שאינו } q_{rej} \text{ ו-} q_{acc} \text{ שלא מבקרים בו לעולם}\}$$

נשים לב שגם אם יש בפ' המעברים מעבר למצב לא בהכרח שנגיע אליו. נראה ש-$U \in \text{co-RE}\backslash\text{RE}$.

(א) ראשית נראה כי $U \in \text{co-RE}$. נבנה מ"ט T שמזהה את $\overline{U}$, כלומר אוסף המ"ט שבהם כל המצבים משומשים, שתפעל כך:

T תבדוק אם הקלט הוא קידוד תקין של מ"ט, אם לא, תקבל. אחרת נסמן $x = \langle M\rangle$ ואז T תסמלץ את ריצת $\langle M\rangle$ במקביל באופן אינקרמנטלי (בסדר minlex) ותשמור על סרט נפרד את כל המצבים שבוקרו עד כה. אם כל המצבים חוץ מ-q_{acc}, q_{rej} של M בוקרו, T תקבל את $\langle M\rangle$ (אחרת נתקע).

T נכונה כי אם $x \in \overline{L}$ אז או ש-x לא קידוד תקין של מ"ט ואז T מקבלת או ש-$x = \langle M\rangle$ ו-M מבקרת בכל המצבים שלה מתישהו כלומר T תקבל. אם $x \notin \overline{L}$ אז $x = \langle M\rangle$ וב-M יש מצב לא ישיג ולכן T אף פעם לא תקבל כלומר תרוץ לנצח. לכן $L(T) = \overline{U}$.

(ב) נוכיח כי $U \notin \mathrm{RE}$. נראה רדוקציית מיפוי מ-$\overline{A_{TM}}$ ל-U. הרדוקציה תקיים

$$\langle M,w\rangle \in \overline{A_{TM}} \iff \langle M'\rangle = f\left(\langle M,w\rangle\right) \in U$$

כלומר, M לא מקבלת את w אם"ם יש ב-M' מצב לא ישיג.

נגדיר f כך: f תמפה את $\langle M,w\rangle$ ל-M' שפועלת כך: בהינתן x, M' תסמלץ את M על w. אם M מקבלת את w, M' תיכנס למצב חדש שממנו תבקר בכל מצביה (של M') לא כולל q_{acc}, q_{rej}, אחרת M' דוחה (ולא עוברת במצב החדש).

אם $\langle M,w\rangle \in \overline{A_{TM}}$ אז M לא מקבלת על w ולכן M' לעולם לא תבקר במצב החדש כלומר $\langle M'\rangle \in U$.

אם $\langle M,w\rangle \notin \overline{A_{TM}}$ אז M מקבלת על w לכן M' עוברת על כל המצבים שלה כלומר $\langle M'\rangle \notin U$.

f ניתן לחישוב כי סמלוץ היא פעולה חשיבה, לכן נותר להראות שניתן לממש את מצב הטיול. נוסיף @ לא"ב של M'. נגדיר מעבר ממצב טיול ל-@ למצב הראשון של M' ובכל מצב נוסיף מעבר עם @ למעבר הבא בקידוד כשאנחנו לא מזיזים את הראש (ראינו שקל לעשות). להוסיף את הקידוד הזה אפשר לעשות בזמן לינארי במספר המצבים, שזה כמובן סופי.

.3

$$REP = REPEAT = \{\langle M,w\rangle : \text{מ"ט שלא עוצרת על } w \text{ ויש קונפ' בריצת } M \text{ על } w \text{ שחוזרת פעמיים } M\}$$

נשים לב שאם יש קונפ' כזו, אף פעם לא נעצור (נחזור עליה שוב ושוב). בנוסף, קל לבנות מכונה שלא עוצרת אבל שאין לה קונפ' חוזרת (לדוגמה הולך ימינה כל הזמן). נראה ש-$REP \in \mathrm{RE}\backslash\mathrm{R}$.

(א) נגדיר T מ"ט שמזהה את REP. T תפעל כך: בהינתן $\langle M,w\rangle$ היא תסמלץ את M על w תוך שמירת כל הקונפ' שבוקרו עד כה בסרט נפרד . בכל שלב היא תסרוק את הקונפ' הקודמות ותשווה לנוכחית. אם נמצאה חזרה, T תקבל את $\langle M,w\rangle$. אם M עוצרת אז T תיכנס ללולאה אינסופית.

T ניתן למימוש כי סמלוץ ראינו איך לעשות ומעקב קונפ' זו פעולה חשיבה.

אם $\langle M,w\rangle \in REP$ אז M לא עוצרת על w ויש חזרה על קונפ' בריצת M על w. לכן T במופע השני של הקונפ' תזהה את החזרה ותקבל את $\langle M,w\rangle$.

אם $\langle M,w\rangle \notin REP$ אז M לא חוזרת על קונפ' בריצת M על w כלומר T לא עוצרת על $\langle M,w\rangle$.

(ב) נראה ש-$REP \notin \text{co-RE}$ ע"י רדוקציה $HALT_{TM} \le_m REP$. צריך להתקיים

$$\langle M,w\rangle \in HALT_{TM} \iff \langle N,w'\rangle \in REP$$

כלומר M עוצרת על w אם"ם יש קונפ' שחוזרת בריצת N על w'.

נגדיר f שבהינתן $\langle M,w\rangle$, מחזירה $\langle N,w'\rangle$ שמסמלצת את M על w, ואם היא עוצרת, N תחזור על קונפ' שלה (תיכנס ללולאה שלא משנה את הסרט), ואחרת נתקע וכמובן לא נחזור על קונפ'.

f ניתן לחישוב כי צריך רק להוסיף עוד מצב ללולאה של הקונפ' החוזרת לקידוד המ"ט. נכונות נובעת ישירות.

שבוע $\mathbb{IX}$ | תורת הסיבוכיות

הרצאה

חלק א׳ של ההרצאה

נסיים את ההוכחה שבעיית הריצוף אינה כריעה. ראינו ש-$TILE$ שקולה לריצוף חוקי של רבע מישור באמצעות הלמה של קניג. נעשה רידוקציה מ-$\overline{HALT^{\epsilon}_{TM}}$ ל-$TILE$ וכך נוכיח ש-$TILE \notin \mathrm{R}$.

מסוף ההרצאה הקודמת:

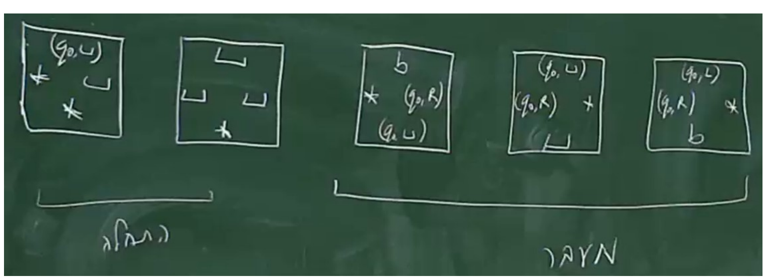
> נגרום לכל קונפ׳ להיות שורה של אריחים ברבע מישור ונגדיר שכנות חוקית רק אם קונפ׳ הן עוקבות בריצה של M על ϵ. לבסוף יהיה ריצוף חוקי אינסופי אם״ם M לא עוצרת אף פעם על ϵ כלומר $\langle M\rangle \in \overline{HALT^{\epsilon}_{TM}}$.

האריחים בהם נשתמש הם כאלה:

1. מרצפות השורה הראשונה: t_0 הוא $\boxed{\begin{array}{ccc} & (q_0,\_) & \\ * & & \_ \\ & * & \end{array}}$ והשאר הם $\boxed{\begin{array}{ccc} & \_ & \\ \_ & & \_ \\ & * & \end{array}}$.
2. מרצפות עבור מעברים:
   - לכל מעבר $\delta(q,a)=(q',b,R)$ עבור $q\notin\{q_{acc},q_{rej}\}$, המרצפת $\boxed{\begin{array}{ccc} & b & \\ * & & (q',R) \\ & (q,a) & \end{array}}$ ולכל אות $c\in\Gamma$ גם $\boxed{\begin{array}{ccc} & (q',c) & \\ (q',R) & & * \\ & c & \end{array}}$.
   - לכל מעבר $\delta(q,a)=(q',b,L)$ עבור $q\notin\{q_{acc},q_{rej}\}$, הרמצפת $\boxed{\begin{array}{ccc} & b & \\ (q',L) & & * \\ & (q,a) & \end{array}}$ ולכל אות $c\in\Gamma$ גם $\boxed{\begin{array}{ccc} & (q',c) & \\ * & & (q',L) \\ & c & \end{array}}$.
3. ריפוד: לכל $c\in\Gamma$, נוסיף את המרצפת $\boxed{\begin{array}{ccc} & c & \\ * & & * \\ & c & \end{array}}$.

נשים לב כי ב-T יש 2 מרצפות התחלתיות, $|\Gamma|+1$ לכל מעבר ו-$|\Gamma|$ ריפוד כלומר מספר סופי פרופורציוני ל-$|\Gamma|$.

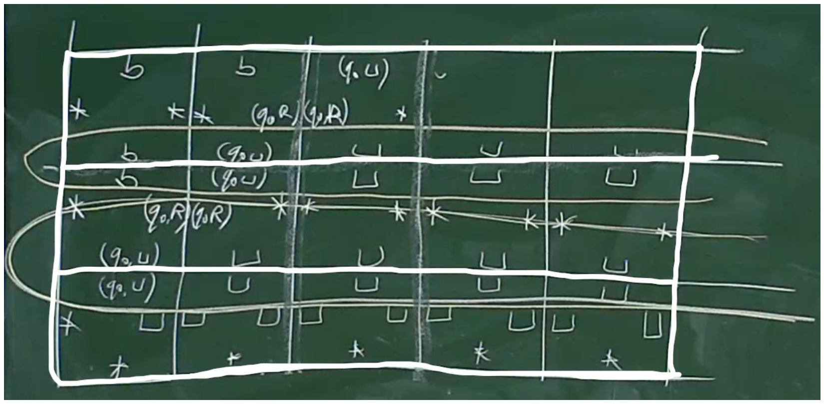
דוגמה נגדיר מ״ט עם $\Gamma=\{\_,b\}$ ופ׳ מעברים $\delta(q_0,\_)=(q_0,b,R)$. זו מכונה שלא עוצרת אף פעם (כל הזמן הולכת ימינה). נראה שאכן הרדוקציה מניבה ריצוף חוקי.



איור 37: המרצפות ב-T המתאים למ״ט שהגדרנו, בלי מרצפות הריפוד

בהינתן הקונפ׳ ההתחלתית (השורה הראשונה, המוגדרת עם t_0), ננסה לבנות ריצוף חוקי. באיור נין לראות את הריצוף, כאשר השרוולים על הצלעות הצמודות מדגימות כיצד הקונפ׳ מתבטאת בחיבור הזה. נשים לב כי לאחר הקונפ׳ ההתחלתית, הדבר היחיד

שאפשר לעשות זה להוסיף מעליה שורה שמגדירה את הקונפ' $bq_0\_$, ואז בשורה הבאה בעיקרון אפשר לבחור משהו אחר עבור האריח השמאלי ביותר אבל נתעלם לעתה מהמקרה הזה - אחד הריצופים החוקיים שניתן לשים הוא באמת הקונפ' השלישית בריצת המ"ט על ϵ וכן הלאה.



איור 38 : דוגמת ריצוף לקונפ' המגדירות את ריצת המ"ט על ϵ

טענה M לא עוצרת על ϵ אם"ם יש ריצוף חוקי של רבע מישור עם T המושרה מ-M.

הוכחה: $\Leftarrow$: זה עתה הראנו את הקונפ' שמאפשרות ריצוף שיכולה להמשיך עד אינסוף לדוגמה הספציפית הזו, אבל זה מתקיים גם במקרה הכללי (פשוט לא נראה פורמלית).

$\Rightarrow$: אם היינו עוצרים אז היה לנו q_{acc}/q_{rej} ואז לא היו לנו מרצפות חוקיות להמשיך איתן למעלה (המרצפות מוגדרות לכל $q \notin \{q_{acc}, q_{rej}\}$).

ברמה העקרונית: אם היינו מוסיפים עוד ראש קורא באריח השמאלי באיזשהו שלב (אפשרי מהגדרת האריחים), היינו רק מקשים על עצמנו כי לכל הפחות שהיו לנו יותר מרצפות לא חוקיות (כאלו עם q_{acc}, q_{rej}). ■

עד כה ראינו את R, RE, co-RE. עתה נסתכל מה קורה בתוך R. ראינו אפיון אחד והוא סיווג לפי REG, CFL וכו'. האפיון הנוסף שניתן להביט בו על R הוא כמות המשאבים שדרושים להכרעה (זמן, זכרון, אקראיות וכו').

דוגמה $L = \left\{0^k 1^k : k \geq 0\right\}$. כדי להכריע את השפה, ניתן להגדיר מ"ט שמכריע את השפה ע"י מחיקה של ה-0 ואז ה-1 הראשון וה-0 וה-1 השני וכו' עד שאין עוד אותיות. הסיבוכיות של האלג' היא $\mathcal{O}\left(k^2\right)$ כי אנחנו עושים k איטרציות שכל אחת מהן דורשת $\mathcal{O}\left(k\right)$ צעדים.

הגדרה לכל $t : \mathbb{N} \to \mathbb{N}$, נגדיר מחלקה

$$TIME\left(t\left(n\right)\right) = \{L : \text{קיימת מ"ט דטרמיניסטית חד סרטית שמכריעה את } L \text{ ועוצרת על כל קלט } w \text{ תוך } \mathcal{O}\left(t\left(|w|\right)\right) \text{ צעדים}\}$$

דוגמה השפה הנ"ל היא ב-$TIME\left(n^2\right)$ ולמעשה גם ב-$TIME\left(n \log n\right)$ ע"י מחיקה של חצי מהאותיות (וציפוף המילה) בכל פעם.

משפט אם ניתן להכריע את L ב-$o\left(n \log n\right)$ (פחות ממש מ-$\mathcal{O}\left(n \log n\right)$) אז L רגולרית.

מסקנה השפה הנ"ל לא ניתנת להכרעה בפחות מ-$\mathcal{O}\left(n\log n\right)$ צעדים.

הערה החד-סטריות חשובה כי אפשר לעשות כל מיני דברים במקביל שמגלמים בתוכם סיבוכיות יותר מורכבת עם כמה סרטים.

טענה (שראינו בתרגול) לכל מ"ט רב סרטית דטר' שרצה בזמן $\mathcal{O}\left(t\left(n\right)\right)$ יש מ"ט דטר' שקולה שרצה בזמן $\mathcal{O}\left(t^{2}\left(n\right)\right)$.

הגדרה נגדיר את המחלקה $PTIME=\bigcup_{i\geq0}TIME\left(n^{i}\right)$, כלומר כל השפות שניתן להכריע בזמן פולינומיאלי, ונסמן $\mathsf{NP}=NPTIME$.

הערה בגלל שנסתכל על סיבוכיות פולינומיאלית לעומת לא פולינומיאלית, לא יעניין אותנו עוד ריבוע על פולינום ולכן נוכל להניח שהמ"ט שלנו יכולה להיות גם רב סרטית.

הערה עבור מ"ט א"ד, נגדיר את זמן הריצה להיות המסלול הכי ארוך בעץ הריצה (וכמובן נאמר שהיא מכריעה שפה אם כל הריצות שלה סופיות).

טענה (שראינו בתרגול) לכל מ"ט א"ד שרצה בזמן $\mathcal{O}\left(t\left(n\right)\right)$, ישנה מ"ט דטר' שקולה שרצה בזמן $2^{\mathcal{O}\left(t\left(n\right)\right)}$ (באמצעות סימלוץ כל הריצות יחד).

הגדרה לכל $t:\mathbb{N}\to\mathbb{N}$ נגדיר

$$NTIME\left(t\left(n\right)\right)=\left\{ L:\text{קיימת מ"ט א"ד חד סרטית שמכריעה את }L\text{ ועוצרת על כל קלט }w\text{ תוך }\mathcal{O}\left(t\left(\left|w\right|\right)\right)\text{ צעדים}\right\}$$

הגדרה נגדיר את המחלקה $NPTIME=\bigcup_{i\geq0}NTIME\left(n^{i}\right)$, כלומר כל השפות שניתן להכריע בזמן פולינומיאלי באמצעות ניחושים, ונסמן $\mathsf{NP}=NPTIME$.

הגדרה $\mathsf{EXPTIME}=\bigcup_{i\geq0}TIME\left(2^{n^{i}}\right)$ כלומר שניתן בסיבוכיות אקס' להכריע אותן עם מ"ט דטר'.

הערה מתקיים $\mathsf{P}\subseteq\mathsf{NP}\subseteq\mathsf{EXPTIME}$ אבל לא ידוע אילו מההכלות הן ממש ואיפה יש שוויון (לא ייתכנו שני שוויונים כי ידועות שפות $L\in\mathsf{EXPTIME}\backslash\mathsf{P}$-ב).

דוגמה בהינתן גרף $G=\left\langle V,E\right\rangle$, מסלול אוילר ב-$G$ הוא מסלול שעובר בככל הקשתות ב-G בדיוק פעם אחת ומסלול אוילר ב-G הוא מסלול שעובר בכל הקודקודים ב-G בדיוק פעם אחת.

נגדיר את המחלקות

$$\mathsf{D-ST-HAMPATH}=\left\{ \left\langle G,s,t\right\rangle :G\text{ גרף מכוון ויש מסלול המילטון מ-}s\text{ ל-}t\right\}$$

ו-

$$\mathsf{U-HAMPATH}=\left\{ \left\langle G\right\rangle :G\text{ לא מכוון ומכיל מסלול המילטון}\right\}$$

לא ידוע האם $\mathsf{D-ST-HAMPATH} \in \mathsf{P}$ אבל ידוע שהיא ב-$\mathsf{EXPTIME} \subseteq \mathsf{NP}$ כי יש מ"ט דטרמיניסטי שמכריעה אותה בזמן אקס' שפועלת באופן הבא: בהינתן G, s, t, עוברת על כל המילים ב-V^n ולכל מילה, בודקת האם מתחילה ב-s מסתיימת ב-t ומכילה את כל הקודקודים בדיוק פעם אחת ומהווה מסלול, ואם כן, מקבלת.

עתה נוכיח כי $\mathsf{D-ST-HAMPATH} \in \mathsf{NP}$. מ"ט א"ד שמכריעה את השפה בזמן פולינומיאלי תפעל כך: בהינתן G, s, t, מנחשת מילה π ב-V^n ומקבלת אם"ם π היא מסלול המילטון מ-s ל-t.

הבדיקה על π דורשת זמן פולינומיאלי ולכן השפה דורשת זמן פולינומיאלי.

דוגמה $\mathsf{COMPOSITE} = \{x \in \mathbb{N} : 1 \neq \exists p, q \in \mathbb{N}, n = pq\}$ כאשר x נתון בבינארית (כל הפריקים).

$\mathsf{COMPOSITE} \in \mathsf{EXPTIME}$ כי אפשר לעבור על כל המילים מ-1 ועד $2^{|x|}$ (מספר הספרות הבינאריות בהן הוא נתון) ולראות אם הם מחלקים. בנוסף $\mathsf{COMPOSITE} \in \mathsf{NP}$ כי אפשר להגדיר מ"ט א"ד שמכריעה את $\mathsf{COMPOSITE}$ בזמן פולי' ע"י כך שבהינתן x, היא תנחש $p \in \mathbb{N}$ עבורו $1 < p < x - 1$ ותקבל אם"ם p מחלק את x ללא שארית.

פ' המעברים לחלק של הגרלת p תקיים $\delta(q, \_) = \{\langle \text{לכתוב } 0 \rangle, \langle \text{לכתוב } 1 \rangle, \langle \text{לסיים את הכתיבה} \rangle\}$. נשים לב כי אין לנו בדיקה ש-$1 < p < x - 1$ אבל פשוט נדחה אם זה המצב.

חלק ב' של ההרצאה

הערה בעיות ב-NP מתאפיינות ע"י התכונות הבאות (מודגמות על $\mathsf{D-ST-HAMPATH}$ אבל נכונות לכולן):

- קשה להכריע האם יש מסלול המילטוני בגרף.
- קל לבדוק האם מועמד למסלול המילטוני אכן משכנע.

הערה לא ברור (אלא אם יש אפיון מתמטי) שאפשר לשכנע בקלות שאין מסלול המילטוני (או כל בעיה אחרת).

דוגמה לבדוק שמספר הוא פריק זה קל, לבדוק האם הוא ראשוני גם אפשר בזמן פולינומיאלי אבל זו תוצאה מה-20 שנים האחרונות.

דוגמה קריאת x והדפסת $*$ לכל $i = 1$ עד x היא בעלת סיבוכיות לינארית באורך הקלט אם x נתון בבסיס אונארי, ואילו בסיבוכיות אקס' אם x נתון בבסיס $b > 1$. זאת משום שבמקרה כזה אורך הקלט הוא $\log_b x$.

הגדרה <u>מוודא</u> V עבור שפה L הוא מ"ט דטר' כך ש-$L = \{w : (w, c)$ מקבלת את V-קיים c כך ש$\}$.

דוגמה נוכל להגדיר מוודא ל-HAMPATH כך ששפתו $L(V) = \left\{ \left(\underbrace{\langle G, s, t \rangle}_{w}, \frac{\pi}{c} \right) : t \text{ ל- } s \text{ גרף מכוון ו-} \pi \text{ מ-המילטוןמסלול } G \right\}$.

הגדרה שפה L היא <u>NP-שלמה</u> אם $L \in \mathsf{NP}$ ואם $L \in \mathsf{P}$ אז $\mathsf{P} = \mathsf{NP}$, כלומר שניתן להכריעם בזמן פולי' עם מ"ט א"ד, ואם נמצא אלג' בזמן פולי' דטר' להכרעת L נפתור בעיה פתוחה במדמ"ח - $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$.

הערה אם L היא NP-שלמה אפשר להפסיק לחפש אלג' פולי' ל-L כי חיפוש אלג' כזה פותר בעיה פתוחה ולא סביר שסתם נפתור עכשיו את $\mathsf{P} = \mathsf{NP}$.

הגדרה משתנה בוליאני הוא משתנה שמקבל ערכים מ-$\{T, F\}$.

נוסחה בולינאית היא משתנה בוליאני, או $\neg\varphi_1, \varphi_1 \wedge \varphi_2, \varphi_1 \vee \varphi_2$ כאשר φ_1, φ_2 נוסחאות בוליאניות.

בהינתן השמה $f : X \to \{T, F\}$ למשתני הנוסחה, ניתן לחשב את ערך האמת של הנוסחה (באינדוקציה).

נוסחה θ היא ב-CNF אם θ מהצורה $\left(\ell_1^1 \vee \ldots \vee \ell_1^{k_1}\right) \wedge \ldots \left(\ell_m^1 \vee \ldots \vee \ell_m^{k_m}\right)$ כאשר $\ell_i^j \in \{x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}\}$.

דוגמה שפת הנוסחאות הספיקות היא NP-שלמה. $\text{SAT} = \{\langle\phi\rangle : \text{CNF נוסחהפ ספיקה } \phi\}$. משפט קוק-לוין הוכיח ש-$\text{SAT} \in \text{P}$ אם"ם $\text{P} = \text{NP}$.

טענה $\text{SAT} \in \text{NP}$.

הוכחה: מ"ט א"ד עבור SAT פשוט תנחש השמה f עבור המשתנים ומשערכת את הנוסחה לפי f ואם השתערכה ל-T, מקבלת. בדומה, ניתן לוודא מועמד להשמה בזמן פולי' ולכן מהאפיון השקול עם מוודאים, SAT גם כן ב-NP עם המוודא ששפתו

$$L(V) = \{\langle\theta, f\rangle : \theta \text{ נוסחה ב-CNF ו-} f \text{ השמה מספקת עבור } \theta\}$$

■

תרגול

תרגיל $L = \{\langle M_1, M_2\rangle : \text{הן 10-מסכימות } L(M_1), L(M_2)\}$ כאשר L_1, L_2 שפות 10-מסכימות אם קיימות לפחות 10 מילים ב-Σ^*-$\{w_i\}_{i=1}^{10}$ כך ש-$w_i \in L_2 \iff w_i \in L_1$ לכל $i \in [10]$. נוכיח כי $L \notin \overline{\text{RE} \cup \text{co-RE}}$.

1. נראה ש-$L \notin \text{co-RE}$ ע"י רדוקציה $\text{HALT}_{TM}^{\epsilon} \leq L$.

נגדיר f באופן הבא: בהינתן M, נחזיר שתי מ"ט M_1, M_2 כך ש-M_1 מסמלצת את M על ϵ ועונה כמוה (אם היא עוצרת), ו-M_2 מקבלת כל קלט. ברור ש-f חשיבה, נראה נכונות.

אם $M \in \text{HALT}_{TM}^{\epsilon}$ אז M_1 תקבל כל קלט וגם M_2 ולכן ברור שהן 10-מסכימות כלומר $\langle M_1, M_2\rangle \in L$.

אם $M \notin \text{HALT}_{TM}^{\epsilon}$ אז M_1 לא תקבל אף קלט ו-M_2 תקבל כל קלט ולכן הן לא מסכימות על שום דבר כלומר $\langle M_1, M_2\rangle \notin L$.

2. נראה ש-$L \notin \text{RE}$ ע"י רדוקציה $\overline{\text{HALT}_{TM}^{\epsilon}} \leq L$.

נגדיר f באופן הבא: בהינתן M, נחזיר שתי מ"ט M_1, M_2 כך ש-M_1 מסמלצת את M על ϵ ועונה כמוה (אם היא עוצרת), ו-M_2 דוחה כל קלט (אותה בנייה רק ש-M_2 הפוכה). ברור ש-f חשיבה, נראה נכונות (הוכחה משלימה לנ"ל).

אם $M \in \overline{\text{HALT}_{TM}^{\epsilon}}$ אז M_1 לא תקבל אף קלט ו-M_2 גם לא תקבל אף קלט ולכן הן מסכימות על הכל ולכן $\langle M_1, M_2\rangle \in L$.

אם $M \notin \overline{\text{HALT}_{TM}^{\epsilon}}$ אז M_1 תקבל כל קלט ו-M_2 לא תקבל אף קלט כלומר $\langle M_1, M_2\rangle \notin L$.

הגדרה תכונה סמנטית של מ"ט היא קבוצה P של מ"ט, כך שלכל זוג מ"ט M_1, M_2, אם $L(M_1) = L(M_2)$ אז $M_2 \in P \iff M_1 \in P$.

משפט (רייס) נגדיר $L_P = \{\langle M\rangle : M \in P\}$ עבור P תכונה סמנטית לא טריוויאלית, אזי $L_{\text{P}} \notin \text{R}$.

דוגמה $L = \left\{\langle M\rangle : \forall w \in \Sigma^*, w \in L(M) \iff ww^Rww^R \in L(M)\right\}$. כאן התכונה הסמנטית P מכילה את כל המ"ט שעונות אותו הדבר על w ו-ww^Rww^R, ואז $L_P = L$ (L מכילה קידודים).

טענה תהי P תכונה סמנטית לא טריוויאלית של מ"ט כך ש-$T_\varnothing \notin P$ (המכונה עם השפה הריקה), אזי $A_{TM} \le L_P$ (כלומר $L_P \notin \text{co-RE}$).

הוכחה: מהיות P לא טריוויאלית, קיימת $\langle H\rangle \in P$ (כך ש-$L(H) \neq \varnothing$ כי $T_\varnothing \notin P$). נרצה f כך ש-$\langle M,w\rangle \in A_{TM}$ אם"ם $f(\langle M,w\rangle) = \langle T\rangle \in L_P$ כלומר $T \in P$.

נגדיר f באופן הבא: בהינתן $\langle M,w\rangle$, תחזיר $\langle T\rangle$ מ"ט שפועלת כך - בהינתן x:

1. T תסמלץ את ריצת M על w. אם M דחה, T דוחה את x. אחרת אם מקבלת. נעבור לשלב הבא.
2. T תסמלץ את ריצת H על x ותענה כמוה.

f חשיבה כי קל להניח מילה על הסרט ולסמלץ מ"ט אחרת שנתון הקידוד שלה מראש, נראה נכונות.

אם $\langle M,w\rangle \in A_{TM}$ אז $L(T) = L(H)$ כי תמיד נעבור לשלב השני. P תכונה סמנטית ו-$H \in P$ ולכן מההגדרה $T \in P$ כלומר $\langle T\rangle \in L_P$.

אם $\langle M,w\rangle \notin A_{TM}$ אז $L(T) = \varnothing$ כי נדחה תמיד בשלב הראשון אבל $L(H) \neq \varnothing$ ולכן $L(H) \neq L(T)$ כלומר מההגדרה $T \notin P$. ■

הוכחה: (משפט רייס) אם $T_\varnothing \notin P$ אז מהלמה $L_P \notin \text{co-RE}$ ולכן $L_P \notin \text{R}$. אם $T_\varnothing \in P$ אז $T_\varnothing \notin \overline{L_P}$ ולכן $\overline{L_P} \notin \text{co-RE}$ ולכן $L_P \notin \text{R}$. ■

דוגמה ניתן להשתמש במשפט רייס (בלמה בתוכו) כדי להוכיח ששפות לא ב-R (לא בדוגמה הנ"ל כי היא הכילה זוגות של מ"ט ואנחנו יכולים להסתכל על שפה של קידודים של מ"ט יחידה).

נסתכל על $\overline{\text{RE} \cup \text{co-RE}} \in \{\langle M\rangle : L(M) = \Sigma^*\} = \mathsf{ALL}_{TM}$. $P = \{\Sigma^*$ כל מ"ט שהשפה שלהן היא$\}$ היא תכונה סמנטית (מתייחס לשפות בלבד) וגם $T_\varnothing \notin P$. מתקיים $L_P = \mathsf{ALL}_{TM}$ ולכן $A_{TM} \le \mathsf{ALL}_{\mathsf{TM}}$ כלומר $\mathsf{ALL}_{TM} \notin \text{co-RE}$.

דוגמה $\{w$ מספר בייצוג בינארי שאינו ראשוני $: w\} = \mathsf{COMPOSITE}$. נוכיח כי $\mathsf{COMPOSITE} \in \mathsf{NP}$: נבנה NTM שמכריעה את השפה - T תנחש גורם בין 1 ל-w a ותבדוק בכל ענף בנפרד אם a מחלק את w. כל בדיקה נעשית בזמן פולינומיאלי.

דרך אחרת להסתכל על השפה (או המ"ט), היא שזה אוסף המספרים שאפשר לבדוק בזמן פולינומיאלי האם הם בשפה באמצעות גורם שייתנו לנו.

הגדרה תהי V מ"ט דטר'. נאמר כי V מוודא לשפה L אם

$$L = \{w : (\exists c : \langle w,c\rangle \in L(V))\}$$

ונאמר ש-V מוודא פולי' אם

$$L = \{w : (\exists c : |w| \text{ בגודל פולינומי ב- } |c| \text{ וגם } \langle w,c\rangle \in L(V))\}$$

ו-V רצה בזמן פולי' ב-w על $\langle w,c\rangle$.

משפט (שקילות הגדרת NP) $L \in \mathsf{NP}$ אם"ם קיים לה מוודא פולי'.

הוכחה: $\Leftarrow$: אם קיים ל-L מוודא פולי' V אז מהיות V פולי', קיים $k \in \mathbb{N}$ כך שלכל w ולכל c, V רץ על $\langle w, c\rangle$ בזמן פולי' ב-$|w|$.

מ"ט א"ד N שמכריעה את L תפעל כך: עבור קלט w, תנחש c בגודל פולי' ב-$|w|$ ותסמלץ את V על הניחוש.

V רצה בזמן פולי' ולכן כל ענף בענף הריצות של N על w הוא באורך פולי'.

$\Rightarrow$: יש מ"ט א"ד N שמכריעה את L. נבנה מוודא V פולינומי ל-L: V יקבל $\langle w, c\rangle$ כאשר c הוא תיאור של ענף בעץ הריצה של N על w. V יבדוק ש-c היא אכן ריצה חוקית לפי פ' המעברים של N והאם היא מסתיימת במצב מקבל/דוחה, ותקבל/תדחה בהתאם.

מהיות N מ"ט א"ד שמכריעה את L בזמן פולי', ענף הריצה c הוא באורך פולי' ($\leq |w|^k$ עבור איזשהו k) ולכן V רץ בזמן פולי' על $\langle w, c\rangle$ (ולכן פולי' ב-$|w|$). $\blacksquare$

שבוע $\mathbb{X}$ | שלמות ב-NP

הרצאה

חלק א' של ההרצאה

רדוקציות פולינומיאליות

הגדרה $f : \Sigma^* \to \Sigma^*$ היא פ' ניתנת לחישוב בזמן פולי' אם קיימת מ"ט M_f שעל קלט x, עוצרת תוך מספר פולי' ב-x של צעדים עם $f(x)$ על הסרט.

הגדרה יהיו $A, B \subseteq \Sigma^*$. נאמר כי A ניתנת לרדוקציה פולי' ל-B ונסמן $A \leq_p B$ אם קיימת $f : \Sigma^* \to \Sigma^*$ ניתנת לחישוב בזמן פולי' כך שלכל $w \in \Sigma^*$, $w \in A \iff f(w) \in B$.

משפט (הרדוקציה עבור P) אם $A \leq_p B$ ו-$B \in \mathsf{P}$ אז $A \in \mathsf{P}$.

הוכחה: בהינתן M_f שמחשבת את הרדוקציה ו-M_B שמכריעה את B בזמן פולי', נבנה M_A שמכריעה את A בזמן פולי': בהינתן $w \in \Sigma^*$, המכונה M_A תריץ את M_f, תחשב (בזמן פולי') את $f(w)$, תריץ את M_B על $f(x)$ (בזמן פולי' ב-$|f(w)|$).

$|f(w)|$ פולי' ב-$|w|$ ולכן זמן הריצה של M_A פולי' ו-M_A נכונה לכן $A \in \mathsf{P}$. $\blacksquare$

מסקנה אם $A \leq_p B$ ו-$A \notin \mathsf{P}$ אז $B \notin P$ (קונטרה-פוזיטיב על משפט הרדוקציה).

הגדרה נאמר ששפה $L \subseteq \Sigma^*$ היא NP-שלמה אם:

1. (חסם עליון) $L \in \mathsf{NP}$.
2. (חסם תחתון) L היא NP-קשה, כלומר שלכל שפה $L' \in \mathsf{NP}$, $L' \leq_p L$.

הערה אינטואיטיבית, החסם התחתון אומר שכל דבר רע שאפשר להגיד (פולי') על כל שפה ב-NP, אפשר להגיד גם על L.

הערה נאמר שבעיה היא פתורה אם החסם התחתון והעליון שלנו הם שווים, לאמור שלמה במחלקה כלשהי (ולא שהיא P-קשה ושייכת ל-EXPTIME לדוגמה, שזה לא מכריע לנו את סיבוכיות הבעיה).

טענה אם L היא NP-קשה ו-$L \in \mathsf{P}$ אזי $\mathsf{P} = \mathsf{NP}$.

הוכחה: תהי $L' \in \mathsf{NP}$. מהיות L NP-קשה, הרי ש-$L' \leq_p L$ ולכן אם $L \in \mathsf{P}$ גם $L' \in P$. ■

טענה תהי L'' שפה NP-קשה, ו-$L \subseteq \Sigma^*$. אם $L'' \leq_p L$ אז L היא NP-קשה (מטרנזיטיביות של רדוקציות).

הערה זו הגדרה שקולה הרבה יותר נוחה להוכחת קושי ב-NP.

טענה אם $A \in \mathsf{P}$ אז $A \leq_p B$ לכל $B \neq \varnothing, \Sigma^*$.

הוכחה: נגדיר M_f שתפעל כך: בהינתן w, תבדוק (בזמן P) האם $w \in A$. יהיו $w_Y \in B, w_N \notin B$. אם $w \in A$ אז M_f מחזירה w_Y אחרת w_N. זו פ' ניתנת לחישוב ונכונה ולכן $A \leq_p B$ ■

דוגמאות

1. $\{\theta$נוסחה ספיקה ב-3CNF$: \langle\theta\rangle\} = \mathsf{3SAT}$ (כאשר נוסחה היא m $\wedge$-ים על פסוקיות עם $\vee$ עם שלושה איברים מ-$\{x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}\}$) היא NP-שלמה.

2. $\{G$ גרף לא מכוון שיש בו קליקה בגודל $k : \langle G, k\rangle\} = \mathsf{CLIQUE}$. כאשר $S \subseteq V$ הוא k-קליקה ב-$G = \langle V, E\rangle$ אם $|S| = k$ ו-$E(v_1, v_2)$ לכל $v_1, v_2 \in S$. $\mathsf{CLIQUE} \in \mathsf{NP}$ כי אפשר לנחש את הקבוצה ולעשות לה ולידציה בזמן פולי' (יש $|V|^2$ צלעות לכל היותר לבדוק).

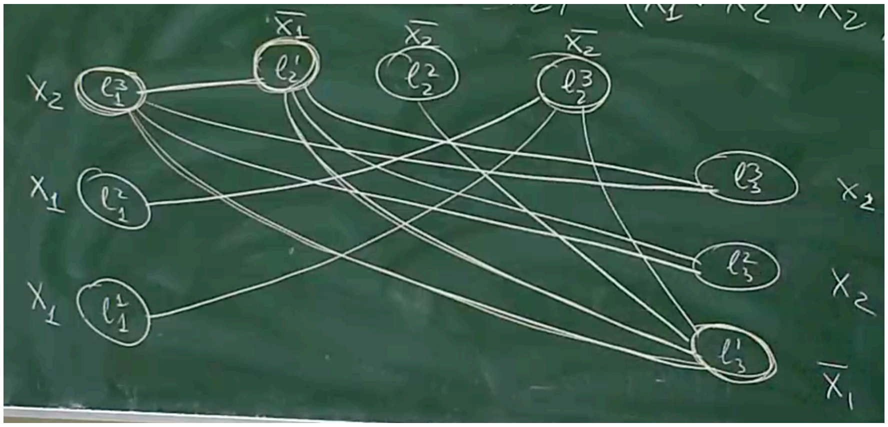
טענה $\mathsf{3SAT} \leq_p \mathsf{CLIQUE}$.

הוכחה: נסמן $\theta = c_1 \wedge \ldots \wedge c_m$, $c_i = \ell_i^1 \vee \ell_i^2 \vee \ell_i^3$ כאשר $\ell_i^j \in \{x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}\}$. נגדיר f באופן הבא: בהינתן θ, נחזיר $G = \langle V, E\rangle$ ו-$k = m$ כאשר: $V = \left\{\ell_1^1, \ell_1^2, \ell_1^3, \ell_2^1, \ldots, \ell_m^1, \ell_m^2, \ell_m^3\right\}$ (ולכן $|V| = 3m$).

את E נגדיר כך ש-3-קליקה תשרה השמה מספקת של θ, מילולית מדובר בכל זוג קודקודים שאינם מאותה הפסוקית או משתנה והשלילה שלו, מתמטית,

$$E = V \times V \backslash \left(\{(v_1, v_2) : \text{מזוהים עם ליטרלים של אותה הפסוקית } v_1, v_2\} \cup \{(v_1, v_2) : \text{מזוהים עם משתנה ושלילתו } v_1, v_2\}\right)$$

דוגמה $\theta = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$. זו נוסחה ספיקה עבור $x_1 = F, x_2 = T$. הגרף שמושרה מ-θ הוא כבאיור



איור 39 : גרף המושרה מהנוסחה θ

נשים לב שעתה $\ell_2^1, \ell_3^1, \ell_1^3$ היא m-קליקה ב-G. הדוגמה כאן היא מקרה פרטי שבו $m = 3$, אבל נשים לב שזה עובר הכללה (אז יהיו לנו יותר צדדים של שלשות בגרף).

הרדוקציה פולינומיאלית כי יש $3m$ קודקודים, ועוברים על $(3m)^2$ קשתות אפשריות בהגדרה של E. נוכיח נכונות.

נניח ש-$\theta \in 3\mathsf{SAT}$, אז קיימת $g : X \to \{T, F\}$ כך ש-g מספקת את θ. בכל פסוקית c_i יש לפחות ליטרל אחד $\ell_i^{j_i}$ ש-g מספקת. נטען ש-$S = \left\{\ell_1^{j_1}, \ldots, \ell_m^{j_m}\right\} \subseteq V$ היא m-קליקה (כלומר שיש קשת בין כל שני ליטרלים מסופקים בפסוקיות השונות).

לכל $u_1, u_2 \in S$ מתקיים $E(u_1, u_2)$ כי הם מזוהים עם ליטרלים מפסוקיות שונות (מהגדרת $\ell_i^{j_i}$) שלא מזוהים עם משתנה ושלילתו, כי g היא השמה ולכל $i \in [n]$ או שרק ליטרלים עם x_i מופיעים ב-S או רק כאלה עם $\overline{x_i}$ (אחרת היו לנו $T, \overline{T}$ מסופקים שניהם וזה לא אפשרי).

נניח שיש ב-G m-קליק S. בהכרח לכל פסוקית c_i יש ב-S רק נציג אחד ℓ_i^1, ℓ_i^2 או ℓ_i^3 (קודקודים מזוהים עם ליטרלים מאותה הפסוקית לא מחוברים בקשת). מהיות $|S| = m$, לכל פסוקית בדיוק נציג אחד. הקליק משרה השמה שכן לכל משתנה לא ייתכן שיש לנו מופע חיובי וגם מופע שלילי (אין קשת בין ליטרלים שמזוהים לא כולם עם x_i או כולם עם $\overline{x_i}$). המשתנים שלא מופיעים בקליק אפשר להשים T/F באופן שרירותי כי יש לנו השמה מספקת באופן ב"ת בהם (יש לנו ליטרל אחד חיובי בכל פסוקית, סה"כ כל הפסקויות מסופקות).

לכן $\langle G, k\rangle \in \mathsf{CLIQUE} \iff \theta \in 3\mathsf{SAT}$ כלומר $3\mathsf{SAT} \leq_p \mathsf{CLIQUE}$. ■

חלק ב' של ההרצאה

משפט $3\mathsf{SAT}$ היא NP-קשה, כלומר $L \leq_p 3\mathsf{SAT}$ לכל $L \in \mathsf{NP}$.

הוכחה: תהי L שפה ב-NP, לכן קיימת מ"ט א"ד M ופולי' $t : \mathbb{N} \to \mathbb{N}$ כך ש-M מכריעה את L, ולכל מילה w, כל הריצות של M על w עוצרות תוך $t(|w|)$ צעדים.

בהינתן w, נייצר נוסחה φ ב-CNF כך ש-$w \in L$ אם"ם φ ספיקה. הרעיון הוא ש-φ תגיד האם יש ריצה מקבלת של M על w. כלומר שיש סדרה $c_0, \ldots, c_m$ של קונפ' כך ש-c_0 הקונפ' ההתחלתית של M על w, לכל $0 \leq i \leq m-1$ c_{I+1} עוקבת ל-c_i ו-c_m קונפ' מקבלת.

נשים לב שלכל $m \leq t\left(|w|\right)$ לכל i, התאים מעבר לתא $t\left(|w|\right)+1$ הם כולם _ כי הראש לא מגיע אליהם. לכן ניתן לייצג ריצה של M על w ע"י מטריצה שבכל קומה תהיה קונפ' (בדומה לריצוף), ושבכל כתובת יש לה אות מ-$S=\Gamma\cup Q\cup\{\#\}$. נתאר קונפ' ע"י מילה ב-$\#\Gamma^{*}Q\Gamma^{*}\#$. המטריצה אם כן תהיה בממדים $\left(t\left(n\right)+3\right)\times t\left(n\right)$ כאשר $n=|w|$ (אורך הייצוג של קונפ' עם ריפוד על מספר הקונפ' לכל היותר).

φ תגיד האם אפשר למלא מטריצה $\left(t\left(n\right)+3\right)\times t\left(n\right)$ באותיות מ-S באופן שמתאר ריצה מקבלת חוקית.

המשתנים שלנו יהיו $x_{i,j,s}$ כאשר $i\in\left[t\left(n\right)+3\right],j\in\left[t\left(n\right)\right],s\in S$, וערכם יהיה T אם"ם $g\left(i,j\right)=S$ כאשר g המטריצה. f ההשמה למשתנים תשרה מטריצה g שמקיימת $f\left(x_{ijs}\right)=T\iff g\left(i,j\right)=s$ (משרה הכוונה שכך נגדיר את g, לאחר שנראה שהיא מגדירה היטב מטריצה).

נגדיר $\varphi=\varphi_{cell}\wedge\varphi_{init}\wedge\varphi_{acc}\wedge\varphi_{move}$ (כך שאם φ סופקה, f משרה מטריצה g מוגדרת היטב, שמגדירה ריצה מקבלת של M על w) כאשר:

1. φ_{cell} תוודא שההשמה אכן מתארת את המטריצה חוקית, כלומר שבכל תא יש אות אחת ורק אות אחת, ופורמלית

$$\varphi_{cell}=\bigwedge_{i\in[t(n+3)],j\in[t(n)]}\left(\left(\bigvee_{s\in S}x_{ijs}\right)\wedge\left(\bigwedge_{s_{1}\neq s_{2}\in S}\overline{x_{ijs_{1}}}\wedge\overline{x_{ijs_{2}}}\right)\right)$$

או מילולית, יש לפחות אות אחת ב-$g\left(i,j\right)$ (שמושרת מההשמה f), ושאין יותר משתי אותיות מושמות באותו התא.

2. φ_{init} תוודא שהשורה הראשונה במטריצה מקודדת את c_{0}, כלומר שהשורה הראשונה היא $\#q_{0}w_{1}\ldots w_{n}\#$, ופורמלית

$$\varphi_{init}=x_{11\#}\wedge x_{12q_{0}}\bigwedge_{i\in[|w|]}x_{1iw_{i+2}}$$

■

תרגול

הגדרה יהי $G=\langle V,E\rangle$ גרף. נאמר כי $C\subseteq V$ <u>כיסוי קודקודי</u> ב-G אם לכל צלע $e=\{u,v\}\in E$, לפחות אחד הקודקודים של e נמצא ב-C.

הגדרה $\text{VC}=\{\langle G,k\rangle:$ G גרף לא מכוון ויש ב-G כיסוי קודקודי מגודל לכל היותר $k\}$.

הערה באלגו ראינו אלג' 2-מקרב לבעיית הכיסוי הקודקודי.

טענה VC היא NP-שלמה.

הוכחה: נראה ראשית ש-VC ב-NP ע"י מציאת מוודא פולי' לה. V יקבל $\langle G,k\rangle$ ו-c, כאשר c היא תת-קבוצה של קודקודי G. V יספור את $|c|$ ויוודא שאכן $|c|\leq k$ וכן ש-c מוכלת בקודקודי G, אם לא, ידחה. אם שתי הבדיקות עוברת, V יעבור על כל הצלעות ב-G ויוודא שיש לכל צלע לפחות קודקוד אחד ב-c, ויקבל אם"ם זה מתקיים.

V רץ בזמן פולי' כי שתי הבדיקות הראשונות הן בזמן פולי' ב-c (שהוא פולי' לכל היותר ב-k כי אחרת נדחה, כאשר k פולי' ב-$|G|$ אם הוא תקין), והבדיקה השלישית לוקחת $\mathcal{O}\left(|E|\cdot|V|\right)$. בנוסף V מוודא נכון (ברור). לכן VC $\in$ NP.

נראה ש-VC היא NPH (NP-קשה) ע"י הרדוקציה CLIQUE $\leq_p$ VC. כלומר נחפש f פולי' כך ש-CLIQUE $\ni \langle G,k\rangle$ אם"ם יש ב-G' k'-קליקה.

טענת עזר יש ב-G k-קליקה אם"ם יש ב-$\overline{G}$ כיסוי קודקודי בגודל $n-k$ כאשר n מספר הקודקודים ב-G ו-$\overline{G}$ הוא G עם הצלעות ההפוכות

- $e\notin E\left(G\right)$ אם"ם $e\in E\left(\overline{G}\right)$.

הוכחה: $\Leftarrow$: נניח שיש ב-G k-קליקה ונסמנה ב-C. נביט ב-$\overline{C}=V\left(G\right)\backslash C$, לכן $\left|\overline{C}\right|=n-k$ ונראה ש-$\overline{C}$ כיסוי קודקודי ב-$\overline{G}$ ונסיים. נניח בשלילה ש-$\overline{C}$, אינו כיסוי קודקודי, ותהי $\{x,y\}\in\overline{E}$ כך ש-$x,y\notin\overline{C}$. כלומר $x,y\in C$ אבל C קליקה ב-G ולכן $\{x,y\}\in E$ כלומר $\{x,y\}\notin E$ סתירה.

$\Rightarrow$: נניח שיש ב-$\overline{G}$ כיסוי קודקודי בגודל $n-k$ ונסמנו ב-$\overline{S}$. נראה ש-S היא k-קליקה ב-G. יהיו $x,y\in S$ ונניח בשלילה ש-$\{x,y\}\notin E$. לכן $\{x,y\}\in\overline{E}$, לכן או ש-$x\notin\overline{S}$ או ש-$y\notin\overline{S}$ ובפרט לא מתקיים $x,y\in\overline{S}$ סתירה להיות $\overline{S}$ כיסוי קודקודי (מצאנו צלע שפיספס). ■

נסיים את הוכחת הטענה. הרדוקציה של f תפעל כך. בהינתן $\langle G,k\rangle$, תחזיר $\left\langle\overline{G},n-k\right\rangle$ כאשר $\overline{G}$ מתקבל מ-G ע"י הפיכת כל הצלעות ו-$n=|V\left(G\right)|$.

f פולינומית כי הפיכת הצלעות לוקחת $\mathcal{O}\left(E\left(G\right)\right)$ וחישוב $n-k$ לוקח $\mathcal{O}\left(V\left(G\right)\right)$ כלומר סה"כ $\mathcal{O}\left(|G|\right)$. הרדוקציה נכונה מהלמה שכן CLIQUE $\ni\langle G,k\rangle$ אם"ם VC $\ni\left\langle\overline{G},n-k\right\rangle$. ■

הגדרה יהי $G=\langle V,E\rangle$ גרף. נאמר כי $D\subseteq V$ היא Dominating Set אם לכל $v\in V$ או ש-$v\in D$ או ש-V חלק מצלע שהקצה השני שלה ב-D, כלומר D קבוצה של קודקודים כך שכל קודקוד במרחק לכל היותר 1 מקודקוד כלשהו ב-D.

נגדיר את השפה

$$\mathsf{DS}=\{\langle G,k\rangle : k\geq \text{ בגודל } DS \text{ } G\text{-יש ב}\}$$

טענה DS היא NPC.

הוכחה: נוכיח כי DS $\in$ NP ע"י מציאת מוודא פולי' V שיפעל כך: V יקבל $\langle G,k\rangle$ ו-D. Vיבדוק ש-$D\subseteq V\left(G\right)$ ו-$|D|\leq$. לאחר מכן יעבור על כל קודקוד ב-G ויבדוק לכל קודקוד u האם הוא ב-D, ואם לא יעבור על הצלעות ב-G ש-u חלק מהן ויבדוק אם הקצה השני של הצלע ב-D. אם לו אף צלע כזו, ידחה. אחרת לאחר מעבר מוצלח על כל הקודקודים, יקבל. הסיבוכיות של V היא

$$\mathcal{O}\left(|V\left(G\right)|\left|V\left(G\right)\right|\left|E\left(G\right)\right|\left|V\left(G\right)\right|\right)$$

שזה פולינומי באורך הקלט ו-V נכון.

עתה נראה כי DS היא NPH ע"י כך שנראה רדוקציה DS $\leq_p$ VC. כלומר רוצים g פולינומית כך ש-VC $\in \langle G,k\rangle$ אם"ם DS $\in \langle G',k'\rangle$.

בהינתן $\langle G,k\rangle$, הרדוקציה g תחזיר $\langle G',k'\rangle$ כך ש-G' מתקבל מ-G באופן הבא: לכל צלע $e\in E\left[G\right]$ $\{x,y\}=$, g תוסיף קודקוד חדש v_e ושתי צלעות חדשות $\{y,v_e\}$, $\{x,v_e\}$ (כל צלע הופכת למשולש x,v_e,y). פורמלית

$$V\left(G'\right)=V\left(G\right)\cup\bigcup_{e\in E(G)}v_e$$

$$E\left(G\right)=E\left(G\right)\cup\left\{\left\{x,v_e\right\},\left\{y,v_e\right\}:\left\{x,y\right\}\in E\left(G\right)\right\}$$

לבסוף, g תסיר את מס' הקודקודים המבודדים ב-G f ותחזיר $\langle G',k'\rangle$ כאשר $k'=f+k$.

g רצה בזמן פולי' כי ספירת קודקודים מבודדים לוקח $\mathcal{O}\left(\left|V\left(G\right)\right|\right)$, הוספת קודקודים לכל צלע $\mathcal{O}\left(E\left(G\right)\right)$ והוספת צלעות חדשות גם $\mathcal{O}\left(E\left(G\right)\right)$. נראה נכונות, כלומר ש-VC $\in \langle G,k\rangle$ אם"ם DS $\in \langle G',k'\rangle$.

$\Leftarrow$: נניח שיש ב-G כיסוי קודקודי C בגודל k. נראה שיש ב-G' קבוצה דומיננטית D מגודל לכל היותר $k+f$ (f גודל אוסף הקודקודים המבודדים, F). נביט ב-$D=C\cup F$ ונראה ש-D היא DS ב-G'. מתקיים $|D|\leq|C|+|F|=k'$ (אולי יש חפיפה בין C,F). נוכיח כי D DS ב-G'.

יהי $v\in V\left(G'\right)$.

- אם $v\in F$ אז $v\in D$ (מהגדרת D).
- אם $v\in V\left(G\right)\backslash F$ אז v חלק מצלע מקורית ב-G ולכן הוא במרחק 1 לכל היותר מ-C ולכן גם מ-D.
- אם $v\in V\left(G'\right)\backslash V\left(G\right)$, בהכרח ש-$v$ הוא מהצורה $v=xy$ עבור $\{x,y\}\in E\left(G\right)$. לכן מכך ש-$C$ כיסוי קודקודי ב-G, או ש-x או ש-y ב-C ובפרט ב-D. בנוסף v_{xy} מחובר בצלע גם ל-x וגם ל-y, ולכן במרחק 1 לכל היותר מ-D (אולי אפילו פעמיים!).

$\Rightarrow$: נניח שיש ב-G' קבוצה דומיננטית D' מגודל $k'=k+f$. נגדיר $D=D'\backslash F$ ונוכיח כי D הוא כיסוי קודקודי בגודל $\leq k$ ב-G'.$D\subseteq F$ (אין קשת שתקרב את הקודקודים המבודדים ל-D אם הם לא כבר שם) ולכן $|D|=|D'|-|F|\leq k'-f=k$.

נוכיח כי בה"כ $D\subseteq V\left(G\right)$. נניח שקיים קודקוד ב-$D$ שאינו ב-G. הקודקודים היחידים שאינם ב-G הם מהצורה v_e. לכן אם $v_{xy}\in D$ אז הוא נוגע רק ב-x וב-y ולכן אם נחליף את v_{xy} ב-x או y נוכל רק להגדיל את מספר הצלעות בהן D נוגעת.

נסיים בכך שנוכיח ש-D כיסוי קודקודי ב-G. תהי $\{x,y\}\in E\left(G\right)$. מהיות D' קבוצה דומיננטית ב-G', כל קודקוד ב-G' הוא במרחק לכל היותר 1 מ-D' ומהיות $D\subseteq V\left(G\right)$, D כיסוי קודקודי ב-G, כי D כולל קודקוד מכל צלע ב-G מהיותו נגזרת של קבוצה דומיננטית (של גרף שמכיל את G), להוציא מקודקודים מבודדים שרלוונטיים רק להגדרת קבוצה הדומיננטית ולא להגדרת הכיסוי הקודקודי. ■