מבוא

<u>מה לומדים?</u> מה מחשבים מסוגלים לפתור ובאיזה מחיר (זמן, שטח, אקראיות).

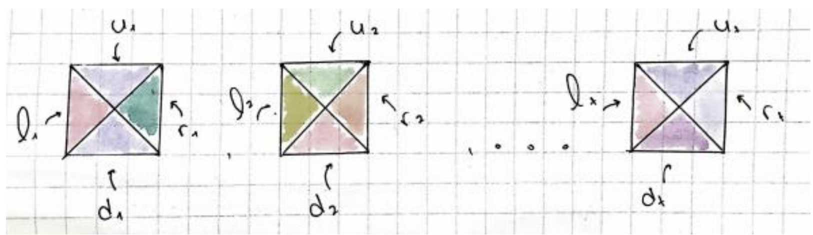
הקורס מחולק לשלושה נושאים:

1. **מודלים חישוביים** (אוטומטים).
2. **חישוביות** – מה המחשב מסוגל לפתור ומה לא, מה ניתן לחשב.
3. **סיבוכיות –** מה המחיר של פתרון הבעיות.

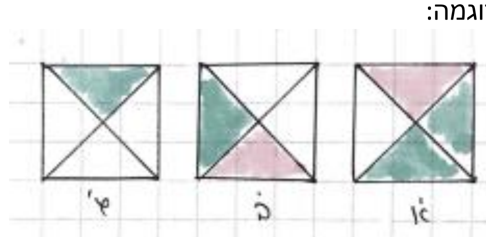
חישוביות

<u>דוגמה 1: בעיית הריצוף.</u>

קלט מס' סופי של אריחים, כל אריח מסומן בארבעה צבעים באופן הבא:



פלט האם ניתן לרצף ריבוע $n \times n$ באופן חוקי לכל $n \geq 1$.
דוגמה:



בקלט זה יש פתרון לכל n:

א					
ג	א				
ב	ג	א			
א	ב	ג	א		
ג	א	ב	ג	א	

אלגוריתם כללי לפתרון הבעיה מכריע בהינתן T (קב' אריחים) האם קיים ריצוף חוקי $n \times n$ לכל $n \geq 1$.
לא קיים אלגוריתם.

<u>דוגמה 2: בעיית העצירה.</u>

בהינתן P תכנית מחשב ו-X קלט לתוכנית, האלגוריתם מכריע האם קיימת תכנית מחשב שמקבלת את X ,P ומחזירה האם P עוצרת על X.
מימוש נאיבי: הרצת P עם X, אם P עוצרת תוך 20 דק' נחזיר כן, אחרת נחזיר לא.
לא קיים אלגוריתם.

סיבוכיות

<u>דוגמה 1: מעגל אוילר בגרף.</u>

מעגל אוילר הוא מעגל העובר בכל קשתות הגרף ובכל קשת בדיוק פעם אחת.
נרצה לפתח אלגוריתם כאשר בהינתן גרף מכריע אם קיים בו מעגל אוילר.
לבעיה קיים אפיון מתמטי ולכן יש אלגוריתם פולינומיאלי.

<u>דוגמה 2: מעגל המילטון בגרף.</u>

מעגל המילטון הוא מעגל אשר עובר בכל קדקודי הגרף ובכל קדקוד בדיוק פעם אחת.
עדיין אין אפיון מתמטי לבעיה, ולכן לא ידוע אם קיים אלגוריתם פולינומיאלי.

באופן כללי, בהינתן בעיה, נסווג אותה לפי:

1. לא כריעה.
2. כן כריעה, ואז סיווג לפי סיבוכיות.

מודלים חישוביים

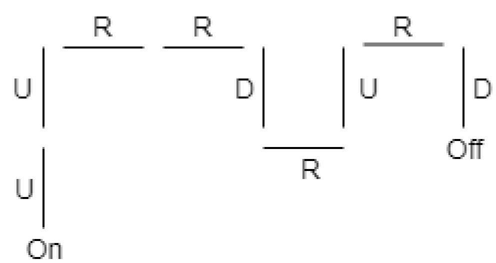
אוטומטים

מהו מודל החישוב?

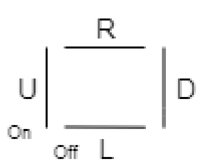
<u>דוגמה:</u> יש עט דיגיטלי וניתן לתת לעט 6 פקודות – {On, Off, Up, Down, Right, Left}.
סדרת פקודות לעט היא חוקית אם:

1. הסדרה מתחילה ב-On ומסתיימת ב-Off.
2. מציירת קו רקיע משמאל לימין.

סדרה חוקית:



סדרה לא חוקית:



אוטומט שמגדיר סדרות חוקיות: גרף שקדקודיו הם מצבים, ומכל מצב נאמר לאן להתקדם (ע"י חץ שיוצא מהמצב) בקריאת פקודה (אות) שכתובה על המעבר. הגרף מתחיל ממצב התחלתי (חץ נכנס) ובעל קבוצה של מצבים מקבלים. האוטומט מקבל סדרת אותיות ורץ על הקלט. סדרת הפקודות חוקית אם היא מסתיימת במצב מקבל.

הגדרות

א"ב – קבוצה סופית של אותיות המסומנת ע"י $\Sigma = \{\varsigma_1, \varsigma_2, \dots, \varsigma_n\}$.

מילה – סדרה של אותיות. קבוצת כל המילים מעל Σ מסומנת ע"י $\Sigma^* = \{w: \Sigma \text{ מילה מעל } w\}$.

$\mathcal{E}$ – המילה הריקה.

שפה – קב' של מילים $L \subseteq \Sigma^*$.

אוטומט סופי דטרמיניסטי A הינו חמישייה:

$$A = < Q, \Sigma, \delta, q_0, F >$$

Q – קבוצת מצבים
Σ – א"ב
δ – מעברים
q_0 – מצב התחלתי
F – קבוצת מצבים מקבלים

- $q_0 \in Q$
- $F \subseteq Q$
- $\delta: Q \times \Sigma \to Q$

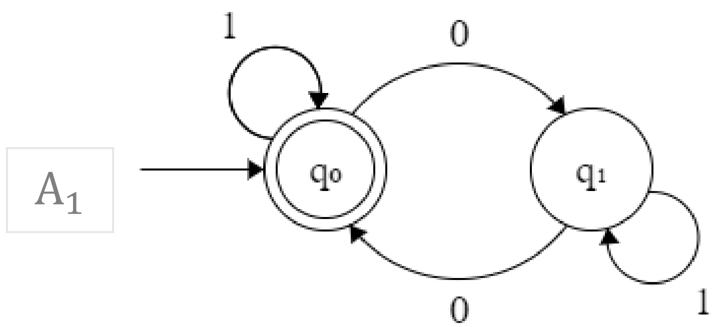
<u>דוגמה 1:</u>

$\Sigma = \{0,1\}$

$Q = \{q_0, q_1\}$

$F = \{q_0\}$

δ	0	1
q_0	q_1	q_0
q_1	q_0	q_1



ריצה של A על מילה w – בהינתן מילה $w = \varsigma_1, \varsigma_2, \dots, \varsigma_n$, $\delta_i \in \Sigma$, $w \in \Sigma^*$, היא סדרה של מצבים $\zeta = q_0, q_1, \dots, q_n$ כך ש-

1. q_0 הוא המצב ההתחלתי של A.
2. לכל $0 \le i < n$ מתקיים $q_{i+1} = \delta(q_i, \varsigma_{i+1})$.

- מהדוגמה, ריצה של A על 0010 תהיה q_0, q_1, q_0, q_0, q_1, וריצה על 11 תהיה q_0, q_0, q_0.

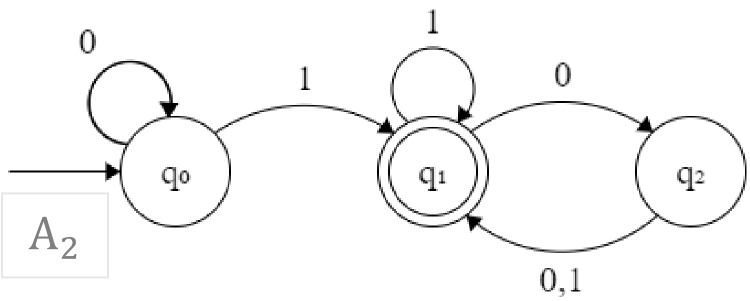
הריצה ζ היא **ריצה מקבלת** אם q_n (המצב האחרון בריצה) מצב מקבל $(q_n \in F)$.

האוטומט A מקבל את המילה w אם הריצה של A על w היא ריצה מקבלת. (יש ריצה אחת של אוטומט על מילה)

השפה של A – $L(A) = \{w: w \text{ מקבל את } A\}$.

- מהדוגמה, $L(A_1) = \{w$: יש ל-w מספר זוגי של 0-ים$\}$. הוכחה נעשית באינדוקציה על אורך המילה.

<u>דוגמה 2:</u>



$$\Sigma = \{0,1\}$$

נבדוק שהאוטומט אכן מוגדר היטב. צ"ל $\delta: Q \times \Sigma \to Q$, ואכן מתקיים.
נרצה להגדיר את השפה של A. נשים לב שכדי שלמילה יהיה סיכוי להתקבל, היא צריכה להכיל 1.
כמו כן, תמיד כשנבקר ב-q_1, אחרי הקריאה ל-1 האחרון, מספר ה-0-ים זוגי. (למשל, אם נקרא אחרי q_1 ל-q_2, ואז בחזרה ל-q_1 דרך 0, קיימים שני אפסים בקריאה. אם דרך 1, אז הוא ה-1 האחרון ומספר האפסים אחריו הוא אפס).

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

<u>דוגמה 3:</u>

נבנה A_3 כך ש-$L(A_3) = \{w$: w מכיל את 001$\}$, $\Sigma = \{0,1\}$.

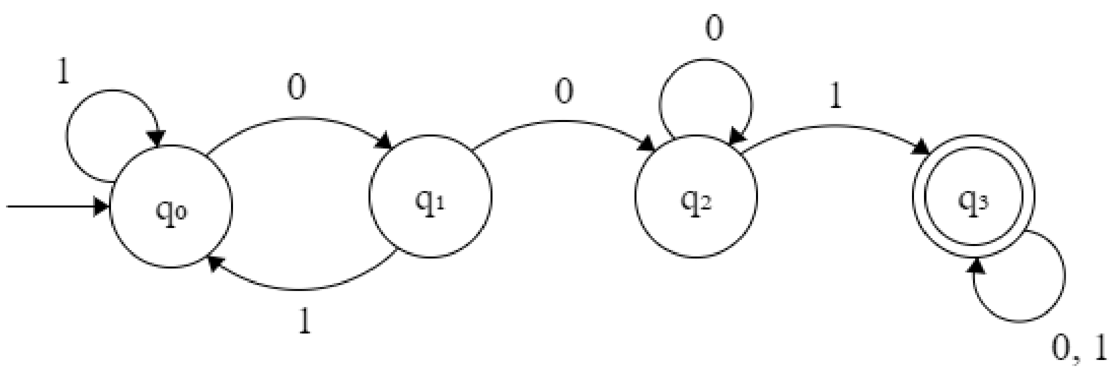
01010010 תתקבל.

00100111001 תתקבל.

1101 לא תתקבל.

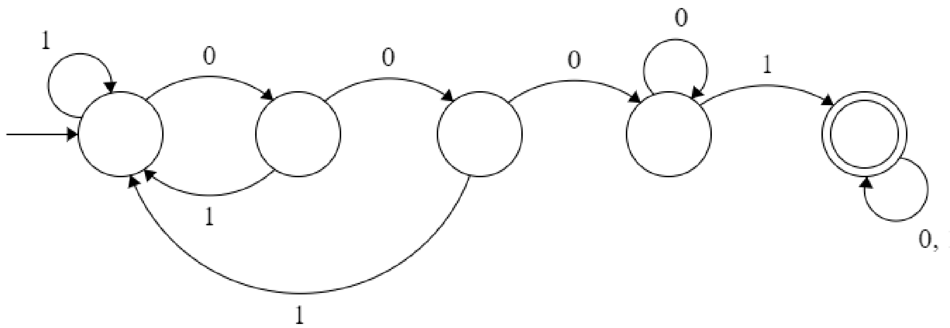
סטטוס:

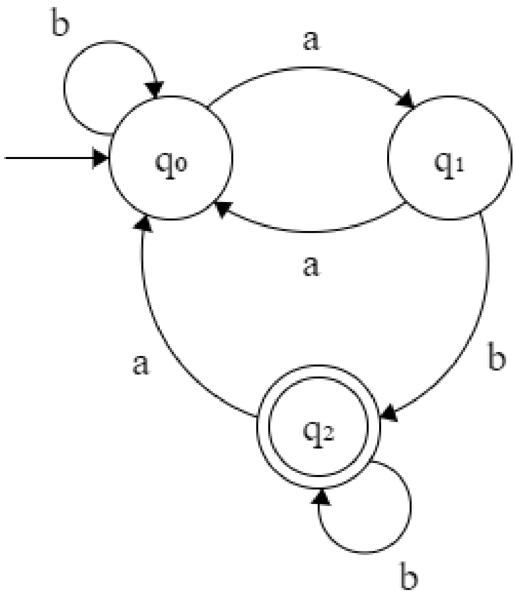
1. q_0: לפני 001. המצב לא מקבל כי המילה הריקה לא בשפה.
2. q_1: ראינו 0, ממתינים ל-01.
3. q_2: ראינו 00, ממתינים ל-1. כשנקרא ל-0 נישאר ב-q_2 כדי לא לשנות את הסטטוס.
4. q_3: ראינו 001, **בור מקבל**. ברגע שראינו לראשונה 001, ההמשך לא משנה.



- ריצה על 0001 תהיה q_0, q_1, q_2, q_2, q_3.

אם נרצה לבנות אוטומט A_4 כך ש-$L(A_4) = \{w:$ מכיל את 0001 $w\}$, הוא יהיה דומה לאוטומט A_3, וייראה כך:





בהינתן האוטומט A, איך נדע מה השפה שלו?

- תזכורת מהתרגול - $\delta^*(q,w)$ מייצגת לאן נגיע בקריאת w מ-q.

נוכיח שלכל מילה $w \in \Sigma^*$ מתקיים:

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

נסיק $\mathrm{L(A)} = \{w:$ מספר ה-a-ים ב-w אי זוגי, ו-w מסתיימת ב-b$\}$

<u>הוכחה באינדוקציה על $|w|$</u>

בסיס: $|w| = 0$ (כלומר $w = \varepsilon$). במקרה זה $\delta^*(q_0,w) = q_0$ וגם $\#_a w = 0$ זוגי.

צעד: נניח שתנאים 1-3 מתקיימים עבור $w \in \Sigma^*$ ונוכיח שמתקיימים עבור המילה $w \cdot a$ והמילה $w \cdot b$.

נראה עבור $w \cdot a$ –

1. $\delta^*(q_0,w \cdot a) = q_0 \Leftrightarrow \delta^*(q_0,w) \in \{q_1,q_2\} \Leftrightarrow$ (מהנחת האינדוקציה ואפיון 2 ו-3) $\#_a w$ אי זוגי $\Leftrightarrow$ $\#_a w \cdot a$ זוגי.
2. $\delta^*(q_0,w \cdot a) = q_1 \Leftrightarrow \delta^*(q_0,w) = q_0 \Leftrightarrow$ (מהנחת האינדוקציה ואפיון 1) $\#_a w$ זוגי $\Leftrightarrow$ $\#_a w \cdot a$ אי זוגי ו-$w \cdot a$ מסתיים ב-a.
3. תנאי 3 מתקיים באופן ריק: $\delta^*(q_0,w \cdot a) = q_2$ לא אפשרי.

פעולות על שפות רגולריות

1. **איחוד** (Union)

$$L_1 \cup L_2 = \{w:\ w \in L_1 \vee w \in L_2\}$$

2. **שרשור** (Concatenation)

$$L_1 \cdot L_2 = \{w_1 \cdot w_2:\ w_1 \in L_1,\ w_2 \in L_2\}$$

כאשר עבור המילים

$$w_1 = \varsigma_1\varsigma_2 \dots \varsigma_n \qquad w_2 = \varsigma'_1\,\varsigma'_2 \dots \varsigma'_n$$

מתקיים

$$w_1 \cdot w_2 = \varsigma_1\varsigma_2 \dots \varsigma_n\varsigma'_1\,\varsigma'_2 \dots \varsigma'_n$$

3. **כוכב** (Star)

$$L^* = \{w_1 \cdot w_2 \cdot \ldots \cdot w_k: \quad k \geq 0, w_i \in L \quad \forall 1 \leq i \leq k\}$$

נשים לב - $\varepsilon \in L^*$ שרשור ריק.

אם $L = \emptyset \ \vee L = \{\varepsilon\}$ אז $L^* = \{\varepsilon\}$.

אם $L \neq \emptyset \ \wedge L \neq \{\varepsilon\}$ אז L^* קבוצה אינסופית.

<u>דוגמה:</u>

$$\Sigma = \{1,2,3,4\} \quad L_1 = \{1, 333\} \quad L_2 = \{22, 4444\}$$

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

$$L_1 \cdot L_2 = \{122, 14444, 33322, 3334444\}$$

$$L_1^* = \{\varepsilon, 1, 11, 13331, 3333331, \ldots.\}$$

פעולות סגור עבור שפות רגולריות

משפט: השפות הרגולריות סגורות לאיחוד סופי.

הוכחה: בהינתן $A_1 = < Q, \Sigma, \delta, q_0, F >$, $A_2 = < Q, \Sigma, \delta, q_0, F >$ (כאשר ניתן להגדיר את Σ כ- $\Sigma = \Sigma_1 \cup \Sigma_2$)

נבנה DFA – A כך ש- $\mathrm{L(A) = L(A_1) \cup L(A_2)}$ (בהוכחה נעשה שימוש בהנחה שיש להם את אותו א"ב).

פעולות סגור עבור שפות רגולריות

משפט: אם L_1 רגולרית ו-L_2 רגולרית אז $L = L_1 \cup L_2$ רגולרית.
(השפות הרגולריות סגורות לאיחוד סופי.)

הוכחה: בהינתן $A_1 = < Q_1, \Sigma, \delta_1, q_1^0, F_1 >$ עבור L_1, $A_2 = < Q_2, \Sigma, \delta_2, q_2^0, F_2 >$ עבור L_2, נבנה DFA – A כך ש-$A =< Q, \Sigma, \delta, Q_0, F >$ עבור $\mathrm{L(A)} = \mathrm{L(A_1)} \cup \mathrm{L(A_2)}$.

נשים לב:

1. L_1, L_2 מוגדרים מעל אותו א"ב (Σ), אחרת היינו לוקחים $\Sigma = \Sigma_1 \cup \Sigma_2$.
2. δ_1, δ_2 שלמות (מוגדרות לכל מצב ואות). ניתן להשלים ע"י מעבר ל**בור דוחה**.
   לכן ניתן להניח ששתי השפות מעל אותו א"ב.

הגדרת A (אוטומט המכפלה) -

הרעיון: לעקוב אחרי שתי הריצות של האוטומטים בו זמנית.

$$\mathrm{Q} = Q_1 \times Q_2 = < q_1, q_2 : q_1 \in Q_1, q_2 \in Q_2 >$$

$$q_0 =< q_1^0, q_2^0 >$$

$$\delta(< q_1, q_2 >, \varsigma) =< \delta_1(q_1, \varsigma), \delta_2(q_2, \varsigma) >$$

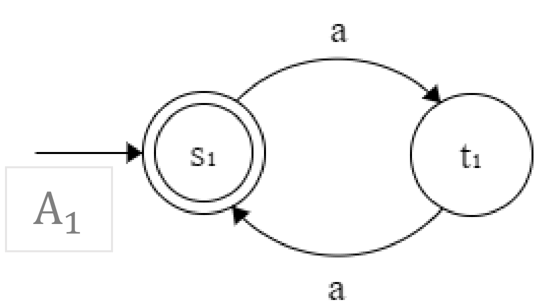
$$F = (F_1 \times Q_2) \cup (Q_1 \times F_2) = \{< q_1, q_2 >:\ q_1 \in F_1 \text{ או } q_2 \in F_2\}$$

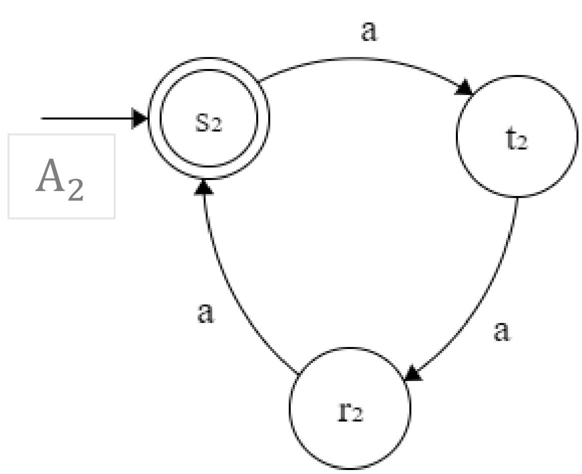
דוגמה:

$$\Sigma = \{a\}$$

$$L_1 = \{w : |w| mod2 = 0\}$$

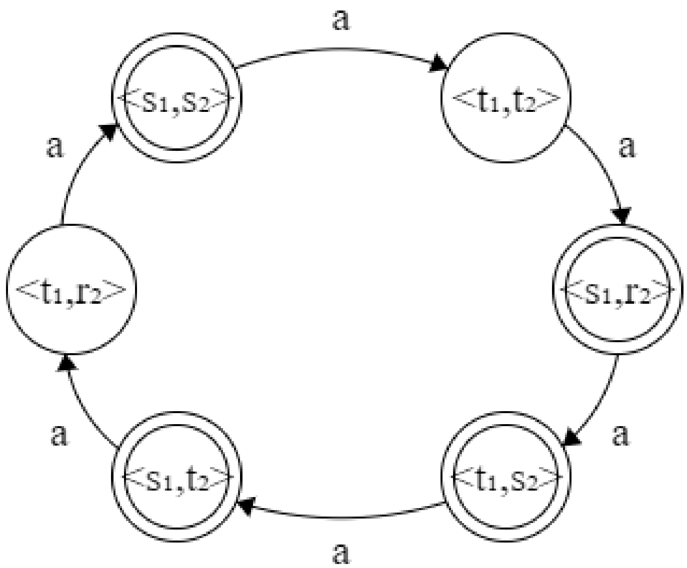
$$L_2 = \{w : |w| mod3 = 0\}$$





אוטומט המכפלה:

$L(A) = \{w: |w| = 0mod2 \ \lor |w| = 0mod3\}$



<u>$L(A) = L(A_1) \cup L(A_2)$ –</u>

שלב א': $L(A) \subseteq L(A_1) \cup L(A_2)$. נראה שלכל $w \in \Sigma^*$, אם הריצה של A על w מקבלת, אז הריצה של A_1 על w מקבלת, או הריצה של A_2 על w מקבלת.

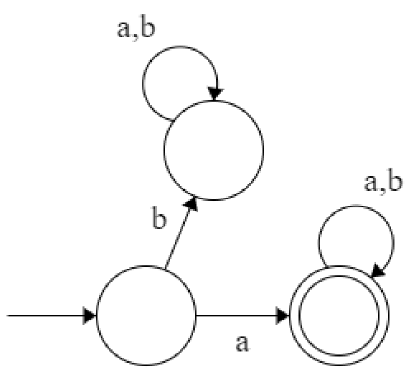
תהי $r = q_0, q_1, \dots, q_n = < q_1^0, q_2^0 >, < q_1^1, q_2^1 >, \dots, < q_1^n, q_2^n >$ הריצה של A על w, $q_i =< q_1^i, q_2^i >$.

מהגדרת A: $r_1 = q_1^0, q_1^1, q_1^2, \dots, q_1^n$ (ההטלה של r על Q_1) הריצה של A_1,

$r_2 = q_2^0, q_2^1, q_2^2, \dots, q_2^n$ הריצה של A_2.

r מקבלת $\Leftrightarrow$ $< q_1^n, q_2^n > \subseteq F$ $\Leftrightarrow$ $q_1^n \in F_1$, $q_2^n \in F_2$ $\Leftrightarrow$ r_1 מקבלת או r_2 מקבלת $\Leftrightarrow$ $w \in L(A_1)$ או $w \in L(A_2)$.

שלב ב': $L(A_1) \cup L(A_2) \subseteq L(A)$. הוכחה דומה.



** בור – לא משנה איזה אות נקרא, תמיד נישאר בו. בור דוחה מבטיח שאף פעם לא נגיע למצב מקבל. בדוגמה בור דוחה באוטומט על כל המילים שמתחילות ב-a.

משפט: השפות הרגולריות סגורות לחיתוך.

הוכחה: בהינתן $\mathrm{DFA}\ A_1$ ו-$\mathrm{DFA}\ A_2$, נבנה A DFA כך ש- $\mathrm{L}(\mathrm{A}) = \mathrm{L}(\mathrm{A}_1) \cap \mathrm{L}(\mathrm{A}_2)$.

אוטומט המכפלה יהיה עם $F = F_1 \times F_2$.

r תהיה ריצה מקבלת אמ"מ r_1 מקבלת וגם r_2 מקבלת.

- נשים לב כי הגודל של אוטומט המכפלה הוא $|Q_1| \cdot |Q_2|$.

מהדוגמה הקודמת,

$$L(A) = \{w: |w| = 0mod6\}, F = \{< s_1, s_2 >\}$$

משפט: השפות הרגולריות סגורות להשלמה.

- פעולת השלמה: $\bar{L} = \Sigma^* - L = \{w: w \notin L\}$

הוכחה: בהינתן A DFA נבנה A' DFA כך ש-$L(A) = L(\bar{A})$.

יהי $A =< Q, \Sigma, \delta, Q_0, F >$, ונגדיר $A' =< Q, \Sigma, \delta, Q_0, F' >$ כך ש- $F' = Q \backslash F$.

לכל מילה w, הריצה של A' על w מגיעה למצב מקבל אמ"מ הריצה של A על w לא הגיעה למצב מקבל.

- אין הגדלה של מס' המצבים.

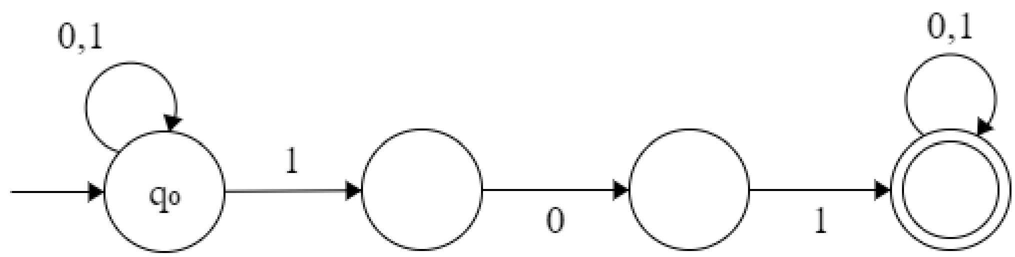
סגור לשרשור: אם L_1 רגולרית ו-L_2 רגולרית, אז גם $L_1 \cdot L_2 = \{w_1 \cdot w_2:\ w_1 \in L_1,\ w_2 \in L_2\}$.

רעיון בניית האוטומט עבור ההוכחה - לקיחת המצבים המקבלים של והמצב ההתחלתי של , ולהקפיץ את הריצה ביניהם.

נוכל לממש את הרעיון אם נוסיף אי-דטרמיניזם.

אוטומטים אי-דטרמיניסטיים (nondeterministic NFA)

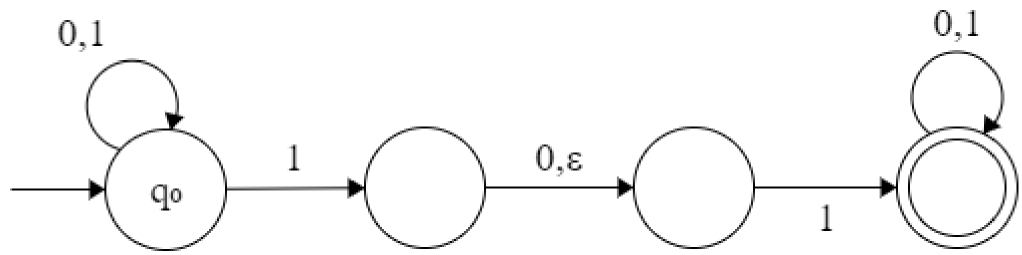
<u>דוגמה:</u>



$L(A) = \{w$ מכיל את הרצף 101 $:w\}$

- לאוטומט עשויות להיות מס' ריצות על מילת הקלט, "מנחש לאן כדאי לו להתקדם".
- לאוטומט מותר לעבור ממצב למצב בלי לקרוא את מילת הקלט (מעברי ε).

מהדוגמה הקודמת,

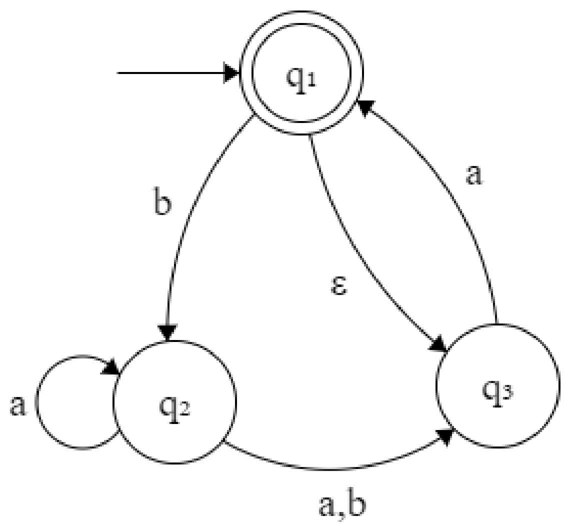


$L(A)=\{w$: מכיל את הרצף 101 או 11 $w\}$

<u>דוגמה:</u>

מקבל: ε, *a*, *baba*, *baaaa*, *bbaa*.

לא מקבל: *b*, *babba*.



הגדרות

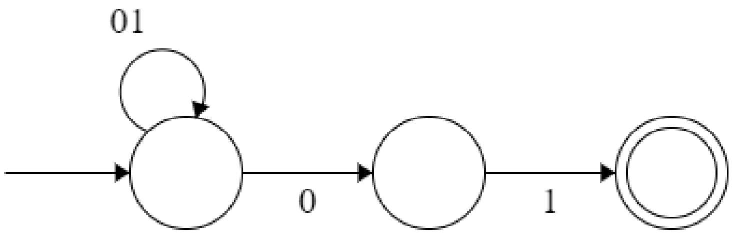
אוטומט סופי אי-דטרמיניסטי $\mathrm{A}=<Q,\Sigma,\delta,Q_0,\mathrm{F}>$ כך ש:

- $Q_0\subseteq Q$ קב' מצבים התחלתיים.
- $\delta: Q\times(\Sigma\cup\{\varepsilon\})\longrightarrow 2^Q$.

ריצה של A על מילה $w=\varsigma_1,\varsigma_2,\dots,\varsigma_n$ היא סדרה של מצבים $r=q_0q_1\dots.q_m$, $n\le m$, כך שניתן לכתוב את w כ- $w=y_1y_2\dots y_m \quad y_i\in\Sigma\cup\{\varepsilon\}$

- $q_0\in Q_0$.
- $\forall 1\le i\le m \quad q_{i+1}\in\delta(q_i,y_{i+1})$

<u>דוגמה:</u>



$0011 \notin L(A)$
$001 \in L(A)$

$L(A) = \{w$: w מסתיימת ב-01$\}$

משפט: לכל NFA יש DFE שקול.

הוכחה: בהינתן NFA A, נבנה DFA A' כך ש-$L(A') = L(A)$. (חרצון/דטרמיניזציה)

נניח של-A אין צעדי ε (הצדקה: כי בתרגול נראה שבהינתן NFA עם צעדי ε, ניתן לבנות בקלות NFA שקול ללא צעדי ε).

הרעיון: A' מגיע אחרי קריאת w למצב $S \in 2^Q \Leftrightarrow$ A יכול להגיע בקריאת w לכל המצבים ב-S.

נבנה A באופן הבא:

$$.Q' = 2^Q$$

$$q_0' = Q_0 \in 2^Q$$

$$\delta'(\delta, \varsigma) = \bigcup_{s \in S} \delta(s, \varsigma) = \{t: t \in \delta(s, \varsigma)\ s \in S \text{ קיים}\}$$

$$F' = \{S: S \cap F \neq \emptyset\}$$

משפט: לכל A NFA יש DFA A' שקול ($L(A) = L(A')$).

הוכחה: יהי $A = < Q, \Sigma, \delta, Q_0, F >$, $\delta: Q \times \Sigma \to 2^Q$ בהנחה שאין צעדי ε.

נבנה $A' = < 2^Q, \Sigma, \delta', Q_0, F' >$ (Q_0 מצב יחיד כי $Q_0 \in 2^Q$).

הרעיון: A' נמצא במצב $S \in 2^Q$ אחרי קריאת w $\Leftrightarrow$ A עשוי להיות במצב ב-S אחרי קריאת w.

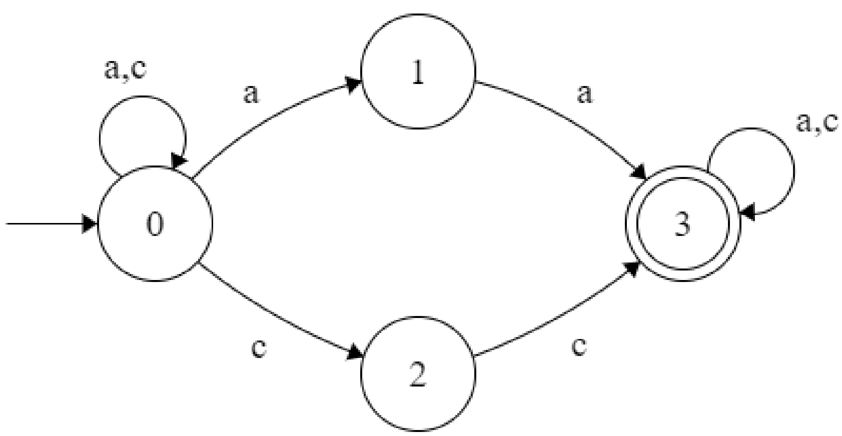
$$\delta'(s, a) = \bigcup_{s \in S} \delta(s, a)$$

$$F' = \{S: S \cap F \neq \emptyset\}$$

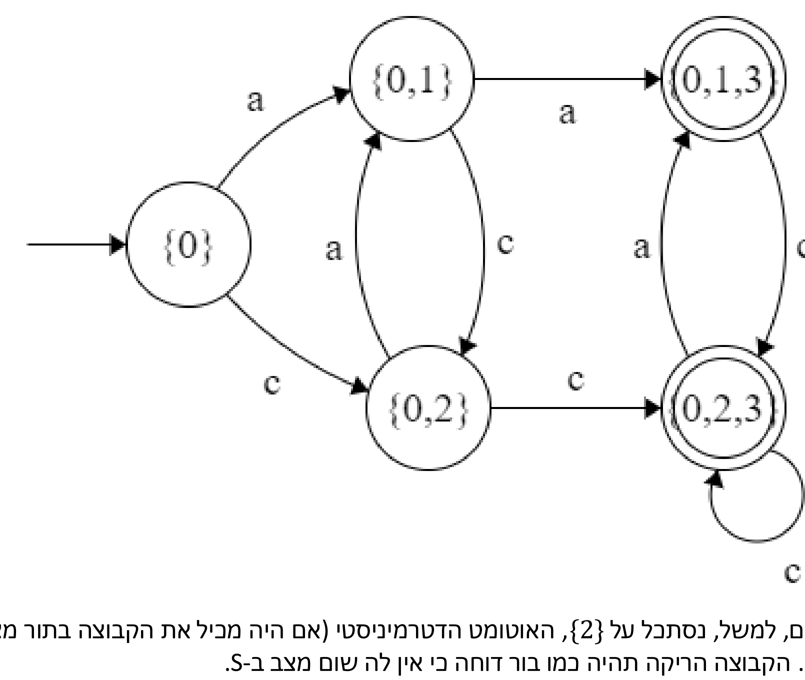
<u>דוגמה:</u>

$$\Sigma = \{a, c\}, L = \{w: \text{מכילה את הרצף } aa \text{ או } cc \; w\}$$

אוטומט לא דטרמיניסטי מנחש האם יהיה הרצף aa או cc ומתי הרצף מתחיל.



בניית DFA מתאים:



** אם, למשל, נסתכל על {2}, האוטומט הדטרמיניסטי (אם היה מכיל את הקבוצה בתור מצב) ייאלץ להתקדם בהינתן a לקבוצה ריקה. הקבוצה הריקה תהיה כמו בור דוחה כי אין לה שום מצב ב-S.

הוכחת הרעיון:

סימון: עבור פונקציית מעברים אי-דטרמיניסטית $\delta: Q \times \Sigma \to 2^Q$, נרחיב את δ ל-

1. קבוצות של מצבים.
2. מילים.

כלומר $\delta: 2^Q \times \Sigma^* \to 2^Q$. אינטואיציה: $\delta(S,w) = S'$ - האוטומט באחד המצבים ב-S, ואחרי קריאת w יגיע לאחד המצבים ב-S'. (הפונקציה לוקחת קבוצה של מצבים ומילה, וממפה אותן לקבוצה של מצבים).

1. $\delta(S,\varepsilon) = S$
2. $\delta(S,a) = \bigcup_{s\in S} \delta(s,a)$
3. $\delta(S, y\cdot a) = \delta(\delta(S,y),a)$

<u>טענה: בבנייה שראינו, $\delta'({Q_0}^{(1)}, w) = \delta({Q_0}^{(2)}, w)$.</u>

(1) Q_0 הוא המצב היחיד שהוא איזשהו $S \in 2^Q$ ש-A' מגיע אליו אחרי קריאת w.
(2) Q_0 היא קבוצת המצבים ש-A עשוי לבקר בהם אחרי קריאת w.

הוכחת הטענה באינדוקציה על $|w|$.

בסיס: $\delta'(Q_0,\varepsilon) = Q_0 = \delta(Q_0,\varepsilon)$ (לכן הגדרנו את המצב ההתחלתי של A' להיות Q_0)

צעד: $\delta'(Q_0, y\cdot a) =^{(1)} \delta'(\delta'(Q_0,y),a) =^{(2)} \bigcup_{s\in\delta'(Q_0,y)} \delta(s,a) =^{(3)} \delta(\delta(Q_0,y),a) =^{(4)} \delta(Q_0, y\cdot a)$

(1) מהרחבת δ' למילים ב-3.
(2) מהגדרת δ' כפונקציית המעברים של האוטומט הדטרמיניסטי- אם נסמן $\delta'(Q_0,y) = S$, ראינו ב-2 את המעבר.
(3) מהגדרת δ' (הנחת האינדוקציה?)
(4) מ-3.

נשים לב –

חדשות טובות 😉 – אי-דטרמיניזם לא מוסיף לכוח ההבעה של אוטומטים.

חדשות רעות ☹ – $|A'| = 2^{|A|}$, כלומר מספר המצבים ב-A' הוא אקספוננציאלי למספר המצבים ב-A. (חסם עליון)

נוכיח חסם תחתון!

נוכיח קיימות שפות שהאוטומט הלא דטרמיניסטי עבורן אקספוננציאלית קטן מהאוטומט הדטרמיניסטי.

חרצון אבן כרוך בפיצוץ אקספוננציאלי.

הוכחה שגויה: נראה שפה L כך שיש ל-L NFA עם 5 מצבים, והאוטומט הדטרמיניסטי הקטן ביותר עבור L צריך לפחות 32 מצבים.

<u>למה לא חסם תחתון?</u>

ההוכחה:

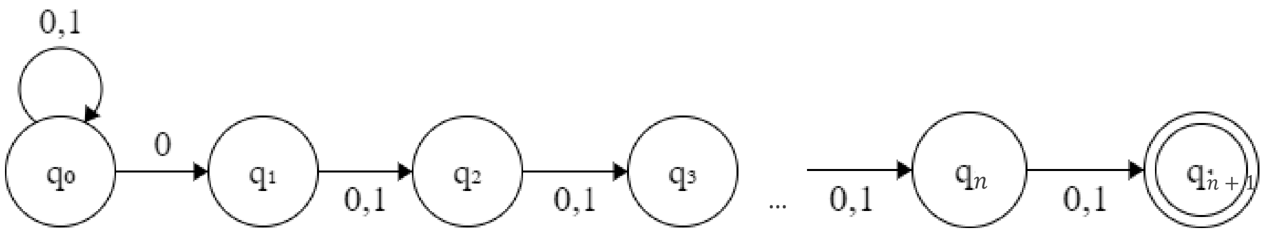
נראה משפחה של שפות $\{L_1, L_2, \dots, L_n\}$ $1 \le n$ כך ש:

1. ל-L_n יש NFA עם $O(n)$ מצבים.
2. כל DFA עבור L_n דורש לפחות 2^n מצבים.

$$\Sigma = \{0,1\},\ \ L_n = \{w: \text{במקום ה-}n+1\text{ מהסוף יש } 0\}$$

נראה אח"כ ש- $L_n = (0+1)^*0(0+1)^n$.

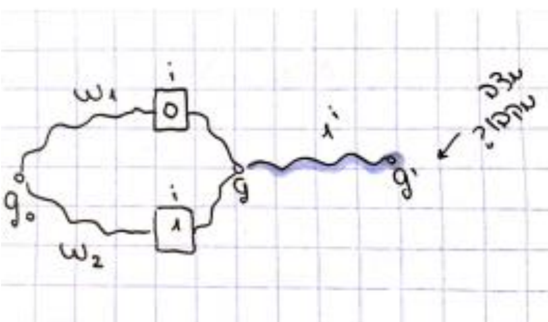
1. NFA עבור L_n בעל $n+2$ מצבים.



2. נניח בשלילה שיש DFA A_n שמזהה את L_n ויש לו פחות מ-2^n מצבים.

מעקרון שובך היונים (כי יש 2^n מילים ופחות מ-2^n מצבים) , יש שתי מילים $w_1, w_2 \in (0+1)^n$ כך ש-A_n בקריאת w_1 ו-w_2 מגיע לאותו המצב:

$$\mathrm{A}_n = < Q, \{0,1\}, \delta, Q_0, F > \qquad \delta(q_0, w_1) = \delta(q_0, w_2) \quad w_1 \neq w_2$$



יהי i אינדקס כך ש- $w_1[i] \neq w_2[i]$, $i \in \{1, \dots, n\}$. נניח בה"כ:

$$w_1[i] = 0, w_2[i] = 1$$

נתבונן במילים עם שרשור 1^i. לדוגמה,

$$w_1 = 00010 \cdot 111$$

$$w_2 = 00100 \cdot 111$$

במצב זה $i = 3, n = 5$.

אבל לפי האוטומט:

$$\begin{cases} \delta(q_0, w_1 \cdot 1^i) = q' \\ \delta(q_0, w_2 \cdot 1^i) = q' \end{cases} \text{A מקבל את } w_1 \cdot 1^i \ \Leftrightarrow\ \text{A מקבל את } w_2 \cdot 1^i \ \Leftrightarrow\ q' \in F.$$

אבל$w_1 \cdot 1^i \in L_n$, $w_2 \cdot 1^i \notin L_n$, כלומר A טעה.

<u>מסקנה: אין בניית חרצון פולינומיאלית.</u>

עבור NFA עם n מצבים לא ניתן להעביר ל-DFA עם $p(n)$ כלשהו כי $p(n) < 2^n$ (לכל $p: \mathbb{N} \longrightarrow \mathbb{N}$ קיים n_0 כך ש-$p(n_0) < 2^{n_0}$) והוכחנו חסם תחתון.

ביטויים רגולריים

ביטוי רגולרי מעל א"ב Σ:

1. $\emptyset, \varepsilon, \sigma \in \Sigma$ הם ביטויים רגולריים.
2. אם r_1 ו-r_2 הם ביטויים רגולריים, כך גם $r_1 + r_2, r_1 \cdot r_2, r_1^*$.

כל ב"ר r מגדיר שפה $L(r)$:

1. $L(\emptyset) = \emptyset, L(\varepsilon) = \varepsilon, L(\sigma) = \sigma$
2. $L(r_1 + r_2) = L(r_1) \cup L(r_2)$

   $L(r_1 \cdot r_2) = L(r_1) \cdot L(r_2)$

   $L(r_1^*) = (L(r_1))^*$

משפט: $L \subseteq \Sigma^*$ היא רגולרית $\Leftrightarrow$ L ניתנת להגדרה ע"י ביטוי רגולרי.

הוכחה בתרגול.

דוגמאות:

1. כל המילים שמסתיימות ב-1: $(0+1)^* \cdot 1$
2. L_n שראינו מקודם: $L_n = (0+1)^* 0 (0+1)^n$
3. מילים שיש בהן בדיוק 1 יחיד: $0^* 1 0^*$
4. מילים שיש בהן לפחות 1 יחיד: $0^* 1 (0+1)^* = (0+1)^* 1 (0+1)^*$
5. מילים שאין בהן את הרצף 00 או 11: $(\varepsilon + 0)(10)^*(1 + \varepsilon)$

אפיון שפות רגולריות

נגדיר יחס $\sim_L \subseteq \boldsymbol{\Sigma}^* \times \boldsymbol{\Sigma}^*$ (שקול L) עבור $L \subseteq \Sigma^*$:

לכל $x, y \in \Sigma^*$ מתקיים $x \sim_L y$ (x שקול y) $\Leftrightarrow$
$\forall z \in \Sigma^* \ \ (\ x \cdot z \in L \ \ \Leftrightarrow \ \ y \cdot z \in L \ )$

** כלומר, אין ל-x ול-y **זנב מפריד** – לא משנה איזה זנב נחבר להן, אם נחבר את אותו זנב שתיהן יהיו יחד (או לא) בשפה.

<u>דוגמה:</u> $L = (0+1)^*0(0+1)$.

- האם $111 \sim_L 11$?
  $\forall z \in \Sigma^* \ \ 11 \cdot z \in L \ \ \Leftrightarrow \ \ z \in L \ \ \Leftrightarrow \ \ 111 \cdot z \in L$, לכן שתי המילים שקולות L.
- האם $11 \sim_L 10$?
  אכן קיים z מפריד – כל z באורך 1. למשל עבור $z = 1$:
  $11 \cdot 1 \notin L$ אבל $10 \cdot 1 \in L$.

<u>$\sim_L$ הוא יחס שקילות:</u>

1. **רפלקסיבי** -
   לכל $x \in \Sigma^*$ מתקיים $x \sim_L x$.
2. **סימטרי** -
   לכל $x, y \in \Sigma^*$ מתקיים $x \sim_L y \Leftrightarrow y \sim_L x$.
3. **טרנזיטיבי** -
   לכל $x, y, v \in \Sigma^*$ אם $x \sim_L y$, $v \sim_L y$ אז $x \sim_L v$.

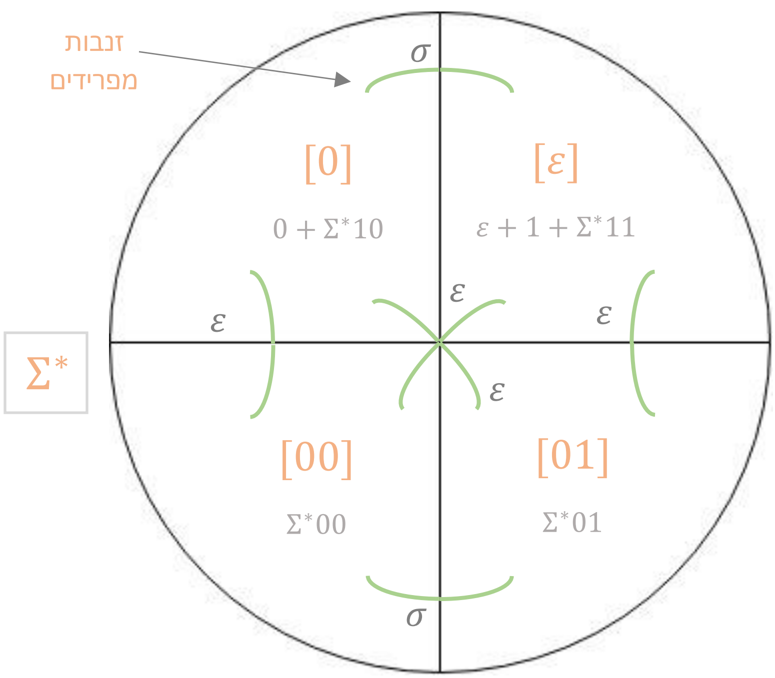
ואכן, אם יש z כך שבה"כ $v \cdot z \in L$, $x \cdot z \notin L$ אז נתהה האם $y \cdot z \in L$ ונקבל סתירה לכך ש-$x \sim_L y$, ואם לא אז זאת סתירה לכך ש-$v \sim_L y$.

מחלקות שקילות

סימון: $[w]$ = המחלקה של w.

מחלקות שקילות עבור $L = (0+1)^*0(0+1)$:

- האם $1 \sim_L 0$? לא, כי כל מילה באורך 1 מפרידה.
- $1 \sim_L \varepsilon$, אין זנב מפריד ולכן יהיו באותה מחלקת שקילות.
- $00 \nsim_L \varepsilon$ כי $00 \cdot \varepsilon \in L$ אבל $\varepsilon \cdot \varepsilon \notin L$.



משפט Myhill Nerode: לכל שפה $L \subseteq \Sigma^*$: (1) L רגולרית $\Leftrightarrow$ (2) מס' מחלקות השקילות של L הוא סופי.

מוטיבציה: $L = \{0^n \cdot 1^n : n \geq 0\}$, נראה שיש לה אינסוף מחלקות שונות ולכן היא לא רגולרית:
לכל $i \neq j$ $\quad 0^i \nsim_L 0^j$, זנב מפריד למשל יהיה 1^i.

הוכחה:

$(1 \Leftarrow 2)$ יהי $A = < Q, \Sigma, \delta, q_0, F >$ DFA עבור L. נגדיר יחס $\sim_A \subseteq \Sigma^* \times \Sigma^*$:

לכל $x, y \in \Sigma^*$ מתקיים $x \sim_A y \iff \delta(q_0, x) = \delta(q_0, y)$.

<u>טענה: מס' מחלקות השקילות של $\sim_A$ $\geq$ מס' מחלקות השקילות של $\sim_L$.</u>

(נראה שליחס $\sim_A$ יש יותר מחלקות שקילות מל-$\sim_L$)

מס' מחלקות השקילות של $\sim_A$ שווה למס' מצבי האוטומט A ($|Q|$ סופי), וזאת כי כל מחלקה מתאימה למצב.

לכל $x, y \in \Sigma^*$ אם $x \sim_A y$ אז $x \sim_L y$:

$x \sim_A y \Leftarrow \delta(q_0, x) = \delta(q_0, y) \Leftarrow$ לכל זנב $z \in \Sigma^*$ $\delta(q_0, x \cdot z) = \delta(q_0, y \cdot z) \Leftarrow$ לכל $z \in \Sigma^*$

$(x \cdot z \in L \iff y \cdot z \in L) \Leftarrow x \sim_L y$.

$(1 \Leftarrow 2)$ נגדיר DFA $A = < Q, \Sigma, \delta, q_0, F >$ עבור L:

$Q =$ מחלקות השקילות של L

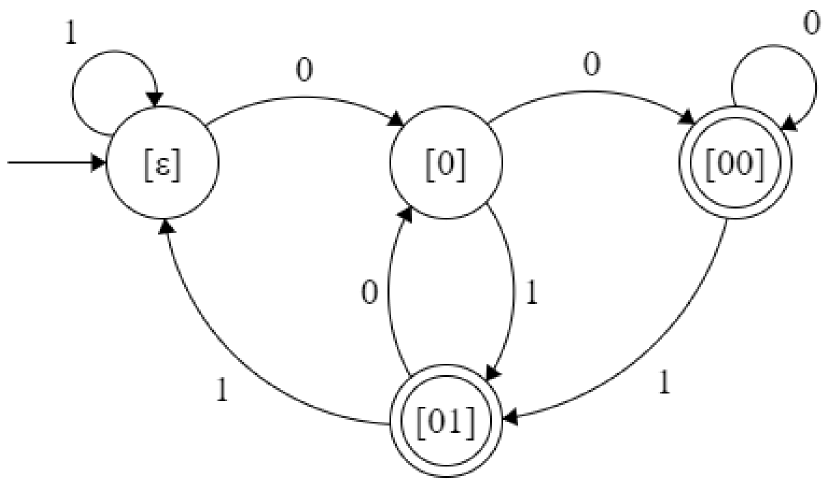
$q_0 = [\varepsilon]$

$\forall w \in \Sigma^*, \sigma \in \Sigma \quad \delta([w], \sigma) = [w \cdot \sigma]$

$F = \{[w] : w \in L\}$ (כל המצבים שהנציג שלהם בשפה)

הגדרת δ לא תלויה בבחירת הנציג: אם $x \sim_L y$ אז לכל $a \in \Sigma$ - $x \cdot a \sim_L y \cdot a$.
גם בהגדרת F בחירת הנציג לא חשובה, כי אם $w \in L$ אז $v \in L$ לכל $v \in [w]$, אחרת ε היה זנב מפריד.

<u>מהדוגמה הקודמת:</u>



ניתן להוכיח באינדוקציה על $|w|$ ש-$[w] = \delta(q_0, w)$, לכן $L(A) = L$ ו-L רגולרית.

שימוש במשפט:

$$L = \{0^i 1^j : \gcd(i,j) = 1\}$$

האם L רגולרית? נראה שיש אינסוף מחלקות ולכן אינה רגולרית.

לכל שני ראשונים $p_1, p_2 \in \mathbb{N}$ $0^{p_2} \nsim_L 0^{p_1}$, למשל 1^{p_1} זנב מפריד: $0^7 \cdot 1^7 \in L, 0^{11} \cdot 1^7 \notin L$.

שפות לא רגולריות

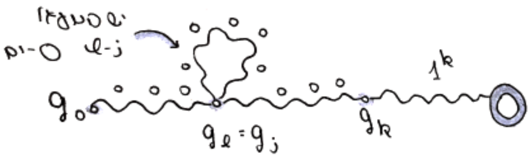
<u>טענה: השפה $L = \{0^n 1^n : n \geq 0\}$ איננה רגולרית.</u>
ראינו מ-Myhill Nerode שהשפה לא רגולרית.
הוכחה: נניח בשלילה שיש DFA A עבור L. יהי k מספר מצבי A. נתבונן בריצה של A על $0^k 1^k \in L$:

$$r = q_0, q_1, \dots, q_{2k} \qquad q_{2k} \in F$$

ברישא $q_0, \dots, q_k$ יש מצב שחוזר על עצמו (שובך היונים): יש $0 \leq l < j \leq k$ כך ש- $q_l = q_j$.

אבל אז, גם המילה $0^{k-(j-l)} 1^k$ מתקבלת, ובעצם

לכל $0 \leq i$ המילה $0^{k+i(j-l)} 1^k$ מתקבלת.



למת הניפוח לשפות רגולריות: אם $L \subseteq \Sigma^*$, אז קיים $p \geq 1$ (קבוע ניפוח) כך שלכל $w \in L$, אם $|w| \geq p$ אז קיימת חלוקה $w = x \cdot y \cdot z$ כך ש:
1. $|y| > 0$
2. $|x \cdot y| \leq p$
3. לכל $i \geq 0$: $x \cdot y^i \cdot z \in L$

<u>דוגמה:</u>

$L = (0+1)^* 0 (0+1)$, נראה שתנאי למת הניפוח מתקיימים: ניקח $p = 3$. נראה שלכל $w \in L$, אם $|w| \geq 3$, יש חלוקה כנדרש. נגדיר - הסיפא באורך $x = \varepsilon, |y| = 1, z = |w| - 1$.

1. $|y| = 1 > 0$ ✓
2. $|x \cdot y| = 1 \leq 3$ ✓
3. $x \cdot y^i \cdot z \in L$ לכל $i \geq 0$ ✓ למה? $|z| \geq 2$, ולכן הניפוח לא משפיע על האות הלפני האחרונה.

הוכחת הלמה:

יהי $A = < Q, \Sigma, \delta, q_0, F >$ DFA עבור L. נבחר $p = |Q|$ ונתבונן במילה $w = w_1 \dots w_n$ עבור $n \geq p$.

תהי $r = q_0, q_1, \dots, q_n$ הריצה המקבלת של A על w. מכיוון שבריצה יש $n + 1 > p$

מצבים, יש מצב שחוזר על עצמו.

לכן משובך היונים קיימים $0 \leq l < j \leq n$ כך ש-$q_l = q_j$. נחלק את w באופן הבא:

$$\overbrace{w_1 \dots w_l}^{x} \overbrace{w_{l+1} \dots w_j}^{y} \overbrace{w_{j+1} \dots w_n}^{z}$$

נראה שעבור חלוקה זו מתקיימים התנאים:

1. $|y| > 0$ ✓ כי $1 \leq j - l$.
2. $|x \cdot y| \leq p$ ✓ נבחר את $q_l = q_j$ להיות המצב הראשון שחוזר על עצמו, ונקבל בוודאות $|x \cdot y| \leq |Q| = p$.
3. $x \cdot y^i \cdot z \in L$ לכל $i \geq 0$ ✓ כי ניתן לנפח את הריצה המקבלת.

שימוש בלמת הניפוח (כדי להראות ששפה נתונה היא לא רגולרית)

<u>מבנה הלמה:</u> אם L רגולרית, אז β. <u>שימוש:</u> אם $\neg\beta$ אז L לא רגולרית.

$\beta \Leftarrow$ קיים p כך שלכל $w \in L$, $|w| \geq p$, קיימת חלוקה $w = x \cdot y \cdot z$ כך ש- $1 \wedge 2 \wedge 3$.

$\neg\beta \Leftarrow$ לכל p קיימת $w \in L$, $|w| \geq p$, ולכל חלוקה $w = x \cdot y \cdot z$ אם 1 ו-2 אז $\neg 3$.

כדי להראות ש-L אינה רגולרית נראה שלכל p קיימת $w \in L$ כך ש-$|w| \geq p$ ולכל חלוקה $w = x \cdot y \cdot z$ אם:
1. $|y| > 0$ 2. $|x \cdot y| \leq p$ $\Leftarrow$ אז קיים $i \geq 0$ כך ש-$x \cdot y^i \cdot z \notin L$.

<u>דוגמה 1:</u>

$L = \{0^n 1^n : n \geq 0\}$, לא רגולרית.

הוכחה:

בהינתן $p \geq 1$, נתבונן במילה $w = 0^p 1^p \in L$, $|w| > p$, ונראה שלכל חלוקה $w = x \cdot y \cdot z$ אם $|y| > 0$ ו-$|x \cdot y| \leq p$, קיים i כך ש-$x \cdot y^i \cdot z \notin L$.

זה נכון, כי בכל חלוקה כזו $y \in 0^+$ (שרשרת לא ריקה של 0-ים). כלומר $y = 0^l$ עבור $l \geq 1 \Leftarrow$

$$x \cdot y^2 \cdot z = 0^{p+l} 1^p$$

ומלמת הניפוח, L היא לא רגולרית.

<u>דוגמה 2:</u>

$L = \{w : \#_0 w = \#_1 w\}$, לא רגולרית.

הוכחה א':

מתכונות סגור. $L \cap 0^* 1^* = \{0^n 1^n : n \geq 0\}$.

מכיוון שהרגולריות סגורות לחיתוך ו-$0^* 1^*$ רגולרית ו-$\{0^n 1^n : n \geq 0\}$ לא רגולרית, אז בהכרח L לא רגולרית.

הוכחה ב':

יש אינסוף מחלקות MN - ל-0^i ו-0^j עבור $i \neq j$ יש זנב מפריד 1^i.

הוכחה ג':

בהינתן p נתבונן במילה $0^p 1^p$. כמו בהוכחה הקודמת, כל חלוקה של $x \cdot y \cdot z$ שמקיימת את תנאים 1 ו-2, אז $y \in 0^+$ ולכן $x \cdot y^2 \cdot z \notin L$.

<u>דוגמה 3:</u>

$L = \{w \cdot w : w \in (0+1)^*\}$, לא רגולרית.

הוכחה:

בהינתן $p \leq 1$ נתבונן במילה $w = 0^p 1 0^p 1$.

√ $w \in L$ √ $|w| \geq p$ √ לכל חלוקה שמקיימת את תנאים 1 ו-2, מתקיים $y \in 0^+$ ולכן $x \cdot y^2 \cdot z = 0^{p+l} 1 0^p 1 \notin L$ עבור $l \geq 1$.

<u>דוגמה 4:</u>

$L = \{0^{n^2} : n \geq 1\}$, $\Sigma = \{0\}$, לא רגולרית.

הוכחה:

בהינתן $p \leq 1$ נתבונן במילה $w = 0^{p^2}$.

√ $w \in L$ √ $|w| \geq p$

√ נתבונן בחלוקה $x \cdot y \cdot z$ שמקיימת $|y| > 0$ ו-$|x \cdot y| \leq p$, ונראה שמתקיים $x \cdot y^2 \cdot z \notin L$.

נניח ש-$|y| = l$, אז $|xy^2z| = p^2 + l$.

נראה ש- $p^2 < p^2 + l < (p+1)^2$, וזה כי $p^2 + l < (p+1)^2$ כי $|x \cdot y| \leq p \Leftarrow l \leq p$.

נסיק שאין n כך ש-$p^2 + l = n^2$, ואז נסיק ש-$x \cdot y^2 \cdot z \notin L$.

בעיות הכרעה על אוטומטים

1. **בעיית הריקנות** – בהינתן NFA או DFA A, להחליט האם $L(A) = \emptyset$.
2. **בעיית הכלת השפות** – בהינתן NFA-ים או DFA-ים A ו-B, להחליט האם $L(A) \subseteq L(B)$.

** הבעיה הראשונה היא מקרה פרטי של השנייה: $L(A) \subseteq \emptyset \iff L(A) = \emptyset$.

1. **ריקנות** – טענה: $L(A) \neq \emptyset$ אמ"מ בגרף המושרה מ-A יש מסלול מ-Q_0 ל-F.

גרף מושרה - $G_A = < Q, E_\delta >$ גרף מכוון המקיים $< q_1, q_2 > \in E_\delta \iff$ יש אות σ כך ש-$q_2 \in \delta(q_1, \sigma)$.

הוכחה: יש מסלול כזה אמ"מ יש מילה וריצה מקבלת עליה.

סיבוכיות: בהינתן גרף, כמה עולה להכריע האם השפה שלו ריקה? ליניארית ב-$|A|$, ע"י BFS או DFS לבדיקת ישיגות.

(אותו דבר ל-DFA ול-NFA).

2. **הכלה** – בהינתן אוטומטים A ו-B, האם $L(A) \subseteq L(B)$?

$$\alpha \subseteq \beta \iff \alpha \cap \bar{\beta} = \emptyset$$

נרצה לבדוק אם $L(A) \cap \overline{L(B)} = \emptyset \Leftarrow$ בדיקת ריקנות של $P = A \times \bar{B}$, אוטומט המקבל מילים שיש ב-A ולא ב-B.

סיבוכיות: פולינומיאלי אם B הוא DFA – אז $|P| = |A| \times |B|$ כי $\bar{B}$ מתקבל מ-B ע"י דואליזציה של F.

(גם אם A הוא NFA).

אקספוננציאלי אם B הוא NFA – אז $|\bar{B}| = 2^{|B|}$ ואז $|P| = |A| \times |2|^{|B|}$.

שפות חסרות הקשר context free languages

שפות חסרות הקשר מוגדרות ע"י <u>דקדוק חסר הקשר</u> G. לדוגמה:

$$G: A \longrightarrow 0A1$$
$$A \longrightarrow B$$
$$B \longrightarrow \#$$

<u>כאשר יש בדקדוק:</u> משתנים (A, B).

טרמינלים $(0,1,\#)$.

חוקי גזירה (למשל מ-A נוכל להפוך ל-$0A1$).

משתנה התחלתי (המשתנה השמאלי בחוק הראשון).

<u>גזירה של מילה בשפה:</u>

- מתחילים מהמשתנה ההתחלתי.
- כל עוד יש משתנים, מפעילים חוק רלוונטי.

למשל:

$$\underline{A} \longrightarrow 0\underline{A}1 \longrightarrow 00\underline{A}11 \longrightarrow 00\underline{B}11 \longrightarrow 00\#11$$

הגדרות

דקדוק חסר הקשר –

$$\boxed{G = < V, \Sigma, R, S >}$$

V – משתנים

Σ – א"ב (טרמינלים – אי אפשר לגזור אותם)

R – חוקים

S – משתנה התחלתי

- $S \in V$.
- $R: V \to (V \cup \Sigma)^*$

<u>דוגמה:</u>

$$G = < \{S, A\}, \{0,1\}, R, S >$$
$$S \longrightarrow A1A, \qquad A \longrightarrow 1A \mid 0A \mid \varepsilon$$

ייצור – אם $u, v, w \in (V \cup \Sigma)^*$ (מילים שהן ערבוב של משתנים ואותיות) ו-$A \longrightarrow W$ חוק בדקדוק, אז נאמר ש-$uAv \Rightarrow uwv$ (uAv מייצר את uwv).

- אם $u, v \in (V \cup \Sigma)^*$ גם משתנים וגם אותיות כך ש- $u \Rightarrow^* v$ (ניתן לייצר את v מ-u בכמה פעולות) אז קיימת סדרה $u_1, u_2, \dots, u_k \in (V \cup \Sigma)^*$ כך ש- $u = u_1 \Rightarrow u_2 \Rightarrow u_3 \Rightarrow \cdots \Rightarrow u_k = v$.

השפה של הדקדוק G – $L(G) = \{w: w \in \Sigma^*\ S \Rightarrow^* w\}$.

חזרה לדוגמה:

$$S \longrightarrow \underline{A}1A \longrightarrow 0\underline{A}1A \longrightarrow 01\underline{A}1A \longrightarrow 011\underline{A} \longrightarrow 011$$

$L(G) =$ כל המילים שיש בהן 1

עץ גזירה

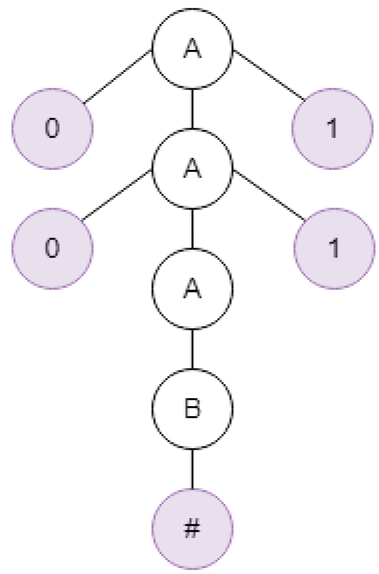
<u>מהדוגמה הקודמת:</u>

$$A \longrightarrow 0A1 \mid B$$

$$B \longrightarrow \#$$

$$\underline{A} \longrightarrow 0\underline{A}1 \longrightarrow 00\underline{A}11 \longrightarrow 00\underline{B}11 \longrightarrow 00\#11$$

ניתן לתיאור ע"י העץ:



כאשר העלים של העץ זו המילה.

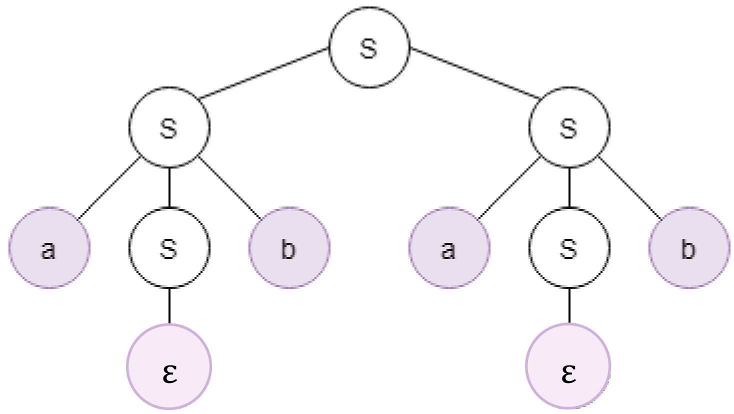
<u>דוגמאות:</u>

1. $G = <\{S\},\{a,b\},R,S>$

$$S \longrightarrow aSb \mid SS \mid \varepsilon$$

abab √

$$S \longrightarrow SS \overset{S\longrightarrow aSb}{\Longrightarrow} aSbS \overset{S\longrightarrow \varepsilon}{\Longrightarrow} abS \overset{S\longrightarrow aSb}{\Longrightarrow} abaSb \overset{S\longrightarrow \varepsilon}{\Longrightarrow} abab$$



√ aababb

- נסתכל על השפה מעל $\{(,)\}$ במקום - שפת הסוגריים המקוננים.
- השפה לא רגולרית: $L(G) \cap a^*b^* = \{a^nb^n : n \geq 0\} \notin \text{REG}$

מסקנה: $\text{CFL} \nsubseteq \text{REG}$.

2. איחוד דקדוקים:

$$\{0^n1^n : n \geq 0\} \cup \{1^n0^n : n \geq 0\}$$

$$S_1 \longrightarrow 0S_11 \mid \varepsilon \qquad L(S_1) = \{0^n1^n : n \geq 0\},$$

$$S_2 \longrightarrow 1S_20 \mid \varepsilon \qquad L(S_1) = \{1^n0^n : n \geq 0\},$$

נגדיר: $S \longrightarrow S_1 \mid S_2$.

משפט: CFL סגור לאיחוד.

3. דקדוק עבור שפת הפלינדרומים מעל $\{a, b\}$:

$$w = w_1 \dots w_k \ s.t \ w_i = w_{(k-i)+1}$$

$$S \longrightarrow aSa \mid bSb \mid a \mid b \mid \varepsilon$$

הוכחה באינדוקציה על סך ההפעלות של כל גזירה שהיינו צריכים בשביל המילה.

4. $L = \{0^n1^n2^n : n \geq 0\}$.

$$L_1 = \{0^n1^n2^i : n, i \geq 0\}$$

$$L_2 = \{0^i1^n2^n : n, i \geq 0\}$$

$$L = L_1 \cap L_2 \notin \text{CFL}$$

CFL לא סגור לחיתוך.

טענה: $\text{REG} \subseteq \text{CFL}$

בהינתן DFA $A=<Q,\Sigma,\delta,q_0,F>$ נבנה $G=<V,\Sigma,R,S>$ כך ש-$L(A)=L(G)$.

הרעיון:

$$V=Q$$

$$q \Rightarrow^* w \text{ אמ"מ } w\in L(A^q) \text{ כלומר } \delta(q,w)\in F$$

$$S=q_0$$

A^q - A עם מצב התחלתי q.

החוקים: לכל מצב q ואות σ כך ש-$\delta(q,w)=q'$, נוסיף ל-R את החוק $q\longrightarrow \sigma q'$,

אם $q\in F$ נוסיף ל-R את החוק $q\longrightarrow \varepsilon$.

<u>נוכיח שאכן $q_0\Rightarrow^* w \Leftrightarrow \delta(q_0,w)\in F$</u>:

$\Leftarrow$ תהי $w=w_1\dots w_n$, הריצה של A על w תהיה $q_0,q_1,\dots,q_n$ כך ש-$\delta(q_i,w_{i+1})=q_{i+1}$.

לכן $q_i\longrightarrow w_{i+1}q_{i+1}$ חוק בדקדוק, לכן $q_0\Rightarrow w_1q_1\Rightarrow w_1w_2q_2\Rightarrow w_1w_2w_3q_3\Rightarrow\cdots\Rightarrow wq_n$ סדרת גזירות חוקית.

$w\in L(A) \ \Leftarrow\ q_n\in F \ \Leftarrow\ q_n\longrightarrow\varepsilon \ \Leftarrow\ wq_n\Rightarrow w$ ולכן $q_0\Rightarrow^* w$, $w\in L(G)$.

$\Longrightarrow$ כיוון שני זהה, סדרת הגזירות משרה ריצה מקבלת.

** אם יהיה בור דוחה נגזור לנצח ולא נגיע למילה טרמינלית: $S\longrightarrow \sigma S\longrightarrow \sigma\sigma S\longrightarrow\cdots$.

דקדוק לינארי ימני: כל החוקים מהצורה $\varepsilon \mid A\longrightarrow \sigma B$. (אפשר להוכיח שהם בדיוק השפות הרגולריות)

חיתוך CFL ו-REG

$$L_1\in\text{CFL}\ \ L_2\in\text{REG}\qquad L_1\cap L_2\notin\text{REG}$$

דוגמה נגדית: $L_2=\Sigma^*$, $L_1=\text{CFL}\backslash\text{REG}$

$L_1\cap L_2=L_1\notin\text{REG}$

משפט: אם $L_1\in\text{CFL}$ $L_2\in REG$, אז $L_1\cap L_2\in CFL$.

** אם שפה L לא ח"ה וניתן להציג אותה כ-$L_1\cap L_2$ כך ש-L_1 רגולרית ניתן להסיק ש-L_2 איננה ח"ה.

הוכחה: בהינתן דקדוק $G=<V,\Sigma,R,S>$ עבור L_1, DFA $A=<Q,\Sigma,\delta,Q_0,F>$ עבור L_2,

נבנה דקדוק חדש G' כך ש-$L(G')=L(G)\cap L(A)$.

הנחות:

1. <u>G נתון בצורה **נורמלית של חומסקי:**</u>

   כלומר כל החוקים הם מהצורה -

   $A\longrightarrow BC$

   $A\longrightarrow \sigma$

וייתכן $S \longrightarrow \varepsilon$.

ניתן להניח זאת לפי משפט שאומר ש**לכל CFL יש CFL שקול בצורה נורמלית של חומסקי.**

2. <u>ל-A יש מצב מקבל יחיד.</u>

הצדקה להנחה: כל שפה רגולרית ניתנת לייצוג כאיחוד של שפות שניתנות לזיהוי ע"י DFA עם מצב מקבל יחיד.

הוכחת ההצדקה: $L(A) = \bigcup(A_{f=\{q\}})$.

$A_{f=\{q\}}$ סימון חדש: A עם מצב מקבל יחיד q.

CFL סגור לאיחוד, ולכן $L_1 \cap L_2 = L_1 \bigcap(\bigcup_i L_2^i) = \bigcup_i L_1 \cap L_2^i$.

הגדרת G':

$$G' = < V', \Sigma, R', S' >$$

<u>המשתנים:</u> $V' = Q \times V \times Q$, כל המשתנים מהצורה $[qAq']$.

הרעיון הוא ש-w ניתנת לייצוג מ-$[qAq']$ אם $A \Rightarrow^* w$ וגם אם $\delta(q, w) = q'$.

<u>המשתנה ההתחלתי:</u> $[q_0 S q_f]$, q_f המצב המקבל היחיד באוטומט.

<u>החוקים:</u>

- לכל חוק $V \longrightarrow V_1 V_2$ ב-R ולכל $q, p, r \in Q$ יהיה חוק ב-R': $[pVr] \longrightarrow [pV_1r][pV_2r]$.
- לכל חוק $V \longrightarrow \sigma$ ב-R יהיה חוק $[pVq]$ לכל $q, p \in Q$ כך ש-$\delta(p, \sigma) = q$.

דקדוקים חסרי הקשר

תזכורות

<u>דוגמה:</u>

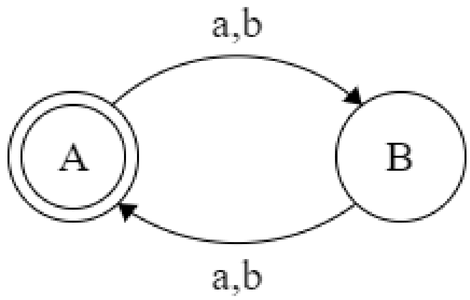
$\Sigma = \{a, b\}$, השפה: כל המילים באורך זוגי.

$A \longrightarrow aaA \mid abA \mid baA \mid bbA \mid \varepsilon$

אם היינו מתרגמים את האוטומט לדקדוק היינו מקבלים **דקדוק לינארי ימני** והיינו מקבלים:

$A \longrightarrow aB \mid bB \mid \varepsilon$

$B \longrightarrow aA \mid bA \mid \varepsilon$



דקדוק לינארי שמאלי:

$A \longrightarrow B\sigma \mid \varepsilon$

<u>בצורה נורמלית של חומסקי (לפי הדוגמה):</u>

A המשתנה ההתחלתי.

$A \longrightarrow BA \mid \varepsilon$ המשתנה ההתחלתי ייצור את כל הצפים האפשריים של מילים באורך 2.

$B \longrightarrow CC$

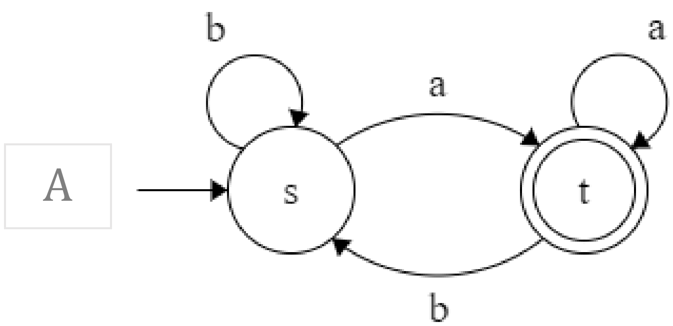
$C \longrightarrow a \mid b$

משפט: אם $L_1 \in \mathrm{CFL}$ $L_2 \in REG$, אז $L_1 \cap L_2 \in CFL$ – המשך

נתון: דקדוק $G = < V, \Sigma, R, S >$ בצורה נורמלית של חומסקי, $A = < Q, \Sigma, \delta, Q_0, F >$ עם מצב מקבל יחיד,

נגדיר $G' = < V', \Sigma, R', S' >$ כך ש-$L(G') = L(G) \cap L(A)$.

<u>דוגמה:</u>



$$G = \begin{cases} A \longrightarrow BA \mid \varepsilon \\ B \longrightarrow CC \\ C \longrightarrow a \mid b \end{cases}$$

G = מגדיר מילים באורך זוגי, A = מגדיר מילים שמסתיימות ב-a.

החיתוך הוא כל המילים באורך זוגי שמסתיימות ב-a.

משתנה התחלתי: $[sAt]$

מצבים: $V' = Q \times V \times Q$ $\quad [q, A, p]$

הרעיון: $[q, A, p] \Rightarrow^* w \Longleftrightarrow A \Rightarrow^* w$ וגם $\delta(q, w) = p$.

משתנה התחלתי: $[q_0, S, q_f]$, q_f המצב המקבל היחיד באוטומט.

ואכן, רוצים לגזור מילים שנגזרות מ-S ומעבירות את A מ-q_0 ל-q_f.

1. (גזירת ε) אם $q_0 = f$ וגם $S \longrightarrow \varepsilon$ נוסיף חוק $[q_0, S, q_f] \longrightarrow \varepsilon$
2. על כל חוק מהצורה $A \longrightarrow BC$ בדקדוק G נוסיף ל-R' את החוקים:

$$[pAq] \longrightarrow [pBr][rCq]$$

עבור כל שלושה מצבים $p, r, q \in Q$.

מהדוגמה:

$$[sAt] \longrightarrow [sBs][tAt] \mid [sBt][sAt]$$

$$[sBs] \longrightarrow [sCs][tCs] \mid [sCt][sCs]$$

3. על כל חוק מהצורה $A \longrightarrow \sigma$ בדקדוק G ולכל מעבר $\delta(q, \sigma) = p$ נוסיף ל-R' חוק: $[qAp] \longrightarrow \sigma$.

מהדוגמה:

$$[sCs] \longrightarrow b$$

$$[tCs] \longrightarrow b$$

$$[sCt] \longrightarrow a$$

<u>טענה: $[q, A, p] \Rightarrow^* w \Leftrightarrow A \Rightarrow^* w$ וגם $\delta(q, w) = p$.</u>

הוכחה: באינדוקציה על $|w|$.

$|w| = 0$ מהגדרת החוק היחיד שגוזר את ε.

$|w| = 1$ מהגדרת החוקים שגוזרים אותיות.

$|w| > 1$ מהרצת החוק עבור $A \longrightarrow BC$.

ריבוי משמעות Ambiguity

<u>אינטואיציה:</u>

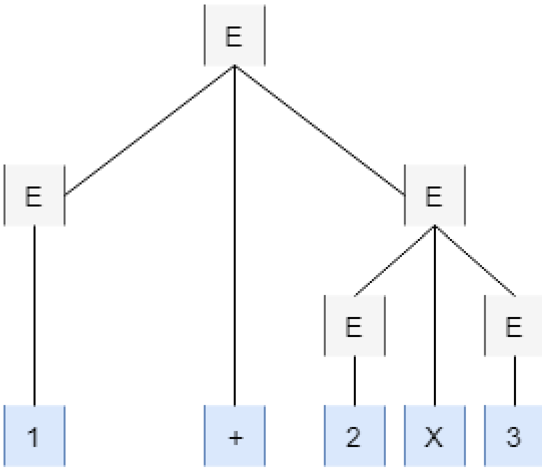
- הילדה נגעה בילד עם הפרח.
- $(5 \times 8) + 3$ או $8 \times (3 + 5) \longrightarrow 3 + 5 \times 8$.

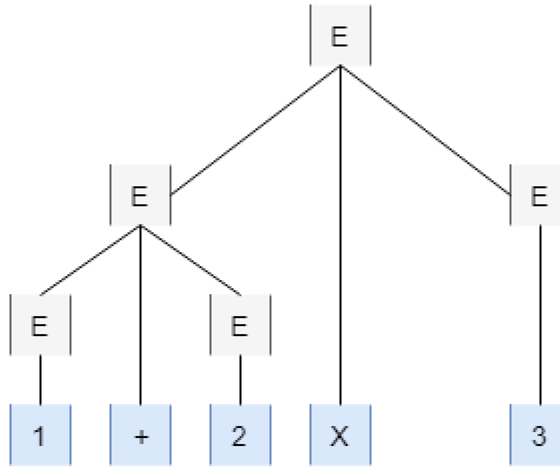
<u>דוגמה:</u>

$$E \longrightarrow E + E \mid E \times E \mid 0 \mid 1 \mid 2 \mid 3 \qquad \Sigma = \{+, \times, 1, 2, 3, 0\}$$

ועבור המילה $1 + 2 \times 3$ יש שני עצי גזירה שונים:

אחד למילה $(1 + 2) \times 3$ ואחד למילה $1 + (2 \times 3)$.





← **דקדוק רב משמעי** – דקדוק כך שיש מילה שניתן לגזור ע"י שני עצי גזירה שונים.

נשים לב שזה שונה מדקדוק בו יש מילה שניתן לגזור ע"י שתי סדרות גזירה שונות.

<u>דוגמה:</u>

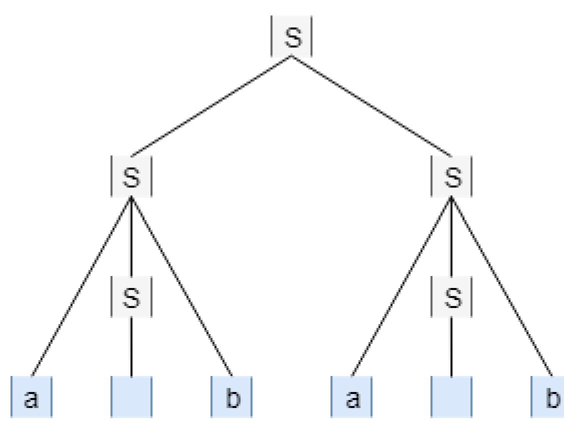
$$S \longrightarrow aSb \mid SS \mid \varepsilon$$

שתי גזירות שונות ל-$abab$:

$$S \longrightarrow SS \longrightarrow aSbS \longrightarrow aSbaSb \longrightarrow abaSb \longrightarrow abab$$

$$S \longrightarrow SS \longrightarrow aSbS \longrightarrow aSbaSb \longrightarrow aSbab \longrightarrow abab$$

אבל עץ גזירה יחיד:



← **גזירה שמאלית ביותר** – גזירה שבה בכל שלב גוזרים את המשתנה הכי שמאלי.

דוגמה: $S \longrightarrow SS \longrightarrow aSab \longrightarrow abS \longrightarrow abaSb \longrightarrow abab$

← **שקול** – דקדוק מילה שניתן לגזור ע"י שתי סדרות גזירה שמאלית ביותר שונות.

תורת החישוביות

מכונת טיורינג Turing machine

מכונת טיורינג מטיילת על מילה, עוברת ממצב למצב ומחליטה האם לקבל אותה או לא.

<u>מה ההבדל בין מכונת טיורינג לבין אוטומט רגיל?</u>

1. סרט העבודה הוא אינסופי.
2. ניתן להזיז את הראש הקורא שמאלה וימינה.
3. יכולת לכתוב על הסרט.
4. מצב מקבל ומצב דוחה.

<u>דוגמה:</u>

M מ"ט עבור $L = \{w\#w : w \in \{0,1\}^*\}$ פועלת כך:

1. סורקת את הסרט ומוודאת שהקלט מהצורה $(0+1)^*\#(0+1)^*$.
2. מזגזגת במיקומים תואמים ומוודאת שהם מסומנים באותה האות:
   - 2.1 – מחוק את התו הנוכחי, כתוב בו x, זכור האם היה 0 או 1.
   - 2.2 – לך לתא הלא מחוק הראשון מימין ל-#.
   - 2.3 – אם תוכנו שווה למה שזכרת, מחק אותו. אחרת דחה.
   - 2.4 – לך שמאלה, עקוף את ה-#, התקדם עד ל-x , ולך צעד אחד ימינה.
     אם #, לך ל-2.5. אם 0 או 1, עבור ל-2.1.
   - 2.5 – לך ימינה עד 0, 1 או __. אם 0 או 1, דחה. אם __, קבל.

הגדרות (עבור מכונת טיורינג דטרמיניסטית)

$$\mathrm{M} = < Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} >$$

Σ – א"ב הקלט, לא כולל את האות __.

Γ – א"ב העבודה (אותיות שמכונת טיורינג עשויה לכתוב על הסרט).

- $\_ \in \Gamma$
- $\Sigma \subseteq \Gamma$

$$Q \ni \begin{cases} q_0 - \text{מצב התחלתי} \\ q_{acc} - \text{מצב מקבל} \\ q_{rej} - \text{מצב דוחה} \end{cases}$$

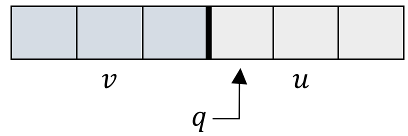
$$\delta : Q \times \Gamma \longrightarrow Q \times \Gamma \times \{L, R\}$$

אם $\delta(q,a) = (q', b, L)$, אז כש-M במצב q וקוראת a, M עוברת ל-q', כותבת b במקום a, ומזיזה את הראש תא אחד שמאלה.

קונפיגורציה של M –

- המצב הנוכחי
- תוכן הסרט
- מיקום הראש

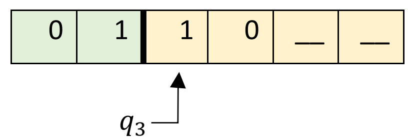
כלומר קונפיגורציה $\boldsymbol{vqu}$ עבור $v, u \in \Gamma^*$, $q \in Q$:



- המצב הנוכחי: q.
- תוכן הסרט: vu.
- מיקום הראש: האות הראשונה של u.

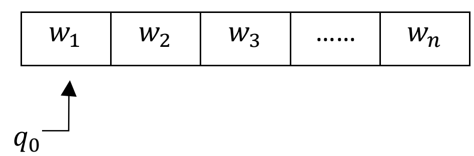
<u>דוגמה:</u>

קונפיגורציה $01q_310$ תיראה כך:



ריצה – ריצה של M על $w \in \Sigma^*$ היא סדרה של קונפיגורציות.

- הקונפיגורציה ההתחלתית היא q_0w.



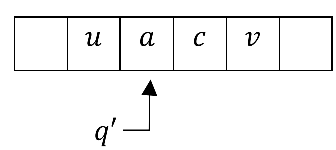
- קונפיגורציה מקבלת – קונפיגורציה שהמצב שלה הוא q_{acc}.
- קונפיגורציה דוחה – קונפיגורציה שהמצב שלה הוא q_{rej}.

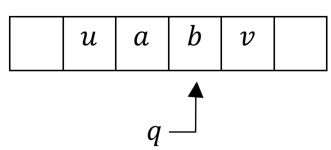
$\Big\}$ קונפיגורציה עוצרת halting configuration

- קונפיגורציות עוקבות – נתבונן בקונפיגורציה $uaqbv$ עבור $u, v \in \Gamma^*$, $a, b \in \Gamma$, $q \in Q$.

  לזיהוי הקונפיגורציה העוקבת:

  - אם $\delta(q, b) = (q', c, L)$, $q' \in Q$, $c \in \Gamma$: $uaqbv \longrightarrow uq'acv$
  - אם $\delta(q, b) = (q', c, R)$: $uaqbv \longrightarrow uacq'v$

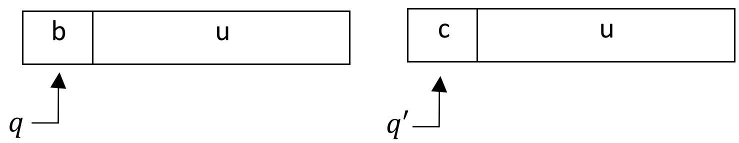




~ חזרה על שיעור קודם ~

<u>מקרה מיוחד</u> – הראש הקורא נמצא על התא השמאלי בסרט.

$\delta(q,b)=(q',c,L)$ - נשארים במקום כשפונק' המעברים מזיזה שמאלה: $qbu \longrightarrow q'cu$.



- M **מקבלת** את w אם קיימת סדרת קונפיגורציות $c_0,\dots,c_k$ כך ש-
  1. c_0 קונפיגורציה התחלתית של M על w (כלומר $c_0=q_0w$).
  2. לכל $0\le i<k$, c_{i+1} עוקבת ל-c_i.
  3. c_k קונפיגורציה מקבלת (q_{acc}).
- **השפה** של M – $L(\mathrm{M})=\{w\in\Sigma^*: w \text{ מקבלת את } \mathrm{M}\}$.
- נאמר ש-M **מזהה** את $L\subseteq\Sigma^*$ אם $L(\mathrm{M})=L$.
- שפה L היא **Recursively enumerate (ב-RE)**, אם קיימת מ"ט שמזהה את L.

נשים 🧡: לריצה של M על w יש שלושה גורלות אפשריים:

1. קבלה (הגעה ל-q_{acc}).
2. דחייה (הגעה ל-q_{rej}).
3. אי עצירה (לא מגיעים לעולם ל-q_{acc} או ל-q_{rej}). המכונה לאו דווקא עוברת על אותה קונפיגורציה פעמיים.

<u>דוגמה לשפה ב-RE:</u> $L=\{\mathrm{P}: 0 \text{ עוצרת על הקלט } \mathrm{P}\}$, P היא תוכנת מחשב שמוגדת על הקלטים 0, 1, 2.

בהינתן P, מ"ט M שמזהה את L תריץ את P על 0.

אם P עוצרת, אז M עוצר ומקבלת.

אם P לא עוצרת, M לא עוצרת.

- נאמר ש-M **מכריעה** את L אם $L(\mathrm{M})=L$ ובנוסף M עוצרת על כל קלט.
- שפה L היא **Recursive (ב-R)**, אם קיימת מ"ט שמכריעה את L.

$\mathrm{R}\subseteq\mathrm{RE}$: M מכריעה את L $\Longleftarrow$ M מזהה את L

<u>דוגמה:</u>

מ"ט שמכריעה את $L=\{0^{2^n}: n\geq 0\}=\{0,00,0^4,0^8,0^{16},\dots\}$ (ראינו לא רגולרית ולא ח"ה)

הרעיון: נתבונן בפרודוקט $\text{good}\subseteq\mathbb{N}$.

$$\text{good}(\text{k})\Leftrightarrow \text{k}=1\ \vee\ \text{good}\left(\frac{\text{k}}{2}\right)\ \text{and k is even}$$

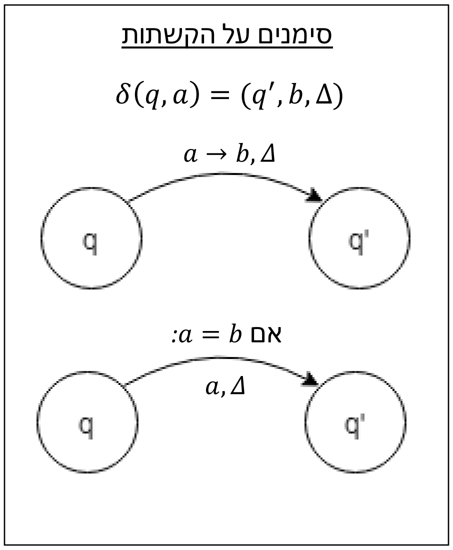
האלגוריתם:

0. אם הסרט ריק, דחה.

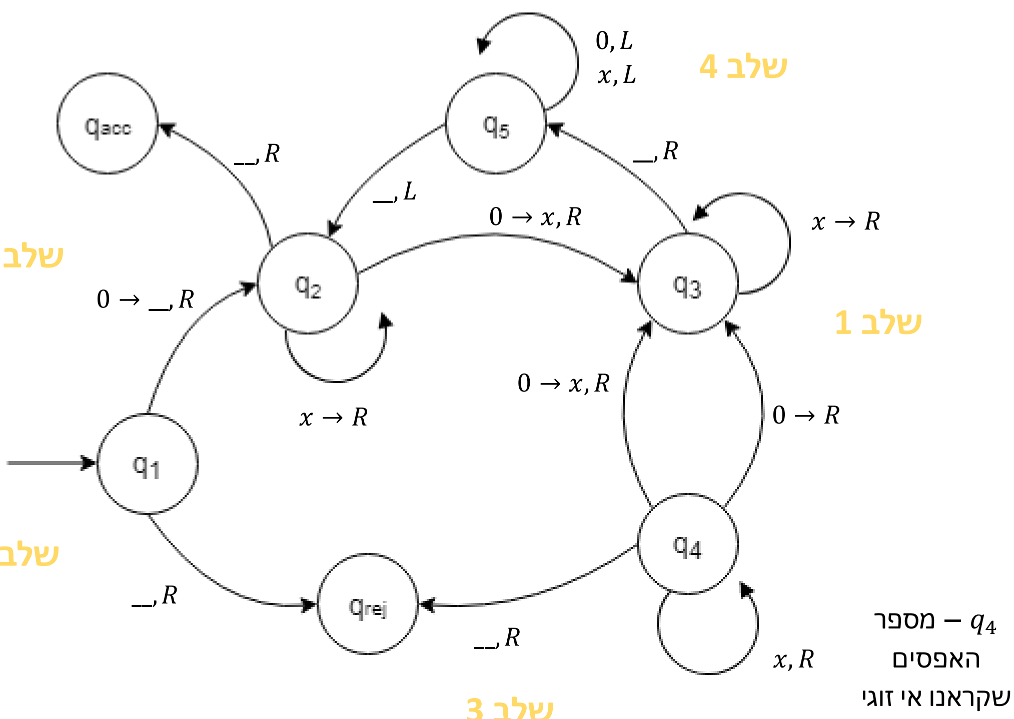
0.5. סמן את התא הראשון ב-__.

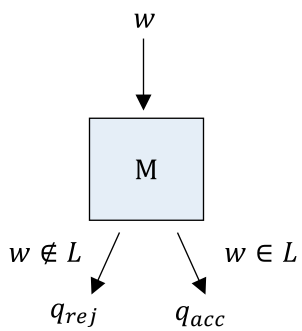
1. סרוק את הסרט משמאל לימין, מחק כל 0 שני (הפוך אותו ל-X).
2. אם היה בקלט 0 יחיד, קבל.
3. אם היה בקלט מס' אי זוגי של 0-ים, דחה.
4. חזור עם הראש הקורא לתחילת הסרט (עד ל-__).
5. לך לשלב 1.

- לכן סרט הקלט סופי וזה מבטיח עצירה $w\in\Sigma^*$.



$\Sigma=\{0\}\quad \Gamma=\{0,\text{x},\_\}$





- **coRE** – המשלים של RE.

<u>$L \in \mathrm{coRE}$ אמ"מ $\bar{L} \in \mathrm{RE}$:</u>

אם יש M מ"ט שמזהה את L, M עוצרת ודוחה מילים שאינן ב-L.

M מקבלת או לא עוצרת על מילים ב-L.

<u>דוגמה: בעיית הריצוף.</u>

קלט קבוצה סופית של אריחים.

פלט האם יש ריצוף חוקי (אריחים שכנים שמסכימים על הצבע בצלע המשותפת) $n \times n$ לכל n.

משפט: $\mathrm{RE} \cap \mathrm{coRE} = \mathrm{R}$

הוכחה:

1. <u>$\mathrm{R} \subseteq \mathrm{RE} \cap \mathrm{coRE}$</u>

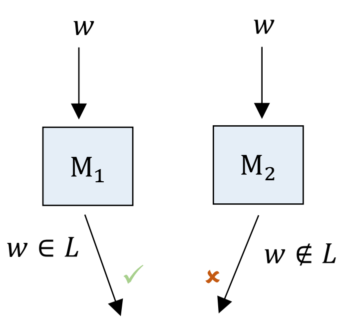
$\mathrm{R} \subseteq \mathrm{RE}$ כי אם M מכריעה את L אז M מזהה את L.

$\mathrm{R} \subseteq \mathrm{coRE}$ תהי $L \in \mathrm{R}$ ותהי M מ"ט מכריעה את L אז M מזהה את L.

נתבונן במ"ט $\widetilde{\mathrm{M}}$ שמתקבלת מ-M ע"י החלפת q_{acc} עם q_{rej}.

קל לראות $\overline{L(\mathrm{M})} = L(\widetilde{\mathrm{M}})$ $\Leftarrow$ יש מ"ט $\widetilde{\mathrm{M}}$ שמכריעה את $\bar{L}$ אז $\widetilde{\mathrm{M}}$ מזהה את $\bar{L}$ $\Leftarrow$ $L \in co-\mathrm{RE}$.

2. <u>$\mathrm{RE} \cap \mathrm{coRE} \subseteq \mathrm{R}$</u>



תהי $\mathrm{L} \in \mathrm{RE} \cap \mathrm{coRE}$. יש מ"ט M_1 שעוצרת ומקבלת מילים ב-L.

יש מ"ט M_2 שעוצרת ודוחה מילים לא ב-L.

רעיון ההוכחה: הרצה במקביל.

נגדיר מ"ט M שמכריעה את L: עבור .... $i = 1,2,3$

- M מריצה את M_1 i צעדים על w.
- M מריצה את M_2 i צעדים על w.

✓ אם M_1 קיבלה את w, M מקבלת.

× אם M_2 דחתה את w, M דוחה.

מכיוון ש-$w \in L$ או $w \notin L$, מובטח שקיים i שבו M_1 תקבל את w או M_2 תדחה את w ⟵ M תעצור.

ספרן Enumerates

מודל שקול ל-RE.

Enumerator – מ"ט עם מדפסת.

השפה של ספרן E, $L(\mathrm{E})$, היא קבוצת המילים שאי פעם מודפסות. ייתכן ש-E לא יעצור, וייתכן שידפיס מילה מסוימת אינסוף פעמים.

משפט: $L \in \mathrm{RE}$ אמ"מ יש ספרן E כך ש-$L(\mathrm{E}) = L$.

הוכחה:

$\Leftarrow$ נניח שיש ספרן E כך ש-$L(\mathrm{E}) = L$.

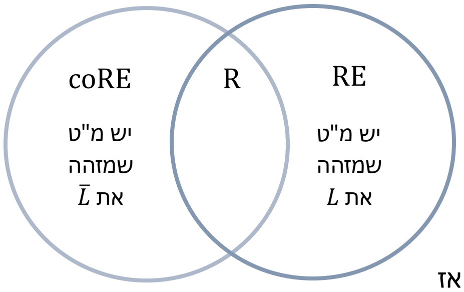
נבנה מ"ט M עבור L:

M מריצה את E. כל פעם ש-E מדפיסה מילה, בודקת האם זו w. אם כן, עוצרת ומקבלת. אם לא, הספרן ממשיך להדפיס.

מובטח: אם $w \in L$, E ידפיס את w $\longleftarrow$ M תעצור ותקבל את w $\longleftarrow$ M מזהה את w.

~ המשך בשיעור הבא ~

משפט: $L \in \mathrm{RE}$ אמ"מ יש ספרן E כך ש-$L(\mathrm{E}) = L$. (המשך הוכחה)



הוכחה:

$\Leftarrow$ אם ספרן E כך ש-$L(\mathrm{E}) = L$, אז יש מ"ט M שמזהה את L – ראינו בשיעור קודם.

$\Rightarrow$ נניח שיש מ"ט M שמזהה את L, נרצה להוכיח שיש ספרן ששפתו היא L.

ניסיון רע ☹ - $\Sigma = \{0,1\}$ ונסתכל על סידור ∞ Σ^* $\varepsilon, 0, 1, 00, 01$.

נריץ את M על ε. אם קיבלה, נדפיס את ε. אם לא, נריץ את M על 0, וכן הלאה.

אבל נשים לב שהיא יכולה להיתקע – אם לא מקבלת את ε למשל, יכול להיות שהיא תיתקע, ואז האנומרטור ידפיס כלום. אם יש לנו מכונה שרק מזהה, לא נוכל להגיד מה היא תעשה אחרי שהיא תידחה מילה.

ניסיון טוב 😊 - E יפעל כך:

יהי $w_1, w_2, w_3, \ldots$ סידור של המילים ב-Σ^*. נחזיק מונה $i = 1$ ובכל איטרציה E יריץ את M על $w_1 w_2 \ldots w_i$ במשך i צעדים. אם M קיבלה את w_j עבור $1 \leq j \leq i$. נדפיס את w_j. נגדיל את המונה בסוף כל איטרציה: $i++$.

<u>טענה: $L(\mathrm{E}) = L(\mathrm{M})$</u>

1. קל לראות שאם E מדפיס מילה w, אז $w \in L(\mathrm{M})$.
2. תהי $w \in L(\mathrm{M})$ $\longleftarrow$ יש ל-M ריצה מקבלת על w.

יהי m מספר הצעדים בריצה. נדפיס את w בכל איטרציה שבה $i \geq m$ והאינדקס של w בסידור קטן מ-i.

- למעשה כל המילים ב-$L(\mathrm{M})$ מודפסות אינסוף פעמים.

<u>1900 הבעיה ה-10 של Hilbert</u>: לתאר אלגוריתם שבהינתן פולינום במס' משתנים יכריע האם יש לו שורש שלם.

אלגוריתם לפי כוונתו – תהליך איתו אפשר להכריע אחרי מספר סופי של פעולות.

אין אלגוריתם!

<u>1936 התזה של Church ו-Turing</u>: ניתן להכריע (יש אלגוריתם) $\Leftrightarrow$ יש מכונת טיורינג שמכריעה. (לפי Turing)

$\Lambda - \mathrm{calculs}$ - לוגיקה מסדר גבוה (לפי Church).

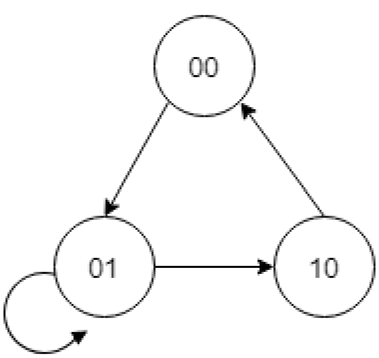
למשל, עבור הבעיה של הילברט נגדיר שפה $D = \{<P>: P$ פולינום שיש לו פתרון בשלמים$\}$.

$<P>$ - קידוד של פולינומים.

<u>מ"ט יכולה לקבל בקלט:</u>

✓ **גרפים:**

G גרף, $<G>$ קידוד לגרף. ולדוגמה מכונת טיורינג שמקבלת גרף ומכריעה אם הוא קשיר. עבור הגרף בדוגמה, סרט הקלט: (מחולק לפי צבעים לקדקודים ולצלעות)



0	0	#	0	1	#	1	0	#	\$	0	0	#	1	0	\$	0	0	#	1	0	\$	...

- ✓ **פולינומים:**

למשל הפולינום: $3x^2y^5$

סרט הקלט:

x	y	z	#	3	2	$	1	5	$	0	1

המשתנים

המקדם של x

המעריך של x

נשים לב $D \in \mathrm{RE}$: M תעבור על כל ההשמות האפשריות בשלמים לכל המשתנים. אם ההשמה מהווה שורש, תקבל.

אם הפולינום במשתנה אחד, ניתן להכריע.

- ✓ **אוטומטים:**

$$A_{DFA} = \{\langle A \rangle, w : A \text{ הוא } DFA \text{ ו־} w \in L(A)\} \in \mathrm{R}$$

סרט הקלט:

q_0	q_1	q_2	#	σ_1	σ_2	#	q_0	#	q_0	σ_1	q_2	#	q_0	σ_2	q_0	#	q_1	#	$	σ_1	σ_2	σ_1

w

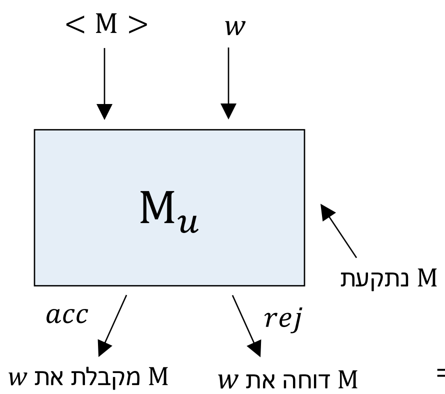
- ✓ **מ"ט**

אי כריעות

משפט: יש שפה ב-RE\R.

$$A_{TM} = \{(<\mathrm{M}>, w): \text{M מקבלת את } w\}$$

הוכחה:



$\boxed{A_{TM} \in \mathrm{RE}}$

נשתמש במ"ט אוניברסלית M_u שמקבלת כקלט $<\mathrm{M}>$ ומריצה את M על w.

M_u פועלת כך: למכונה שני סרטים -

1. סרט הקלט של M_u (תיאור המכונה M):

Q	Σ	Γ	.....

$$\Rightarrow \underbrace{0\#01\#10}_{Q}\,\$\,\underbrace{0\#1}_{\Sigma}\,\$\,\underbrace{0\#1\#\_\#a}_{\Gamma}\,\$\,\underbrace{00}_{q_0}\,\$\,\underbrace{\overbrace{00\#0\#01\#0\#L}^{**}\,\&\,\overbrace{\ldots}\,\&\ldots}_{\delta}\,\$\,\underbrace{\ }_{q_{acc}}\,\$\,\underbrace{\ }_{q_{rej}}\,\$\,w$$

$$** \; \delta(00,0) = (01,0,L)$$

2. סרט הסימולציה. בכל איטרציה כתובה קונפיגורציה בריצה של M על w.

M_u מעדכנת את סרט הסימולציה:

מחפשת בסרט הקלט את המעבר הרלוונטי ומפעילה אותו.

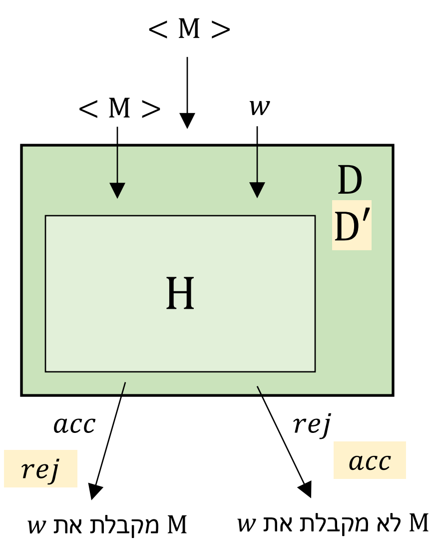
אם M_u מגיעה לקונפיגורציה מקבלת, אז היא עוצרת ומקבלת. אם הגיעה לקונפיגורציה דוחה היא עוצרת ודוחה.

ייתכן ש-M לא עוצרת על w ואז גם M_u לא עוצרת.

למשל:

00	$w = 0w_1 \ldots w_n$	......

עבור $q_0 w$ תחפש באזור של δ איפה יש 00#0.



$\boxed{A_{TM} \notin \mathrm{R}}$

- נניח בשלילה שיש מ"ט **H** שמכריעה את A_{TM},

$$\mathrm{H}(<\mathrm{M}>, w) = \begin{cases} acc, & \mathrm{M}\ acc\ w \\ rej, & \mathrm{M}\ rej\ w \end{cases}$$

- נבנה מ-H מ"ט **D** שמקבלת כקלט מ"ט $<\mathrm{M}>$ ופועלת כך:

$$\mathrm{D}(<\mathrm{M}>) = \begin{cases} acc & \mathrm{M}\ acc <\mathrm{M}> \\ rej & \mathrm{M}\ not\ acc <\mathrm{M}> \end{cases}$$

<u>הבהרות:</u>

- $<\mathrm{M}>$ מילה ב-$\{0,1,\#,\$\}^*=\Sigma^*$.
- הקלט ל-H: $<\mathrm{M}>$ מילה מעל Σ^*, w מילה מעל Σ^*.

הסבר על D: היא מקבלת תיאור מ"ט בקלט עם ומריצה אותה על עצמה, בעצם הופכת אותה לקלט ל-H.

H תבדוק האם המכונת טיורינג שקיבלה עוצרת על קידוד של עצמה.

- נבנה מ-D מ"ט $\mathbf{D'}$ שמקבלת בקלט מ"ט $<\mathrm{M}>$ ופועלת כך:

$$\mathrm{D}'(<\mathrm{M}>)=\begin{cases}acc & \mathrm{M}\ not\ acc<\mathrm{M}> \\ rej & \mathrm{M}\ acc<\mathrm{M}>\end{cases}$$

D' מתקבלת מ- D ע"י החלפת q_{acc} ו q_{rej}.

- נתבונן בריצה של D' על $<\mathrm{D}'>$:

$$\mathrm{D}'(<D'>)=\begin{cases}acc & D'\ not\ acc<\mathrm{D}'> \\ rej & D'\ acc<\mathrm{D}'>\end{cases}.$$

סתירה.

מסקנה: אין מ"ט H כזו $\Leftarrow$ $\mathrm{A_{TM}}\notin R$

הוכחה אלטרנטיבית לפי שיקולי ספירה:

- כמה שפות מעל $\{0,1\}$ יש?

  יש $\aleph_0$ מילים מעל $\{0,1\}$ $\longleftarrow$ יש $2^{\aleph_0}$ שפות מעל $\{0,1\}$.

  אותה ספירה ניתן לעשות עבור $\{0,1,\$,\#\}$

- כמה מכונות טיורינג יש?

  יש $\aleph_0$ מ"ט (מ"ט משרה מילים מעל $\{0,1,\$,\#\}$) $\longleftarrow$ $2^{\aleph_0}>\aleph_0$ $\Leftarrow$ **יש שפה שאין לה מכונה.**

$$\overline{A_{TM}}=\left\{(<\mathrm{M}>,w):w\ \text{לא עוצרת}\ \mathrm{M}\right\}\notin \mathrm{RE}$$

כי $\mathrm{RE}\cap\mathrm{coRE}=\mathrm{R}$

$A_{TM}\in\mathrm{RE}$ אבל $A_{TM}\notin\mathrm{R}$ ולכן המשלימה שלה לא יכולה להיות ב-coRE

~ הבהרה לגבי ההוכחה משיעור קודם ~

$$\boxed{A_{TM} \in \mathrm{RE/R}}$$

$$A_{TM} = \{(<\mathrm{M}>, w): \text{מקבלת את } w \text{ M}\}$$

$$A_C = \{(P, w): \text{תוכנית (פונקציה) ב} - \mathrm{C} \text{ שמחזירה כן על } w\ P\}$$

נניח בשלילה שיש תוכנית ב-C , H שמכריעה את A_C:

$$function\ H\big(P{:}\ string\ (\text{קידוד לתוכנית}), w{:}\ string\big){:}\ Boolean$$

← אז אם יש כזאת H, יש גם תוכנית D:

$$function\ D(P{:}\ string){:}\ Boolean$$

שקוראת ל-H עם: $H(P, P)$

← D' מתקבלת ע"י החלפת return yes $\leftrightarrow$ return no.

← לקבלת סתירה התבוננו ב-$D'(D)$, כי D' אמורה להחזיר yes.

רדוקציות

כלי להוכחת אי כריעות.

<u>דוגמה:</u>

$$HALT_{TM} = \{(<\mathrm{M}>, w): \text{עוצרת על } w \text{ M}\}$$

$HALT_{TM} \notin \mathrm{R}$ ← נראה שלו הייתה מכונה T שמכריעה את $HALT_{TM}$,

היינו יכולים לבנות מכונה S שמכריעה את A_{TM}.

S פועלת כך:

על קלט $(<\mathrm{M}>, w)$ נריץ את T על $(<\mathrm{M}>, w)$.

אם T עצרה ודחתה (סימן ש-M לא עוצרת על w, אז M לא מקבלת את w), אז S תדחה.

אם T עוצרת ומקבלת, סימן ש-M עוצרת על w, אז נריץ את M על w, מובטח שנעצור, ונענה כמוה.

מסקנה: אין T כזו, ולכן $HALT_{TM} \notin \mathrm{R}$.

הגדרות

פונקציה $f{:}\ \Sigma^* \longrightarrow \Sigma^*$ תקרא **פונקציה ניתנת לחישוב**, אם קיימת מ"ט M_f שעל קלט $w \in \Sigma^*$ עוצרת עם $f(w)$ על הסרט.

<u>דוגמאות:</u>

- $add{:}\ (0+1)^* \longrightarrow (0+1)^*$.

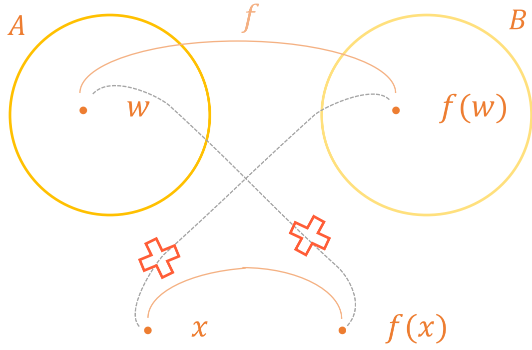
$add(111011) = 11111$ חיבור לקלטים מקודדים באונרית.

$add(010\#1100) = 14$ חיבור לקלטים מקודדים בבינארית.

- $f{:}$ מ"ט $\longrightarrow$ מ"ט. בהינתן M, f מחזירה M' כך ש-$L(\mathrm{M}) = L(\mathrm{M}')$ ו-M' לעולם לא מגיעה ל-q_{rej}.

M' תתקבל מ-M ע"י כיוון המעברים שהולכים ל-q_{rej} למצב חדש - q_{loop}, שחוזר על עצמו.

רדוקציית מיפוי – שפה $A \subseteq \Sigma^*$ ניתנת לרדוקציית מיפוי לשפה $B \subseteq \Sigma^*$, ונסמן $\boldsymbol{A \leq_m B}$, אם קיימת פונקציה ניתנת לחישוב $f: \Sigma^* \longrightarrow \Sigma^*$ כך שלכל $w \in \Sigma^*$, $w \in A \iff f(w) \in B$.



<u>דוגמה:</u>

$$A = \{x: |x| \leq 5\}, B = \{x: |x| \leq 10\}, \qquad f(x) = 2x$$

אינטואיציה: A יותר קלה מ-B -
אם אפשר לפתור את B,
אפשר לפתור את A.

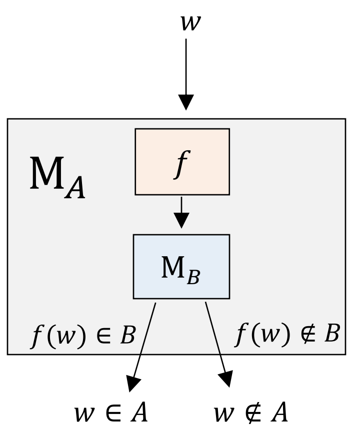
משפט הרדוקציה: אם $A \leq_m B$ ו-$B \in \mathrm{R}$ אז $A \in \mathrm{R}$.

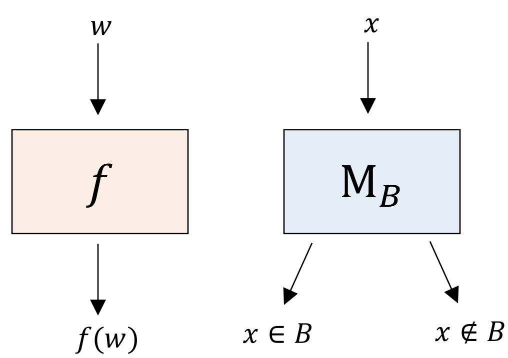
הוכחה: נבנה מ"ט M_A שמכריעה את A.

<u>M_A תפעל כך:</u>

תהי f פונקציה ניתנת לחישוב שמעידה ש-$A \leq_m B$.

בהינתן קלט w, תחשב את $f(w)$ ותריץ את M_B (המכונה שמכריעה את B) על $f(w)$ ותענה כמוה.





מסקנה חשובה: אם $A \leq_m B$ ו-$A \notin \mathrm{R}$ אז $B \notin \mathrm{R}$.

דוגמאות

1. $HALT_{TM} \notin \mathrm{R}$

נראה $A_{TM} \leq_m HALT_{TM}$, ומכיוון שהוכחנו $A_{TM} \notin \mathrm{R}$ נסיק ש-$HALT_{TM} \notin \mathrm{R}$ -

אם היינו מצליחים להכריע את $HALT_{TM}$ היינו מצליחים להכריע את A_{TM}.

נראה: קלט ל$HALT_{TM} \longleftarrow$ קלט לA_{TM} $f:$ כך ש $f(<\mathrm{M}>, w) = (<\mathrm{M}'>, w')$

כך ש-M מקבלת את w אמ"מ M' עוצרת על w'.

f תפעל כמו הפונקציה בדוגמה 2. כש-M הולכת ל-q_{rej} אז M' הולכת ל-q_{loop}, $w = w'$.

אם M קיבלה את w אז M' תעצור על w.

אם לא, יש שתי אפשרויות –

- M נתקעה ואז גם M'.
- M הגיעה ל-q_{rej} אז M' הולכת ל-q_{loop}.

2. $HALT_{TM}^{\varepsilon} = \{<\mathrm{M}>: \mathrm{M}\ halts\ on\ \varepsilon\} \notin \mathrm{R}$ (עוצרת על הסרט הריק)

נראה ש-$HALT_{TM} \leq_m HALT_{TM}^{\varepsilon}$ ונסיק $HALT_{TM}^{\varepsilon} \notin \mathrm{R}$.

רוצים: מ"ט f: מ"ט + מילה ⟶ מ"ט כך ש $f(<\mathrm{M}>, w) = \mathrm{M}'$ היא כזו ש-M' עוצרת על הסרט הריק אמ"מ M עוצרת על w.

<u>M' תפעל כך:</u>

כותבת w על הסרט הריק, חוזרת עם הראש הקורא לתחילת הסרט ומריצה את M.

ומתקיים -M' עוצרת על הסרט הריק $\Leftrightarrow$ M עוצרת על w.

3. $INF_{TM} = \{<\mathrm{M}>: \text{אינסופית } L(\mathrm{M})\} \notin \mathrm{R}$

$A_{TM} \leq_m INF_{TM}$.

נראה פונקציה מ"ט f: מ"ט + מילה ⟶ מ"ט כך ש $f(<\mathrm{M}>, w) = \mathrm{M}'$ מקיימת:

- אם M מקבלת את w אז $L(\mathrm{M})$ אינסופית.
- אם M לא מקבלת את w אז $L(\mathrm{M})$ סופית.

<u>M' פועלת כך:</u>

בהינתן $x \in (0+1)^*$, M' מריצה את M על w (מתעלמת מ-x), ועונה כמוה.

אם M מקבלת את w אז M' תקבל את כל ה-$x \in (0+1)^*$, $L(\mathrm{M}) = (0+1)^*$, אז $\mathrm{M}' \in INF_{TM}$.

- הפונקציה f (שמחשבת את M' בהינתן M ו-w) ניתנת לחישוב:

התהליך בו בהינתן M ו-w כותב את M' עוצר תמיד. העובדה שייתכן ש-M לא עוצרת על w לא מטרידה אותנו.

4. $REG_{TM} = \{<\mathrm{M}>: \text{רגולרית } L(\mathrm{M})\} \notin \mathrm{R}$

$A_{TM} \leq_m REG_{TM}$.

מ"ט מעל (0, 1) f: מ"ט + מילה ⟶ מ"ט בהינתן M ו-w, f מחזירה M' כך ש-$L(\mathrm{M}')$ רגולרית אמ"מ M מקבלת את w.

<u>M' פועלת כך:</u>

בהינתן $x \in (0+1)^*$ אם $x \in (0^n 1^n : n \geq 0)$, M' מקבלת.

אחרת, M' מריצה את M על w ומשיבה כמוה.

מתקיים:

אם M מקבלת את w אז $\mathrm{M}' \in REG_{TM} \Leftarrow L(\mathrm{M}') = (0+1)^*$

אם M לא מקבלת את w אז $\mathrm{M}' \notin REG_{TM} \Leftarrow L(\mathrm{M}') = (0^n1^n : n \geq 0)$

רדוקציות – בעיית הריצוף

קלט:

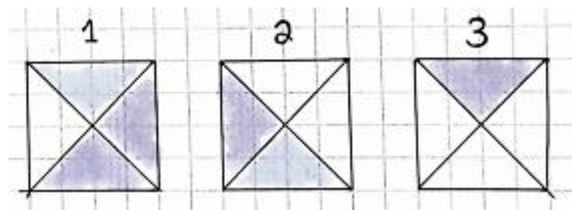
- T – קבוצה סופית של אריחים.
- $\mathrm{H}, \mathrm{V} \subseteq \mathrm{T} \times \mathrm{T}$.

V = vertical condition – רשימת זוגות שמספרת איזה אריח יכולה לבוא מעל אריח.

H = horizontal condition – תנאי שכנות. רשימה של זוגות כך שניתן לשים אריח אחד במאונך לשני.

- $t_{init} \in \mathrm{T}$

<u>דוגמה:</u>



$H = \{(2,1), (2,1), (2,3), (3,1)\}$ ניתן לשים את אריח 2 במאונך לאריח 1.

$V = \{(1,2), (2,3), (3,1)\}$ אפשר לשים את 1 מעל 3.

$t_{init} = 3$

פלט:

האם יש ריצוף חוקי $n \times n$ לכל $n \geq 1$?

<u>ריצוף חוקי $n \times n$</u> – פונקציה $f: \{1, \dots, n\} \times \{1, \dots, n\} \longrightarrow \mathrm{T}$ כך ש:

- $f(1,1) = t_{init}$
- תנאי שכנות במאונך - לכל $1 \leq i < n, 1 \leq j \leq n$

$H\big(f(i,j), f(i+1,j)\big)$

- תנאי שכנות במאוזן - לכל $1 \leq i \leq n, 1 \leq j < n$

$V\big(f(i,j), f(i,j+1)\big)$

<u>מהדוגמה:</u>

3				
2	3			
1	2	3		
3	1	2	3	

השפה: $TILE = \{T, H, V, t_{init} :$ יש ריצוף חוקי $n \times n$ לכל $1 \le n\}$

נשים ♥ $TILE \in coRE$ – יש מ"ט שמזהה קלטים שאינם ב-$TILE$.

<u>נוכיח באמצעות רדוקציה ש-$TILE \notin \mathrm{RE}$</u>

נראה רדוקציה $\overline{HALT^{\varepsilon}_{TM}} \le_m TILE$.

$$HALT^{\varepsilon}_{TM} = \{<\mathrm{M}>: \mathrm{M} \text{ עוצרת על הסרט הריק}\} \in \mathrm{RE}$$

$$HALT_{TM} \in \mathrm{RE}$$

למה?

- ראינו ברדוקציה $A_{TM} \le_m HALT_{TM}$ ש-$HALT_{TM} \notin R$.
- $HALT_{TM} \le_m HALT^{\varepsilon}_{TM}$ אז נרצה פונקציה $f(<\mathrm{M}>, w) = \mathrm{M}'$ כך ש-M' עוצרת על הסרט הריק אמ"מ M עוצרת על w. וראינו? $HALT^{\varepsilon}_{TM} \notin \mathrm{R} \Leftarrow A_{TM} \le_m A^{\varepsilon}_{TM}$.

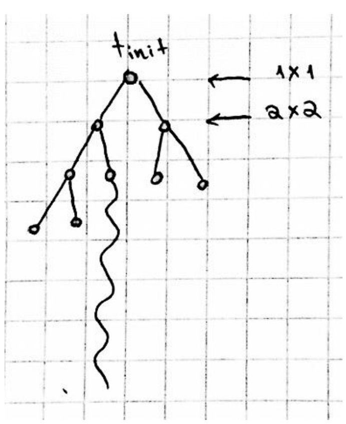
נראה:

קלטים ל-$TILE$ ⟶ קלטים ל-$\overline{HALT^{\varepsilon}_{TM}}$:f ⇐ $f(<\mathrm{M}>) =< \mathrm{T}, H, V, t_{init} >$

כך ש-M לא עוצרת על הסרט הריק ⇔ $< \mathrm{T}, H, V, t_{init} >$ מאפשרים ריצוף חוקי $n \times n$ לכל $n \ge 1$.

מסקנות:

1. $TILE \notin \mathrm{R}$
2. $TILE \notin \mathrm{RE}$ - נובע ממסקנה 1 + $TILE \in \mathrm{coRE}$, ואנחנו יודעים $\mathrm{RE} \cap \mathrm{coRE} = \mathrm{R}$.



<u>**למה:** יש ריצוף חוקי $\mathrm{n} \times \mathrm{n}$ לכל $\mathrm{n} \ge 1$ אמ"מ יש ריצוף חוקי לכל רבע המישור $f: \mathbb{N} \times \mathbb{N} \longrightarrow \mathrm{T}$.</u>

הוכחה:

⇒ קל.

⇐ נובע מ**הלמה של קניג** – בעץ אינסופי בו לכל קדקוד יש דרגת פיצול סופית, יש מסלול אינסופי.

ההוכחה תהיה קניג על עץ הריצופים הסופיים.

הרעיון:

ריצה של מכונת טיורינג שלא עוצרת תהיה מתוארת ע"י:

...	...	...						
a	a	a	q'a	b	a			
a	a	qb	a	b	a			
						...	...	...

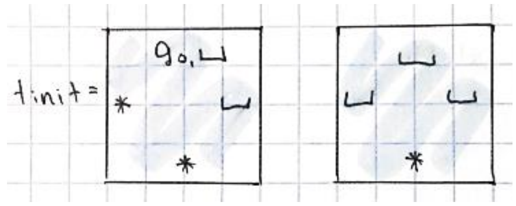
→ תיאור קונפיגורציה

$\delta(q, b) = (q', a, R)$

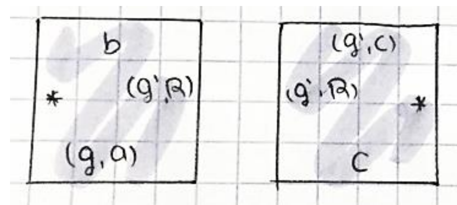
כל קונפיגורציה תהיה שורה בריצוף, ואם מ"ט לא תעצור על הסרט אז יהיה ריצוף אינסופי.

סוגי הבלטות:

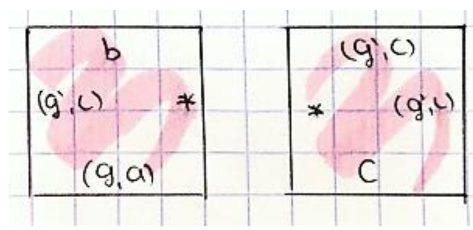
1. אריחי השורה הראשונה.



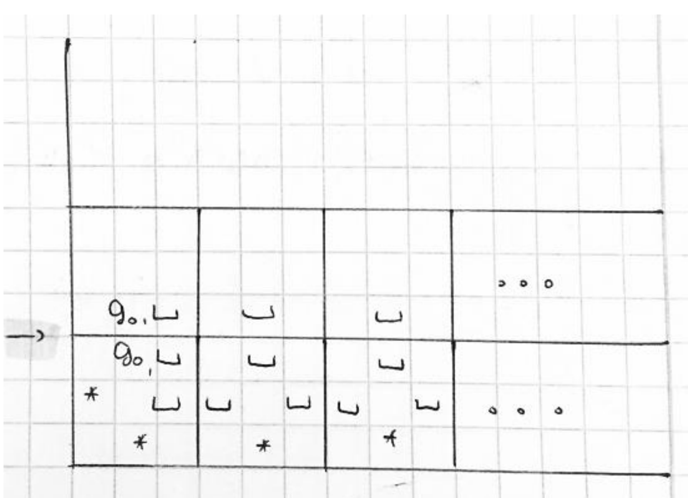
2. R – לכל מעבר $\delta(q,a)=(q',b,R)$ יש אריחים:



L – לכל מעבר $\delta(q,a)=(q',b,L)$ יש אריחים:



~ המשך בשבוע הבא ~



~ תזכורת ~

רצינו להראות רדוקציה $\overline{HALT^{\varepsilon}_{TM}} \leq_m TILE$, כך ש-

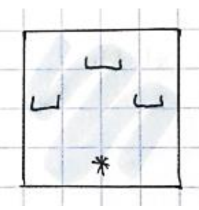
קלטים ל-$TILE$ $\longrightarrow$ מ"ט: f ⇐ אם $f(<\mathrm{M}>) =< \mathrm{T}, H, V, t_{init} >$, M לא עוצרת על הסרט הריק ⇔ יש ריצוף חוקי לרבע הראשון.

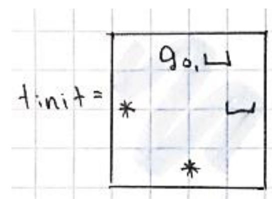
ראינו $TILE \in \mathrm{coRE}$.

הרעיון - כל קונפיגורציה תהיה שורה בריצוף, ואם מ"ט לא תעצור על הסרט הריק אז יהיה ריצוף אינסופי.

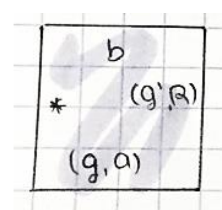
<u>סוגי הבלטות:</u>

3. אריחי השורה הראשונה:

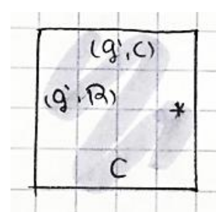




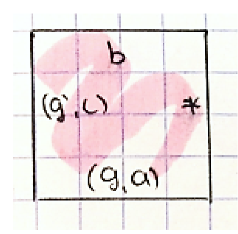
4. R – לכל מעבר $\delta(q,a) = (q', b, R)$, $q \neq \{q_{acc}, q_{rej}\}$:



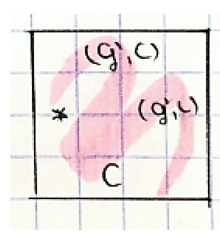
+ לכל $c \in \Gamma$:



L – לכל מעבר $\delta(q,a) = (q', b, L)$, $q \neq \{q_{acc}, q_{rej}\}$:

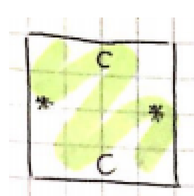


+ לכל $c \in$



Γ:

5. לכל $c \in \Gamma$: (מתאים למצב בו לא קורה כלום)



<u>דוגמה:</u>

מ"ט עם מצב מעבר יחיד: $\delta(q_0, \_\_) = (q_0, b, R)$

ריצה על הסרט הריק:

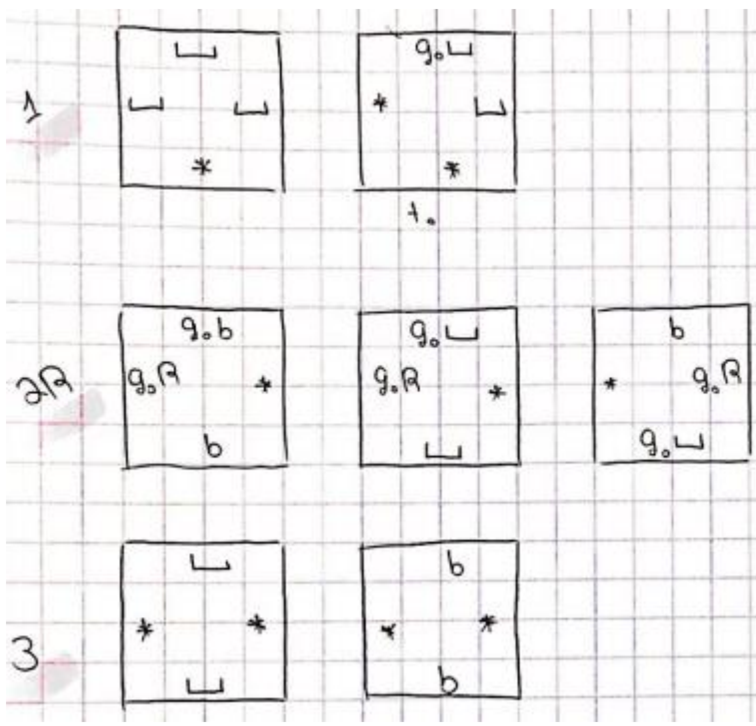
קונפיגורציה התחלתית $\rightarrow$ $q_0, \_\_, \_\_, \_\_, \_\_, \_\_, \ldots$

הקונפיגורציה הבאה $\rightarrow$ $b, q_0, \_\_, \_\_, \_\_, \_\_, \ldots$

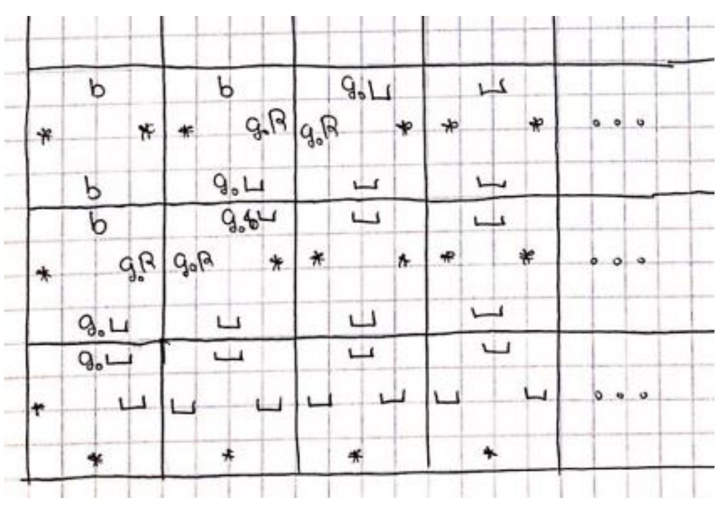
$\rightarrow$ $b, b, q_0, \_\_, \_\_, \_\_, \ldots$

המכונה לא תעצור על הסרט הריק.

האריחים שתייצר הרדוקציה נראים כך:



נראה שיש ריצוף חוקי של רבע המישור:



M לא עוצרת על ε $\Leftarrow$ יש ריצוף חוקי אינסופי.

סדרת הקונפיגורציות האינסופית משרה ריצוף אינסופי.

יש ריצוף חוקי אינסופי $\Leftarrow$ יש ריצה אינסופית $\Leftarrow$ M לא עוצרת.

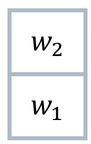
למה:

0. קומה 1 מקודדת את הקונפיגורציה ההתחלתית.
1. כל קומה מקודדת קונפורמציה – בכל קומה רק בלטה אחת בה יש מצב.
2. קומה $i+1$ מקודדת קונפורמציה עוקבת לזו שמקודדת בקומה i.

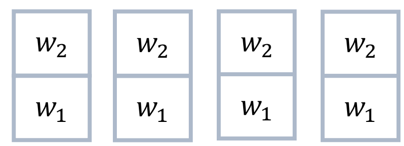
בעיות נוספות

PCP – post correspondence problem

קלט: אוסף אבני דומינו כאשר בכל אבן יש שתי מילים $w_1, w_2 \in \Sigma^*$:

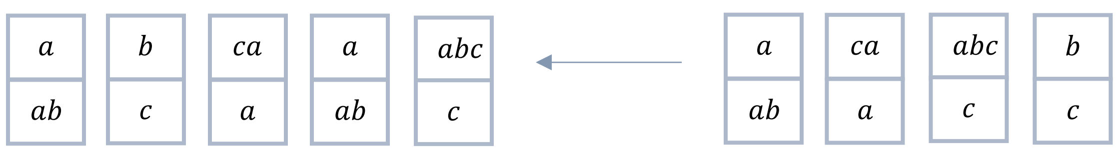


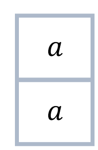
דוגמה:



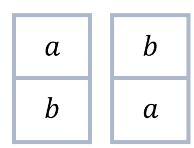
פלט: האם ניתן לארגן match. הרצף בשורה העליונה שווה לרצף בשורה התחתונה.

דוגמאות:





פלט: כן



פלט: לא

$$PCP \in RE$$

A_1 A_2 אוטומטים $\quad L = \{< A_1 >< A_2 > :\ L(A_1) \subseteq L(A_2)\} \in \mathrm{R}$

נשים לב ש-$L \subseteq \mathrm{coRE}$, ונוכל לבדוק האם $L(A_1) \cap \overline{L(A_2)} = \emptyset$.

רדוקציות נוספות

$A_{TM} \leq_m REG_{TM}$ ⇐ $REG_{TM} \notin \text{coRE}$ ⇐ כדי להראות $REG_{TM} \notin \text{RE}$ נראה $A_{TM} \leq_m \overline{REG_{TM}}$.

נראה $f(<\text{M}>, w) = <\text{M}'>$ כך ש-M מקבלת את w אמ"מ M' איננה רגולרית.

<u>M' על קלט x תפעל כך:</u>

נראה שאם M מקבלת את w ← $L(\text{M}') = \{0^n1^n : n \geq 0\}$, ואם M לא מקבלת את w ← $L(\text{M}') = \emptyset$

- אם $x \in \{0^n1^n : n \geq 0\}$ אז תריץ את M ותקבל כמוה.
- אם $x \notin \{0^n1^n : n \geq 0\}$ אז M' דוחה.

$INF_{TM} = \{\text{M}: L(\text{M})$ אינסופית$\}$, נראה $HALT_{TM} \leq_m \overline{INF_{TM}}$ ומכך נסיק $INF_{TM} \notin \text{RE}$.

נראה $f(<\text{M}>, w) = <\text{M}'>$ כך ש-$L(\text{M}')$ סופית אמ"מ M עוצרת על w.

<u>M' על קלט x תפעל כך:</u>

- הרץ את M על w $|x|$ צעדים.
- אם M עצרה על w במהלך x הצעדים, דחה.
- אחרת, קבל.

$<\text{M}, w> \in HALT_{TM}$ ⇐ קיים $l \geq 0$ כך ש-M יוצרת על w תוך l צעדים ⇐ M' תקבל את כל המילים באורך לכל היותר l ⇐

$$L(M') = \begin{cases} \Sigma^{<l}, & \text{M עוצרת על } w \text{ תוך } l \text{ צעדים} \\ \Sigma^*, & \text{M לא עוצרת} \end{cases}$$

⇐ $L(\text{M}')$ סופית אמ"מ M עוצרת על w.

סיבוכיות

הקדמה

נרצה לעשות סיווגים לשפות ב-R.

נראה את המשאבים הדרושים להכרעת השפה:

- זמן
- זיכרון
- אקראיות
- תקשורת

ניתוח סיבוכיות של אלגוריתמים

<u>דוגמה:</u>

נרצה למצוא מ"ט שתכריע את השפה $L = \{0^n1^n : n \geq 0\}$.

בהינתן $w \in (0+1)^*$:

1. סרוק את הסרט וודא שהוא ב-0^*1^*. $O(n)$
2. כל עוד יש 0ים ו-1ים, מחק 0 ראשון ו-1 ראשון. $O(n)$ איטרציות, כל איטרציה $O(n)$.
3. אם ה-0ים וה-1ים הסתיימו יחד, קבל. אחרת, דחה.

סה"כ $O(n^2)$ ניתן להכריע גם ב-$O(nlogn)$.

משפט: אם L ניתנת להכרעה ב-$O(nlogn)$, אז L רגולרית.

מחלקת סיבוכיות זמן

עבור פונקציה $t: \mathbb{N} \longrightarrow \mathbb{N}$ **מחלקת סיבוכיות הזמן**:

$$\mathrm{TIME}\big(t(n)\big) =$$

{L: L ניתנת להכרעה ע"י מ"ט דטרמיניסטית בעלת סרט יחיד העוצרת על כל קלט תוך $O\big(t(n)\big)$ צעדים}

$$\{0^n1^n : n \geq 0\} \in TIME(nlogn)$$

מכונת טיורינג לא דטרמיניסטית

$$\mathrm{M} = < \Sigma, \Gamma, Q, Q_0, \delta, q_{acc}, q_{rej} >$$

$Q_0 \subset Q$ קבוצת מצבים התחלתיים.

$$\delta: Q \times \Gamma \longrightarrow 2^{Q \times \Gamma \times \{L,R\}}$$

- מ"ט אי דטרמיניסטית M **מכריעה** את L אם M עוצרת על כל מילה בכל חישוביה, ומקבלת בדיוק את כל המילים ב-L.
- בעץ ריצה על L אין ענף אינסופי.

זמן ריצה של M על w הוא מספר הצעדים בחישוב הכי ארוך (גם אם הוא דוחה).

$$\mathrm{TIME}\big(t(n)\big) =$$
$\{L$ ניתנת להכרעה ע"י מ"ט **דטרמיניסטית** בעלת סרט יחיד העוצרת על כל קלט תוך $O\big(t(n)\big)$ צעדים $:L\}$

$$\mathrm{NTIME}\big(t(n)\big) =$$
$\{L$ ניתנת להכרעה ע"י מ"ט **אי דטרמיניסטית** בעלת סרט יחיד העוצרת על כל קלט תוך $\underbrace{O\big(t(n)\big)}_{\text{חסם על החישוב הארוך ביותר}}$ צעדים $:L\}$

משפט: תהי $t: \mathbb{N} \longrightarrow \mathbb{N}$ פונקציה המקיימת $t(n) \geq n$.

א. לכל מ"ט דטרמיניסטית עם k סרטים הרצה בזמן $\mathrm{O}\big(t(n)\big)$, יש מ"ט דטרמיניסטית שקולה עם סרט יחיד שרצה בזמן $O\big(t^2(n)\big)$.

ב. לכל מ"ט אי דטרמיניסטית בעלת סרט יחיד הרצה בזמן $O\big(t(n)\big)$, יש מ"ט דטרמיניסטית שקולה בעלת סרט יחיד הרצה בזמן $2^{O(t(n))}$.

המחלקות P ו-NP

$$\mathrm{PTIME} = \bigcup_k TIME\ (n^k)$$

P (**PTIME**) – בעיות שניתן להכריע בזמן פולינומיאלי.

(מסלול אוילר, עץ פורש מינימלי, מיון...)

$$\mathrm{NPTIME} = \bigcup_k NTIME\ (n^k)$$

NP (**NPTIME**) – בעיות שניתנות להכרעה בזמן פולינומיאלי ע"י מכונה אי דטרמיניסטית.

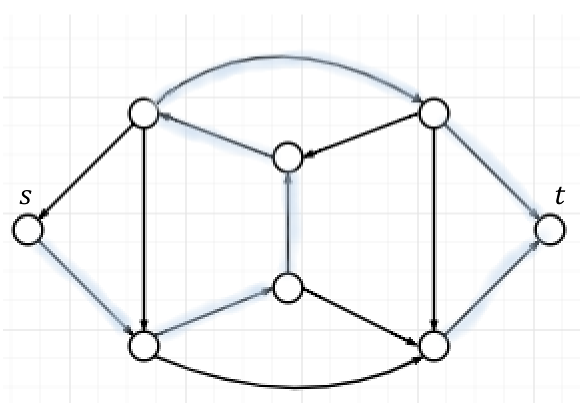
$$\mathrm{EXPTIME} = \bigcup_k NTIME\ (2^{n^k})$$

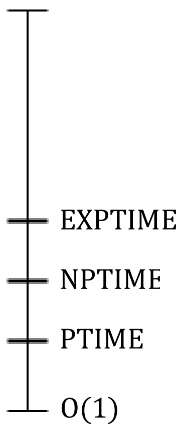
ניתנות להכרעה בזמן אקספוננציאלי.

- $\mathrm{PTIME} \subseteq \mathrm{NPTIME} \subseteq \mathrm{EXPTIME}$ לפי המשפט.

<u>דוגמה 1:</u> **מסלול המילטוני בגרף.** מסלול העובר בכל קדקודי הגרף, בכל קדקוד בדיוק פעם אחת.

$\mathrm{D\text{-}ST\text{-}HAMPATH} = \{< G, s, t >:$ יש מסלול המילטוני מ-s ל-t$\}$





בהינתן בעיה, נרצה למצוא -

- **חסם עליון:** אלגוריתם.
- **חסם תחתון:** אי אפשר יותר טוב.
- **חסם הדוק:** כשהעליון והתחתון מתלכדים.

<u>מה הסיבוכיות של D-ST-HAMPATH?</u>

1. D-ST-HAMPATH ∈ EXPTIME.

בהינתן $< G, s, t >$ המכונה תעבור על כל המסלולים מאורך n ($|V| = n$) ותבדוק את המילטוניותם של המסלולים מ-s ל-t.

2. D-ST-HAMPATH ∈ NP.

בהינתן $< G, s, t >$, נניח ש-$V = \{1, .., n\}$ $G =< V, E >$.

המכונה תפעל כך:

2.1 נחש (יש למכונה מעברים אי דרטרמיניסטים) סדרה $p_1, \dots, p_n$ של מספרים מהקבוצה $\{1, .., n\}$.

2.2 אם יש מספר שמופיע פעמיים, דחה.

2.3 אם $p_1 \neq s \vee p_n \neq t$, דחה.

2.4 לכל $1 \leq i \leq n - 1$ אם $\neg E(p_i, p_{i+1})$, דחה.

2.5 קבל.

נשים ❤ - קשה (לא הצלחנו בזמן פולינומיאלי): להכריע האם $< G, s, t >$ שייך ל-D-ST-HAMPATH.

קל (פולינומיאלי): לוודא שפתרון נתון עבור D-ST-HAMPATH הוא נכון.

<u>דוגמה 2:</u> $\text{COMPOSIME} = \{x : x = p \cdot q \text{ כך ש } p, q > 1 \text{ קיימים}\} \subseteq \mathbb{N}$, x נתון בבסיס בינארי.

נשים ❤ - אם x היה נתון בבסיס בינארי, אז השפה ב-P. כי כשנעבור ונבדוק האם יש $1 < q \leq \sqrt{x}$ שמחלק בלי שארית את x ← פולינומיאלי ב-x. לגיטימי באורך הקלט.

COMPOSIME ∈ NP, המכונה תנחש q ותבדוק האם $x \bmod q = 0$.

מוודא

ראינו:

$\text{PTIME} = \bigcup_{k\geq 1} TIME\ (n^k)$ - קל לפתור

$\text{NPTIME} = \bigcup_{k\geq 1} NTIME\ (n^k)$ - קל לוודא שפתרון נתון הוא אכן פתרון

מוודא (verified) עבור שפה $L \subseteq \Sigma^*$ הוא מ"ט דטרמיניסטית V כך ש-

$$L = \{w: \text{כלשהו } c \in \Sigma^* \text{ עבור } < w,c > \text{ מקבלת את } V\}$$

כאשר c נקרא **certificated - עד**.

<u>סיבוכיות המוודא נמדדת ביחס ל-w:</u>

מוודא פולינומיאלי – רץ על $< w,c >$ בזמן פולינומיאלי ב-$|w|$.

$\Leftarrow$ c צריך להיות פולינומיאלי ב-w.

הגדרה אלטרנטיבית למוודא פולי' -

$$L = \{w: \text{בזמן ריצה פולינומיאלי } \text{w} - \text{פולינומיאלי ב } c \in \Sigma^* \text{ עבור } < w,c > \text{ מקבלת את } V\}$$

<u>דוגמאות:</u>

1. מוודא עבור D-ST-HAMPATH: מ"ט דטרמיניסטית המקבלת $< \underbrace{< G,s,t >}_{w}, \underbrace{\pi}_{c} >$ אמ"מ π מסלול המילטוני מ-s ל-t ב-G. אכן $\text{D-ST-HAMPATH } = \{w: \text{כלשהו } \pi \text{ עבור } << G,s,t >,\pi > \text{ מקבלת את } V\}$.
המוודא פולינומיאלי.

2. $\text{COMPOSITE} = \{x : x = p \cdot q \text{ כך ש } p,q > 1 \text{ קיימים}\}$.
אמרנו ש-x נתון בבינארי.
אם היה נתון באונרי, יש x 1-ים, אז אם בסרט הקלט כתובים x 1-ים מותר לעשות מספר פולי' של פעולות שמכריע ב-x, והפרוצדורה הבאה פולי':

$read(x)$:
  $for\ i = 1, \dots, x$:
    $print\ "*"$

אם x נתון לא באונרי, למשל בבסיס 10, הפרוצדורה אקספוננציאלית.

אם למשל הקלט יהיה 1,000,000 הפרוצדורה תבצע 10^6 צעדים.

- מוודא עבור COMPOSITE: יקבל את $< x,p >$ אם $p \neq 1$ ו-$x \bmod p = 0$ בזמן פולינומיאלי.

משפט: $L \in \text{NP} \Leftrightarrow$ יש ל-L מוודא פולינומיאלי.

$\Longrightarrow$ נניח שיש V דטרמיניסטית הרצה בזמן פולי' כך ש-

$$L = \{w: \text{w} - \text{ב}\ \text{פולי}'\ c \in \Sigma^*\ \text{עבור}\ < w, c >\ \text{מקבלת את}\ V\}$$

מ"ט אי דטרמיניסטית שמכריעה את L בזמן פולי' תפעל כך:

בהינתן w, תנחש עד c (רק באורך פולי'), ותאכיל את V ב-$< w, c >$.

אם V תקבל את אחד החישובים, אכן $w \in L$.

הראינו ש-$L \in \text{NP}$.

$\Longleftarrow$ $L \in \text{NP}$ אז יש מ"ט אי דטרמיניסטית M שמכריעה את L בזמן פולי'.

לכל $w \in L$ יש ריצה מקבלת r (סדרה של קונפיגורציות) של M על w.

V תקבל את $< w, c >$ אם c ריצה מקבלת של M על w, והיא אכן פולינומיאלית.

- ראינו $\text{P} \subseteq \text{NP} \subseteq \text{EXPTIME}$.
- יודעים $\text{P} \neq \text{EXPTIME}$.
- אז אחת ההכלות היא הכלה ממש, לא יודעים איזו.

שלמות ב-NP

שפה L היא **NP-שלמה** אם $^{(1)}$ $L \in \text{NP}$ $^{(2)}$ נצליח למצוא אלגוריתם פולי' עבור L. ינבע מזה ש-$\text{P} = \text{NP}$.

<u>נובע מההגדרה:</u>

1. כדי להוכיח $\text{P} = \text{NP}$, די למצוא שפה אחת L שהיא NP-שלמה ולהוכיח ש-$L \in \text{P}$.
2. כדי לקבל מוטיבציה לאלגוריתם לא פולינומיאלי/קירוב עבור L, די להוכיח ש-L היא NP-שלמה (כי מאמינים $\text{P} \neq \text{NP}$).

משפט קוק לוין: $\text{P} = \text{NP} \Leftrightarrow 3\text{SAT} \in \text{P}$

3SAT – ספיקות של נוסחאות מהצורה 3CNF.

רדוקציות פולינומיאליות

נאמר ש-$B \leq_p A$ ($A \subseteq \Sigma^*$) ניתנת לרדוקציה פולי' ל-$B \subseteq \Sigma^*$) אם קיימת $f: \Sigma^* \longrightarrow \Sigma^*$ ניתנת לחישוב <u>בזמן פולינומיאלי</u> ולכל $w \in \Sigma^*$ $w \in A \iff f(w) \in B$

משפט הרדוקציה: אם $B \in P$ ו-$A \leq_p B$ אז $A \in B$

הוכחה: מ"ט דטרמיניסטית שמכריעה את A בזמן פולי' תפעל כך:

בהינתן $w \in \Sigma^*$, תחשב את $f(w)$ ותאכיל את המכונה של B ב-$f(w)$.

נשים ♥, $|f(w)|$ פולי' ב-$|w|$.

המחלקה NP-complete – שפה L היא $\mathrm{NP}\text{-}C$ (NP-שלמה) אם:

1. $L \in \mathrm{NP}$ (חסם עליון)
2. L היא NP-HARD (חסם תחתון): לכל $L' \in \mathrm{NP}$ $L' \leq_p L$.

נשים ♥, אם L היא NP-קשה ו-$L \in \mathrm{P}$ אז $P = \mathrm{NP}$.

<u>הוכחה:</u> $\mathrm{P} \subseteq \mathrm{NP}$ תמיד. בנוסף $\mathrm{NP} \subseteq \mathrm{P}$ כי בהינתן $L' \in \mathrm{NP}$ נכריע אותה בזמן פולי' ע"י הורדתה (רדוקציה ממנה) ל-L (ממשפט הרדוקציה).

דוגמה לרדוקציה פולינומיאלית: $\mathrm{3SAT} \leq_p \mathrm{CLIQUE}$

3SAT – ספיקות של נוסחאות ב-3CNF.

- <u>משתנים:</u> $X = \{x_1, \dots, x_n\}$
- <u>ליטרלים:</u> משתנה x או שלילתו $\bar{x}$.
- <u>פסוקיות:</u> $\vee$ על מס' ליטרים, למשל: $x_1 \vee x_2 \vee \overline{x_2}$.
- <u>נוסחה ב-CNF:</u> $\wedge$ על מס' פסוקיות, למשל $\varphi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$

3CNF – בכל פסוקית יש שלושה ליטרלים.

$$\mathrm{3SAT} = \{< \varphi > :\ \text{נוסחה ספיקה ב} - \mathrm{3CNF}\ \varphi\}$$

עבור הדוגמה $(\overline{x_1} \vee \overline{x_1} \vee \overline{x_2}) \wedge (x_1 \vee x_2 \vee \overline{x_2})$,

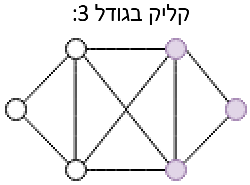
עד קצר יהיה השמה מספקת - $\begin{cases} f(x_1) = \mathbb{F} \\ f(x_2) = \mathbb{T} \end{cases}$

CLIQUE – עבור גרף לא מכוון $G = < V, E >$, קליקה בגרף היא $U \subseteq V$ כך ש-$E(v_1, v_2)$ לכל $v_1, v_2 \in U$.

$$CLIQUE = \{< G, k >:\ \text{יש ב} - G\ \text{קליק בגודל}\ k\}$$

- $k \leq |v|$, לא משנה אם נתון באונרי או בבינארי.

קליק בגודל 3:



נרצה פונקציה שבהינתן נוסחה φ תייצר $< G, k >$ בזמן פולי'.

$$\begin{array}{ccc} \mathrm{3SAT} & \leq_p & \mathrm{CLIQUE} \\ \varphi & \longrightarrow & < G, k > \end{array}$$

קל לראות, $\mathrm{CLIQUE} \leq_m \mathrm{3SAT}$. בהינתן φ נבדוק האם ספיקה (ב-R) ונדע להחזיר גרף ומספר בהתאם.

<u>הרדוקציה הפולינומיאלית:</u>

תהי $\varphi = (\ell_1^1 \vee \ell_1^2 \vee \ell_1^3) \wedge (\ell_2^1 \vee \ell_2^2 \vee \ell_2^3) \wedge \ldots \wedge (\ell_m^1 \vee \ell_m^2 \vee \ell_m^3)$ בעלת m פסוקיות.

נבנה $< G, k >$ כך ש-φ ספיקה אמ"מ יש ב-G k-קליק!

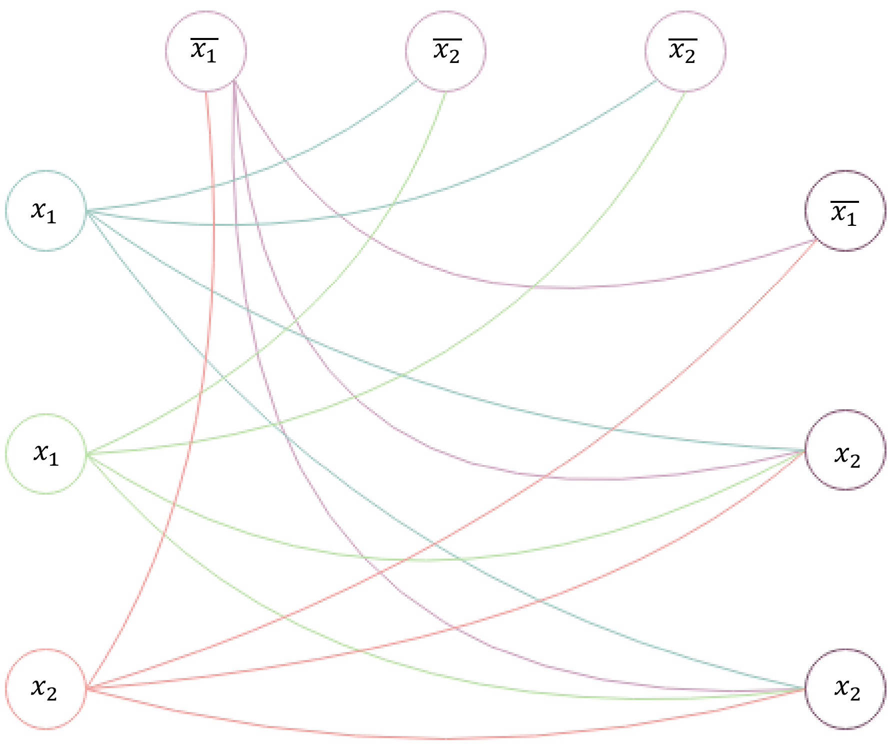
- הקדקודים של G:

  $V = \{\ell_1^1, \ell_1^2, \ell_1^3, \ldots, \ell_m^1, \ell_m^2, \ell_m^3\}$ קבוצת כל הליטרלים, $|V| = 3m$.
- הקשתות של G:

  $V \times V \ \setminus \{(v_1, v_2)$: v_1 ו v_2 מזוהים על משתנה ושלילתו$\} \ \setminus$
  $\{(v_1, v_2)$: v_1 ו v_2 מזוהים עם ליטרלים באותה הפסוקית$\}$

<u>דוגמה:</u>

$$\varphi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (x_1 \vee x_2 \vee x_2)$$



** לא כל הצלעות צוירו.

דוגמה לרדוקציה פולינומיאלית: $3\text{SAT} \leq_p \text{CLIQUE}$

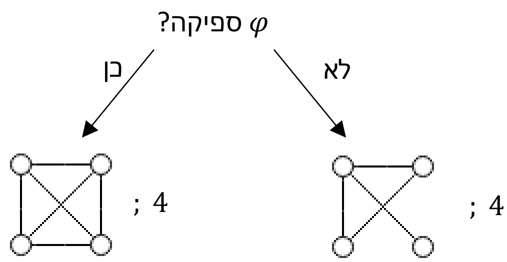
נראה דוגמה לרדוקציה אחרת.

תזכורת:

$$\varphi = C_1 \wedge C_2 \wedge \ldots \wedge C_m \qquad C_j = \ell_j^1 \vee \ell_j^2 \vee \ell_j^3 \qquad X = \{x_1, \ldots, x_n\} \qquad < G, k >$$

$f: X \longrightarrow \{\mathbb{T}, \mathbb{F}\}$ ← פולינומיאלית כך ש-φ ספיקה $\Leftrightarrow$ יש ב-G k קליק

<u>דוגמה לרדוקציה לא פולינומיאלית:</u>



C_j היא מעל שלושה משתנים $X_j = \{x_j^1, x_j^2, x_j^3\}$.

יש לכל היותר 8 השמות אמת ל-X_j, 7 מתוכן מספקות את C_j.

נגדיר את F_j בתור הקבוצה של 7 השמות אלה.

<u>הרדוקציה:</u>

$\boldsymbol{G} =< V, E > \qquad V = \bigcup_j F_j \longrightarrow$ $7m$ קדקודים

$E = \{(u_1, u_2):$ u_1 ו – u_2 השמות עקביות$\}$

$\boldsymbol{k} = m$

השמה עקבית – אין משתנה שגם u_1 וגם u_2 מתייחסות אליו, ומקבל ערך שונה בהן.

נשים ❤ שהרדוקציה פולי' - $|V| = 7m$, $|E| \leq |V|^2$, והחישוב של k, E, V קל.

<u>נכונות:</u> יש השמה מספקת ל-φ $\Leftrightarrow$ יש ב-G k קליק.

$\Leftarrow$ נניח ש-$\varphi \in 3\text{SAT}$, תהי $f: X \longrightarrow \{0,1\}$ השמה שמספקת את φ.

בכל פסוקית C_j יש קדקוד אחד u_j שמסכים עם f, כלומר לכל $x \in X_j$ מתקיים $u_j(x) = f(x)$.

נראה ש-$u = \{u_1, \ldots, u_n\}$ מהווה k קליק,

וזה כי ההשמות u_i, u_j ב-V עקביות עם f ולכן עקביות זו עם זו ולכן $(u_i, u_j) \in E$.

$\Rightarrow$ נניח שיש ב-G k קליק.

טענה א': אין קשתות בין קדקודים ב-F_j לכל $1 \leq j \leq m$.

(כי מדובר בהשמות שונות למשתנים ב-X_j)

מסקנה: לכל פסוקית C_j יש נציג אחד בקליק u_j.

טענה ב': ההשמות ב-$\{u_1, \dots, u_m\}$ עקביות (כי הקדקודים מחוברים בקשת).

מסקנה: ניתן להרחיב אותן להשמה אחת (לכל המשתנים ב-X) והשמה זו מספקת את φ.

(כי היא מורכבת מהשמות שמספקות את כל הפסוקיות)

$$\leftarrow \varphi \in 3SAT$$

Subset Sum

קלט: קבוצה $A = \{a_1, a_2, \dots, a_n\} \subseteq \mathbb{N}$ ומס' יעד $S \in \mathbb{N}$.

פלט: האם יש $B \subseteq A$ כך ש-$S = \sum_{a_i \in B} a_i$.

$$\text{SS} = \{< A, s >: \sum_{a_i \in B} a_i = S \text{ ו } B \subseteq A \text{ יש}\}$$

1. $\text{SS} \in \text{NP}$, בהינתן עד B ניתן לבדוק $B \subseteq A$ ו-$\Sigma B = S$ בזמן פולי'.
2. SS היא NP-קשה. נראה רדוקציה מ-$\text{3SAT} \leq_p \text{SS}$.

<u>הגדרנו:</u> L היא NP-קשה אם לכל $L' \in \text{NP}$, $L' \leq_p L$.

<u>שקול:</u> אם קיימת L' שהיא NP-קשה ו-$L' \leq_p L$ (שקול מטרנזיטיביות של רדוקציות).

Subset Sum

$$SS = \{< A, s >: \sum_{a_i \in B} a_i = S - \text{ו } B \subseteq A \text{ יש}\}$$

<u>נראה רדוקציה $3SAT \leq_p SS$:</u>

- n מספר המשתנים
- $X = \{x_1, \dots, x_n\}$
- m מספר הפסוקיות

נבנה $\mathbf{2n + 2m}$ **מספרים** שיהיו כל אחד בני $\mathbf{n + m}$ **ספרות**: (בבסיס 10)

לכל משתנה x_i יהיו שני מספרים: t_i, f_i.

- הספרה ה-i $(1 \leq i \leq n)$ של t_i ושל f_i היא 1, כל השאר 0.

הספרות יסמנו לנו על כל משתנה ושלילתו באיזה פסוקית מופיע:

- הספרה ה-$n + j$ של t_i עבור $1 \leq j \leq n$ היא 1 אם x_i מופיע חיובי בפסוקית C_j, אחרת 0.
- הספרה ה-$n + j$ של f_i עבור $1 \leq j \leq n$ היא 1 אם x_i מופיע שלילי בפסוקית C_j, אחרת 0.

לכל פסוקית C_j שני מספרים: p_j, q_j.

- לכל $1 \leq j \leq m$ ולכל $1 \leq i \leq n$ המספרים ה-i של p_j ושל q_j תהיה 0.
- לכל $1 \leq j' \leq m$ הספרה ה-$n + j'$ של p_j ושל q_j תהיה 1, השאר 0.

<u>טענה:</u> φ ספיקה אמ"מ יש תת קבוצה של A שסכומה S המוגדר כך:

הספרה ה-$1 \leq i \leq n$ היא 1

הספרה ה-$n + 1 \leq j \leq n + m$ היא 3

(בדוגמה 1,113,333)

הוכחה רשמית תעלה למודל.

<u>דוגמה:</u>

$$\varphi = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$$

14 מספרים, 7 ספרות בכל מספר.

	1	2	3	4 (פסוקית ראשונה)	5 (פסוקית שנייה)	6 (פסוקית שלישית)	7 (פסוקית רביעית)
t_1	1	0	0	1	0	0	1
f_1	1	0	0	0	1	1	0
t_2	0	1	0	1	0	1	0
f_2	0	1	0	0	1	0	1
t_3	0	0	1	1	1	0	1
f_3	0	0	1	0	0	1	0
p_1	0	0	0	1	0	0	0
q_1	0	0	0	1	0	0	0
p_2	0	0	0	0	1	0	0
q_2	0	0	0	0	1	0	0
p_3	0	0	0	0	0	1	0
q_3	0	0	0	0	0	1	0
p_4	0	0	0	0	0	0	1
q_4	0	0	0	0	0	0	1
S	**1**	**1**	**1**	**3**	**3**	**3**	**3**

שפה NP-קשה ראשונה

תזכורת: L כך שלכל $L' \in \mathrm{NP} \leftarrow L' \le_p L$.

$\{\mathrm{M}$ מכונת טיורנג דטרמיניסטית שמקבלת את w תוך t צעדים $:\mathrm{BA_{NTM}} = \{< \mathrm{M}, w, 1^t >$ $(bounded\ A_{NTM})$

- t נתון באונרית.

<u>$\mathrm{BA_{NTM}}$ היא NP-שלמה:</u>

1. $\mathbf{BA_{NTM} \in NP}$

בהינתן $< \mathrm{M}, w, 1^t >$ נריץ את M על w במשך t צעדים ונקבל אם M קיבלה את w.

2. $\mathbf{BA_{NTM} \in NP\text{-}HARD}$

לכל $L' \in \mathrm{NP}$ *מתקיים* $L' \le_p \mathrm{BA_{NTM}}$.

f ניתנת לחישוב בזמן פולי' כך שלכל $w \in \Sigma^*$ $\;f(w) \in \mathrm{BA_{NTM}} \iff w \in L'$.

$L' \in \mathrm{NP}$ אז יש מ"ט א"ד M שמכריעה את L' בזמן $p(n)$ עבור פולינום p (מניחים שנתון).

$$f(w) = < M, w, 1^{p(|w|)} >$$

הרדוקציה אכן פולי' והכל מסתדר. ☺

בעיית הריצוף החסום

$$\mathrm{BTILE} = \{\mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n\}$$

- T קבוצת אריחים.
- $\mathrm{H}, \mathrm{V} \subseteq \mathrm{T} \times \mathrm{T}$ תנאי שכנות במאוזן ובמאונך.
- $t_{init}, t_{fin} \in \mathrm{T}$.

קיים ריצוף חוקי $n \times n$:

$$f: \{1, \ldots, n\} \times \{1, \ldots, n\} \longrightarrow \mathrm{T}$$

$$f(1,1) = t_{init} \qquad f(1,n) = t_{fin}$$

<u>BTILE היא NP-שלמה:</u>

1. **$\mathbf{BTILE \in NP}$**

בהינתן $\mathrm{I} = < \mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n >$ ניתן לוודא בזמן פולי' בקלט שריצוף נתון $n \times n$ הוא חוקי.

2. **$\mathbf{BTILE \in NP\text{-}HARD}$**

נראה $\mathrm{BTILE} \le_p \mathrm{BA_{NTM}}$.

$$< \mathrm{M}, w, 1^t > \underbrace{\longrightarrow}_{f} < \mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n >$$

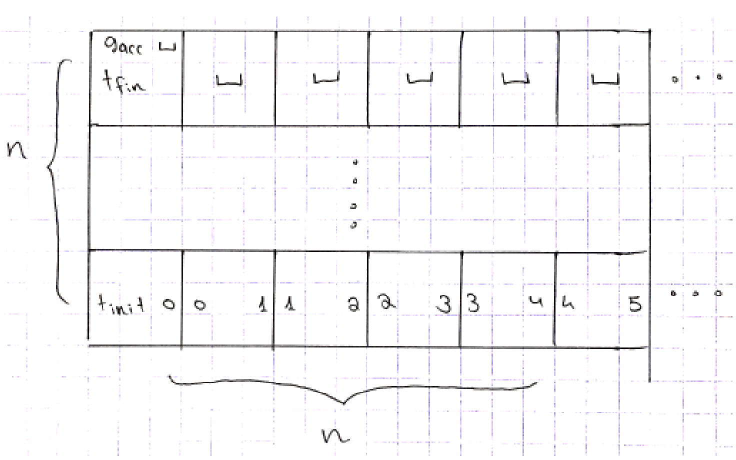
הבנייה תהיה כמו שראינו ברדוקציה $\overline{HALT^{\varepsilon}_{TM}} \le TILE$ עם השינויים הבאים:

- נניח של-M יש קונפ' מקבלת יחידה $q_{acc}, \_\_, \_\_, \_\_ \ldots$

_	_	_	...	_

q_{acc}

ההנחה לגיטימית כי כש-M באה לקבל, תעבור למצב שממנו מוחקים את הסרט, וזזים עם הראש הקורא שמאלה.



- הגדרת הבלטות עם מספרים.
- האריחים של הקומה שמקודדת את הקונפ' המקבלת יכולים לטפס ללא הגבלה.

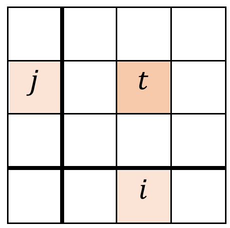
3SAT היא NP-שלמה

<u>3SAT היא NP-קשה</u>

נראה רדוקציה $3SAT \leq_p BTILE$.

בהינתן $I = < T, H, V, t_{init}, t_{fin}, 1^t >$ נבנה נוסחה φ ב-CNF כך ש- $I \in BTILE \iff \varphi \in CNF$

(אח"כ נעביר בזמן פולי' את φ ל-3CNF)



הרעיון:

לכל אריח $t \in T$ יהיו n^2 משתנים:

$x_{i,j,t}$ עבור $1 \leq i,j \leq n$.$t \in T$ יקבל ערך אמת $true$ אם $f(i,j) = t$.

<u>דוגמה:</u>

$$I = < \underbrace{\{a,b\}}_{T}, \underbrace{\{(a,b),(a,a)\}}_{H}, \underbrace{\left\{\binom{b}{a},\binom{a}{a}\right\}}_{V}, \underbrace{a}_{t_{init}}, \underbrace{a}_{t_{fin}}, 11 >$$

- האם קיים ריצוף 2×2? כן -

a	a
a	a

- $x_{1,1,a}$: האם $(1,1) = a$?
- $f(1,1,a) = \mathbb{T}$ ולא ייתכן שגם $f(1,1,b) = \mathbb{T}$
- $f(1,1,b) = \mathbb{F}$

<u>הנוסחה φ</u> - $\wedge$ של הנוסחאות הבאות:

א. לכל מיקום מותאם <u>לפחות</u> אריח אחד:

לכל $1 \leq i,j \leq n$ $\quad \theta_{ij} = \vee_{t \in T}\, x_{i,j,t}$

ב. לכל מיקום מותאם <u>לכל היותר</u> אריח אחד:

$$\theta'_{ij} = \wedge_{t \in T} \left(x_{i,j,t} \to \wedge_{t' \in T} \overline{x_{i,j,t'}}\right)$$

או באופן שקול (ב-CNF): $\theta'_{ij} = \wedge_{t \in T} \wedge_{t' \in T} \left(x_{i,j,t} \to \overline{x_{i,j,t'}}\right)$

$\leadsto$ א' + ב' מבטיחים לנו שהשמה מספקת משרה ריצוף.

כי השמה מספקת תתאים לכל קואורדינטה (i,j) רק אריח אחד ככה ש-$x_{i,j,t} = \mathbb{T}$ וכל השאר $\mathbb{F}$.

ג. התנאים על t_{init} ועל t_{fin} מתקיימים:

$$x_{1,1,t_{init}} \wedge x_{1,n,t_{fin}}$$

ד. מתקיימים תנאי שכנות במאוזן:

$\{f(i,j), f(i+1,j)\} \in \mathrm{H}$, לכל $1 \le i \le n-1$, $1 \le j \le n$:

$$\theta_{ij}^{\mathrm{H}} = \bigvee_{(t,t') \in \mathrm{H}} x_{i,j,t} \wedge x_{i+1,j,t'}$$

לכל קואורדינטה (i,j) חייב להיות איזשהו זוג ב-H (t,t') כך שבמקום ה-(i,j) ממוקם t ובמקום ה-$(i+1,j)$ ממוקם t'.

(הסימון בהתאם לסימונים בהרצאה הבאה ולא לפי ההרצאה הזאת)

באופן שקול (ב-CNF):

$$\bigwedge_t (\overline{x_{i,j,t}} \vee \bigvee_{t':V(t,t')} x_{i+1,j,t'})$$

או שהבלטה t לא נמצאת בקואורדינטה (i,j), או שהיא כן נמצאת ויש איזשהו t'..

~ תזכורת משיעור קודם ~

$$\mathrm{BTILE} = \{\mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n\}$$

$$3\mathrm{SAT} = \{\varphi : \text{3CNF} - \text{נוסחה ספיקה ב } \varphi\}$$

$$\mathrm{BA}_{\mathrm{NTM}} \leq_p \mathrm{BTILE} \leq_p 3\mathrm{SAT}$$

- <u>ריצוף חוקי:</u> $f: \{1, \dots, n\} \times \{1, \dots, n\} \longrightarrow \mathrm{T}$
- <u>השמה:</u> $g: X \longrightarrow \{0,1\}$
- <u>ספיקה:</u> אכן מתאים לריצוף + חוקי (התקבל מא' + ב')
- <u>המשתנים:</u> $X = \{x_{i,j,t} : 1 \leq i, j \leq n, t \in \mathrm{T}\}$

$$f(i,j) = t \iff x_{i,j,t} = 1$$

א. לכל מיקום מותאם <u>לפחות</u> אריח אחד:

לכל $1 \leq i, j \leq n$ $\quad \theta_{ij} = \bigvee_{t \in \mathrm{T}} x_{i,j,t}$

ב. לכל מיקום מותאם <u>לכל היותר</u> אריח אחד:

$$\theta'_{ij} = \bigwedge_{t \in \mathrm{T}} \left(x_{i,j,t} \rightarrow \bigwedge_{t' \in \mathrm{T}} \overline{x_{i,j,t'}}\right)$$

ג. התנאים על t_{init} ועל t_{fin} מתקיימים:

$$\theta_{border} = x_{1,1,t_{init}} \wedge x_{1,n,t_{fin}}$$

ד. תנאי שכנות במאוזן (כיבוד H)

ה. תנאי שכנות במאונך:

$$\theta_{ij}^{\mathrm{V}} = \bigvee_{(t,t') \in \mathrm{V}} x_{i,j,t} \wedge x_{i,j+1,t'}$$

$$\boxed{\varphi = \underbrace{\bigwedge_{1 \leq i,j \leq n} \theta_{ij}}_{\text{א}} \underbrace{\bigwedge_{1 \leq i,j \leq n} \theta'_{ij}}_{\text{ב}} \bigwedge \theta_{border} \bigwedge_{1 \leq i \leq n-1, 1 \leq j \leq n} \theta_{ij}^{\mathrm{H}} \bigwedge_{1 \leq i \leq n, 1 \leq j \leq n-1} \theta_{ij}^{\mathrm{V}}}$$

נשים ❤ שהרדוקציה פולי' – יש $|\mathrm{T}| \cdot n^2$ משתנים, והאורך של φ הוא $O(n^2(|\mathrm{T}|^2 + |\mathrm{H}| + |\mathrm{V}|))$.

נכונות:

$$< \mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n > \in \mathrm{BTILE} \iff \text{ספיקה } \varphi$$

$\Longrightarrow$ $< \mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n > \in \mathrm{BTILE}$ אז קיים ריצוף חוקי.

תהי g השמה ל-X כך ש-$g(x_{i,j,t}) = 1$ אמ"מ $f(i,j) = t$ לכל ריצוף השמה אחת.

קל לראות ש-g השמה מספקת של φ ו-$\varphi \in \mathrm{SAT}$.

$\Longleftarrow$ נניח ש-φ ספיקה ותהי $g: X \longrightarrow \{0,1\}$ השמה מספקת.

א' + ב' מבטיחים שקיים ריצוף f כך ש-$g(x_{i,j,t}) = 1 \Leftrightarrow f(i,j) = t$ (כל השמה מספקת משרה ריצוף יחיד).

ג' + ד' + ה' מבטיחים שהריצוף הוא חוקי.

$\longleftarrow$ $< \mathrm{T}, \mathrm{H}, \mathrm{V}, t_{init}, t_{fin}, 1^n > \in \mathrm{BTILE}$.

המחלקה coNP

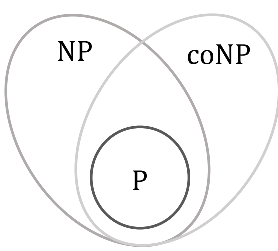
שפה $L \subseteq \Sigma^*$ היא ב-coNP אמ"מ $\bar{L} \in \mathrm{NP}$.

<u>דוגמה:</u>

$$\mathrm{VAL} = \{\varphi: \text{טאוטולוגיה } \varphi\}$$

טאוטולוגיה – כל השמה מספקת את φ.

φ היא טאוטולוגיה אם $\neg\varphi$ אינה ספיקה.



$\mathrm{P} \subseteq \mathrm{coNP}$ כי P סגור למשלים.

א. $\mathrm{P} = \mathrm{NP}$ ב. $\mathrm{NP} = \mathrm{coNP}$

<u>האם א' $\Longleftarrow$ ב'?</u>

כן, א $\mathrm{P} = \mathrm{NP}$ אז $\mathrm{NP} = \mathrm{coNP}$ כי P סגור למשלים, ואז $\bar{\mathrm{P}} = \mathrm{NP}$.

<u>האם ב' $\Longleftarrow$ א'?</u>

לא יודעים.

יש $L \in \mathrm{NP} \cap \mathrm{coNP}$ שלא יודעים אם $L \in \mathrm{P}$.

סיבוכיות זיכרון (שטח) Space complexity

בהינתן מ"ט דטרמיניסטית חד-סרטית M העוצרת על כל קלט, **סיבוכיות הזיכרון** של M היא פונקציה $S: \mathbb{N} \longrightarrow \mathbb{N}$ כך ש-$S(n)$ הוא חסם על מספר התאים בהם M משתמשת בריצתה על קלט באורך n.

מה עדיף? זמן ריצה $f(n)$ או שטח ריצה $f(n)$? שטח ריצה, כי $\mathrm{TIME}(f(n)) \subseteq \mathrm{SPACE}(f(n))$.

כל מה שניתן להכריע בזמן לינארי ניתן להכריע בשטח לינארי.

כמו כן, $\mathrm{SPACE}(f(n)) \subseteq \mathrm{TIME}(2^{O(f(n))})$ אינטואיציה שתפורמל: אם ייקח יותר זמן מזה, חזרנו על קונפ' ולא נעצור.

~ המשך בשיעור הבא ~