

הרצאה 4: מגבלות של אוטומטים סופיים

Based on previous iterations of this course, given by Nir Bitansky, Rotem Oshman, Iftach Haitner, and Omer Paneth.

מרצה: אורי שטמר

בהרצאה הקודמת דיברנו על אסל"ד וראינו כי הם שקולים בכוחם לאס"ד. השתמשנו במושג האסל"ד על מנת להראות סגירות לפעולות רגולריות. היום נדון במגבלות של אס"ד וננסה להבין איזה שפות לא ניתן להכריע באמצעות אס"ד.

דוגמאות:

$$\{0^n 1^n : n \geq 0\}$$

$$\{x \in \{0,1\}^* : \#_0(x) = \#_1(x)\}$$

בשתי הדוגמאות נראה שהאוטומט צריך "לזכור" כמה "0" קרא, לא נשמע אפשרי עם זיכרון סופי. אבל איך מוכיחים?

הוכחה בציר עבור $L = \{0^n 1^n : n \geq 0\}$:
נניח בשלילה כי קיים אס"ד $A = (Q, \Sigma, \delta, q_0, F)$ המקבל את L . ניקח $n > |Q|$ כלשהו ונחשוב על המילה $0^n 1^n$ אשר אמורה להתקבל ע"י האוטומט. אז קיימת סדרת מצבים (עם חזרות) המקיימת:

$$q_0 \xrightarrow{0} q_n \xrightarrow{1} q_{n+1} \xrightarrow{1} q_{2n}$$

כאשר q_0 הוא המצב ההתחלתי ו- q_{2n} הוא מצב מקבל.

מכיון ש- $|Q| > n$, לפי עקרון שוברך היונים, בסדרה (q_0, q_1, \dots, q_n) קיים מצב המופיע פעמיים, נניח $q_i = q_j = q$ עבור $0 \leq i < j \leq n$. כלומר החישוב נראה כך:

$$q_0 \xrightarrow{0} \dots \xrightarrow{0} q \xrightarrow{0} \dots \xrightarrow{0} q \xrightarrow{0} \dots \xrightarrow{0} q_n \xrightarrow{1} q_{n+1} \xrightarrow{1} \dots \xrightarrow{1} q_{2n}$$

לכן גם המילה $0^{n-(j-i)} 1^n$ מתקבלת ע"י האוטומט, כי נקבל את אותו מסלול חישוב רק ללא "המעגל האדום", מה שמביא לסתירה.

עכשיו נכליל את השיטה הזאת כדי להראות משפט שיאפשר לנו להוכיח אי-רגולריות של הרבה שפות אחרות.

למת הניפוח

למה: תהי L שפה רגולרית. אזי קיים $\ell > 0$ כך שלכל $w \in L$ באורך $|w| \leq \ell$ קיים פירוק $w = xyz$ כאשר:

1. לכל $k \geq 0$ מתקיים $x y^k z \in L$ מתאפשר ניפוח, או "כיווץ" אם נבחר $k = 0$
2. $|y| > 0$ הניפוח הוא לא טריוויאלי, כלומר y הוא לא המחרוזת הריקה
3. $\ell \geq |xy|$ זה תנאי טכני שלפעמים יהיה שימושי. הוא אומר לנו שהחלק של המילה אותו אפשר לנפח הוא יחסית בתחילת המילה (ב- ℓ התווים הראשונים)

הגדרה: ה- ℓ המינימלי עבורו מתקיימת הלמה נקרא קבוע הניפוח של L

הוכחת למת הניפוח:

יהי $A = (Q, \Sigma, \delta, q_0, F)$ אס"ד המקבל את L . נקבע $|Q| = \ell$. תהי $w \in L$ באורך $|w| \leq \ell$. יהיו q_0, q_1, \dots, q_ℓ המצבים בהם A עובר בריצה על $w_1 \dots w_\ell$. כלומר לכל t מתקיים

$$q_t = \hat{\delta}(q_0, w_1 \dots w_t)$$

מכיוון שיש $|Q| > \ell + 1$ מצבים, מעיקרון שובר היונים קיימים $0 \leq i < j \leq \ell$ עבורם $q_i = q_j = q$.

בציור:

$$q_0 \xrightarrow{w_1} q_1 \xrightarrow{w_2} \dots \xrightarrow{w_i} q \xrightarrow{w_{i+1}} \dots \xrightarrow{w_j} q \xrightarrow{w_{j+1}} q_{j+1} \xrightarrow{w_{j+2}} \dots$$

נגדיר $w = xyz$ כאשר

$$x = w_1 \dots w_i \quad y = w_{i+1} \dots w_j \quad z = w_{j+1} \dots$$

מתקיים:

2. $0 < j - i = |y|$ כלומר האורך של y גדול מאפס כי חוזרים על המצב q

3. $\ell \geq j = |xy|$ כלומר קיים מצב שחוזר על עצמו מבין ℓ המעברים הראשונים

1. לכל $k \geq 0$ מתקיים

$$\hat{\delta}(q_0, x y^k z) = \hat{\delta}(\hat{\delta}(q_0, x), y^k z) = \hat{\delta}(q, y^k z) = \hat{\delta}(q, yz) \underset{\text{מצד שני}}{=} \hat{\delta}(q_0, xyz)$$

ולכן $x y^k z \in L(A)$

(פורמלית חלק מהמעברים הנ"ל דורשים אינדוקציה...)

מ.ש.ל.

נקודה למחשבה (אפשר לדלג): שפה סופית אי אפשר לנפח. זה מסתדר עם למת הניפוח כי קבוע הניפוח יהיה גדול יותר מאורך המילה הארוכה ביותר בשפה (ואז הלמה נכונה באופן ריק). ההוכחה שראינו עכשיו בעצם אומרת שעבור אוטומט A , כל מילה באורך לפחות $|Q|$ ניתנת לניפוח. לכן, אם $A(L)$ סופית, לא יתכן שיש מילה ב $L(A)$ באורך לפחות $|Q|$, כי אז היה אפשר לנפח אותה כרצוננו. במילים אחרות, אם A מקבל שפה סופית, אז מספר המצבים שלו חייב להיות גדול לפחות כמו אורך המילה הארוכה ביותר בשפה...

נשתמש בלמת הניפוח כדי להראות ששפות מסויימות אינן רגולריות: בהינתן שפה L שאנחנו רוצים להראות שאינה רגולרית, נראה כי L אינה מקיימת את למת הניפוח. ספציפית, נראה כי לכל קבוע ℓ קיימת מילה באורך $\ell \leq$ שלא מקיימת את תנאי הלמה.

טענה: השפה $L = \{x \in \{0,1\}^* : \#_0(x) = \#_1(x)\}$ אינה רגולרית.

הוכחה:

נניח בשלילה כי השפה רגולרית ויהי ℓ קבוע הניפוח שלה. נסתכל על המילה $w = 0^\ell 1^\ell \in L$. לפי למת הניפוח, קיים פירוק $w = xyz$ עבור $|y| > 0$ ועבור $\ell \geq |xy|$. אז בהכרח $y = 0^k$ עבור $1 \leq k \leq \ell$ כלשהו.

קעת לפי למת הניפוח, גם המילה xy^2z אמורה להיות בשפה, אבל יש בה יותר אפסים מאחדות. סתירה.

טענה: השפה $L = \{0^i 1^j : i > j\}$ אינה רגולרית.

הוכחה:

נניח בשלילה כי השפה רגולרית ויהי ℓ קבוע הניפוח שלה. נסתכל על המילה $w = 0^\ell 1^{\ell-1} \in L$. לפי למת הניפוח, קיים פירוק $w = xyz$ עבור $|y| > 0$ ועבור $\ell \geq |xy|$. אז בהכרח $y = 0^k$ עבור $1 \leq k \leq \ell$ כלשהו. קעת לפי למת הניפוח, גם המילה xy^0z אמורה להיות בשפה, אבל אין בה יותר אפסים מאחדות. סתירה.

טענה: השפה $\{a^p : p \text{ ראשוני}\}$ אינה רגולרית.

הוכחה:

נניח בשלילה כי השפה רגולרית ויהי ℓ קבוע הניפוח שלה. יהי $p \geq \ell$ ראשוני ונסתכל על המילה $w = a^p \in L$.

לפי למת הניפוח, קיים פירוק $w = xyz$ עבור $|y| > 0$. אז בהכרח $y = a^k$ עבור $1 \leq k \leq p$ כלשהו. קעת לפי למת הניפוח, גם

$$x y^{p+1} z = x y y^p z = a^{p+kp}$$

אמורה להיות בשפה, אבל $p + kp = p(k + 1)$ אינו ראשוני. סתירה.

שאלה: האם כל שפה שניתן לנפח בהכרח רגולרית?

דוגמה:

$$L = \{a^i b^n c^n : n \geq 0, i \geq 1\} \cup \{b^n c^m : n, m \geq 0\}$$

טענה 1: L ניתנת לניפוח עם קבוע ניפוח 1

הוכיחו בעצמכם. רמז: הראו כי אם $w \in L$ אז גם $w_1^k w_2 \dots w_{|w|} \in L$

טענה 2: L אינה רגולרית

איך נוכיח את זה? לא ניתן להשתמש בלמת הניפוח...

דרך 1: ע"י תכונות סגירות. נסתכל על השפה הבאה:

$$L' = L \cap \underbrace{\{a b^n c^m : n, m \geq 0\}}_{\substack{\text{שפה רגולרית} \\ \text{(שרשור 3 שפות רגולריות)}}} = \underbrace{\{a b^n c^n : n \geq 0\}}_{\substack{\text{לא רגולרית} \\ \text{אפשר להראות ע"י למת הניפוח}}}$$

לכן L אינה רגולרית, כי חיתוך של שפות רגולריות היה יוצא רגולרי

דרך 2: מחלקות שקילות

הגדרה: תהי $L \subseteq \Sigma^*$ שפה. מילים $x, y \in \Sigma^*$ נקראות L-שקולות אם לכל $z \in \Sigma^*$ מתקיים $xz \in L$ אם ו"ם $yz \in L$.

נסמן זאת על ידי $x \sim_L y$. בנוסף, נסמן ב $[x]_L$ את מחלקת השקילות של x ונסמן ב- Σ^*/\sim_L את אוסף מחלקות השקילות.

שימו לב שזה אכן יחס שקילות (רפלקסיבי, סימטרי וטרנזיטיבי)

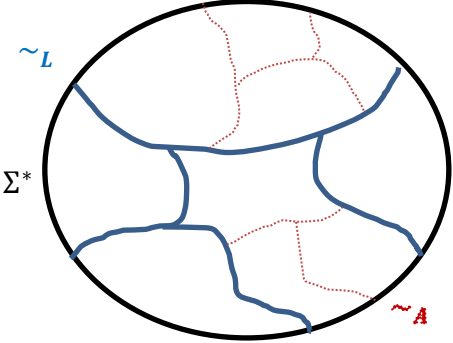
הגדרה: יהי $A = (Q, \Sigma, \delta, q_0, F)$ אוטומט. $x, y \in \Sigma^*$ נקראות A-שקולות אם $\hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)$.

נסמן $y \sim_A x$, $[x]_A$, Σ^*/\sim_A באופן אנלוגי

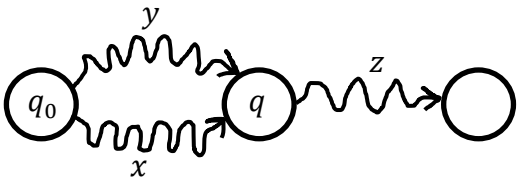
שימו לב כי $|\Sigma^*/\sim_A| \geq |Q|$ (מדוע?)

טענה: יהי $A = (Q, \Sigma, \delta, q_0, F)$ אס"ד, נסמן $L = L(A)$, ויהיו $x, y \in \Sigma^*$, אם $x \sim_A y$ אז $x \sim_L y$.

כלומר \sim_A הוא עידון של \sim_L .
בציור:



הוכחת הטענה: בציור



פורמלית:

אם $x \sim_A y$ אז לכל $z \in \Sigma^*$ מתקיים

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

מסקנה 1:
 $|Q| \geq |\Sigma^*/\sim_A| \geq |\Sigma^*/\sim_L|$
 כלומר מס' מח' השקילות ב \sim_L חסום ע"י מספר המצבים בכל אוטומט (או באוטומט המינימלי) שמקבל את L

מסקנה 2: אם L רגולרית אז Σ^*/\sim_L סופית
 כי אם L רגולרית אז יש אס"ד שמקבל אותה ואוסף מח' השקילות הוא בגודל של לכל היותר קב' המצבים

משפט מִיִּיהִל-גֶּרֻוד: L רגולרית אם"ם Σ^*/\sim_L סופית

המשפט הזה (וגם מסקנה 2) נותנים לנו כלי להוכיח ששפות מסויימות אינן רגולריות: אם נראה ש Σ^*/\sim_L אינסופית אז L אינה רגולרית.

כיוון אחד של הוכחת המשפט אנחנו כבר יודעים.

הוכחת הכיוון השני:

תהי L שפה כך ש- Σ^*/\sim_L סופית, נניח בגודל n , ויהיו x_1, x_2, \dots, x_n נציגים של מחלקות השקילות של היחס \sim_L . כלומר לכל מילה $y \in \Sigma^*$ קיים יחיד i כך ש- $y \in [x_i]_L$. נסמן אינדקס i זה ע"י $\text{Class}(y)$.

כלומר לכל $y \in \Sigma^*$ מתקיים $\text{Class}(y) = i \in \{1, 2, \dots, n\}$ כך ש- $y \in [x_i]$.

נבנה אוטומט $A = (Q, \Sigma, \delta, q_0, F)$ המקבל את L :

$$\begin{aligned} Q &= \{1, 2, \dots, n\} \\ \delta(i, \sigma) &= \text{Class}(x_i \sigma) \\ q_0 &= \text{Class}(\varepsilon) \\ F &= \{i : x_i \in L\} \end{aligned}$$

טענת עזר: לכל $y \in \Sigma^*$ מתקיים $\hat{\delta}(q_0, y) = \text{Class}(y)$

לכן:

$$y \in L \quad \underbrace{\text{אם"ם}}_{\sim_L} \quad x_{\text{Class}(y)} \in L \quad \underbrace{\text{אם"ם}}_{\text{הגדרת } F} \quad \text{Class}(y) \in F \quad \underbrace{\text{אם"ם}}_{\text{ט.ע.}} \quad \hat{\delta}(q_0, y) \in F \quad \underbrace{\text{אם"ם}}_{\hat{\delta} \text{ הגדרת}} \quad y \in L(A)$$

הוכחת טענת העזר באינדוקציה על $|y|$. בסיס $y = \varepsilon$ לפי הגדרה. עבור צעד האינדוקציה, יהי $y = w\sigma$ ונניח כי $y \in [x_j]_L$, $w \in [x_i]_L$. אזי

$$\hat{\delta}(q_0, w\sigma) = \delta(\hat{\delta}(q_0, w), \sigma) \stackrel{\text{א.ה.}}{=} \delta(i, \sigma) = \text{Class}(x_i \sigma) \stackrel{x_i \sim_L w}{=} \text{Class}(w\sigma) = \text{Class}(y) = j$$

שימוש במסקנה 2: נראה כי

$$L = \{a^i b^n c^n : n \geq 0, i \geq 1\} \cup \{b^n c^m : n, m \geq 0\}$$

אינה רגולרית ע"י שנראה כי Σ^*/\sim_L אינסופית.

אכן, לכל $n \neq m$ מתקיים

$$[ab^n]_L \neq [ab^m]_L$$

מדוע?

אנחנו מסתכלים על סדרת המילים האינסופית הבאה:

$$ab, ab^2, ab^3, ab^4, ab^5, \dots$$

אנחנו טוענים שאין אף זוג מילים בסדרה הזאת שהן שקולות. למשל, נסתכל על ab^2, ab^4 . כדי להוכיח שהן לא שקולות מספיק להראות שיש סיפא שמובילה "לגורל" שונה (כי אם הן היו שקולות אז כל סיפא הייתה מובילה לאותו גורל). ואמנם, עבור c^2 נקבל $ab^4 c^2 \notin L$, $ab^2 c^2 \in L$. מסקנה, קיבלנו סדרה אינסופית של מילים, בה אף זוג לא יכול להיות שקול, לכן יש אינסוף מחלקות שקילות, לכן השפה לא יכולה להיות רגולרית.

שימוש במסקנה 1: נוכיח כי התקורה האקספוננציאלית במעבר מאסל"ד לאס"ד הכרחית.

דוגמה: יהי $n \in \mathbb{N}$ ותהי $\Sigma = \{1, 2, \dots, n\}$. עבור $x \in \Sigma^*$ נסמן ב- S_x את קבוצת התווים המשתתפים ב- x כלומר

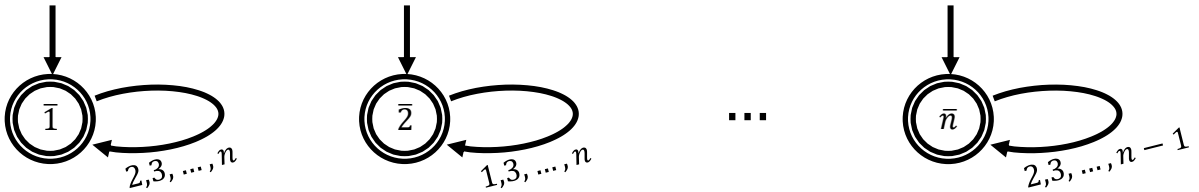
$$S_x = \{\sigma \in \Sigma^* : \exists j \text{ such that } x_j = \sigma\}$$

נגדיר שפה

$$L = \{x \in \Sigma^* : S_x \neq \Sigma\}$$

טענה: קיים אסל"ד בן n מצבים המזהה את L אבל כל אס"ד המזהה את L בעל לפחות 2^n מצבים.

הוכחה:



נראה כעת כי $2^n \leq |\Sigma^*/\sim_L|$

לשם כך מספיק להראות כי לכל $x, y \in \Sigma^*$ כך ש- $S_x \neq S_y$ מתקיים $[x]_L \neq [y]_L$ (זה מספיק כי יש 2^n תתי-קבוצות של תווים)

אז יהיו $x, y \in \Sigma^*$ כנ"ל. בה"כ נניח כי קיים תוו a אשר מופיע ב- x אבל לא ב- y . כעת תהי $z \in \Sigma^*$ מילה כלשהי המכילה (בדיוק) את כל התווים שאינם ב- x . נשים לב ש- a לא מופיע ב- z ולא מופיע ב- x .

מתקיים:

- $S_{xz} = S_x \cup S_z = \Sigma$ ולכן $xz \notin L$
- $a \notin S_{yz}$ ולכן $yz \in L$

מ.ש.ל.

שאלות אלגוריתמיות לגבי אוטומטים

האם קיים "אלגוריתם יעיל" לבעיה הבאה:

שאלה 1: בהינתן אסל"ד N וקלט $x \in \Sigma^*$, האם $x \in L(N)$?

טרם הגדרנו פורמלית מה הכוונה באלגוריתם יעיל ונשאיר את זה כרגע ברמה הלא פורמלית. קונקרטי ניתן חשוב על תוכנית פייתון עם זמן ריצה פולינומי באורך הקלט. הקלט נתון ע"י קידוד (בה"כ בינארי) של מרכיבי האסל"ד $Q, \Sigma, \delta, q_0, F$.

תשובה: ניתן לפתרון אלגוריתמי:

- אפשרות 1: נריץ ישירות את N . כלומר נעבור על הקלט תוו-תוו ובכל פעם נחשב את "חזית המצבים" אפשר להגיע אליה. בסוף (בחזית האחרונה) נבדוק אם מופיע מצב מקבל. זמן ריצה בערך $|Q| \cdot |x|$

- אפשרות 2: נחשב אס"ד A עבורו $L(A) = L(N)$ ואז נריץ אותו. זמן ריצה בערך $|x| + 2^{|Q|}$

שאלה 2: בהינתן אס"ד N , האם $L(N) \neq \emptyset$?

תשובה: קיים אלגוריתם יעיל: נבדוק האם קיים מסלול מאיזשהו מצב תחילי לאיזשהו מצב מקבל

בקורס באלגוריתמים מראים איך אפשר לחפש מסלולים בגרפים ביעילות. אם עדיין לא לקחתם קורס באלגוריתמים אז לפחות צריך להיות ברור לכם אינטואיטיבית שאפשר לעשות את זה לא ביעילות (ממש לעבור על כל המסלולים).

שאלה 3: בהינתן אס"ד N , האם $L(N) = \Sigma^*$?

תשובה: נבנה אוטומט ל- $\overline{L(N)}$ ונחזור לשאלה 2.

איך בונים אוטומט ל- $\overline{L(N)}$? באס"ד היינו יכולים פשוט להפוך את התפקידים של המצבים המקבלים והלא מקבלים. אם מתחילים מאס"ד אז אפשר להמיר אותו לאס"ד ואז לעשות אותו דבר. אבל ההמרה מאס"ד לאס"ד הייתה דיי יקרה (אקספוננציאלית במס' המצבים). אז זה לא הכי יעיל...

שאלה 4: בהינתן אס"דים N, N' , האם $L(N) \subseteq L(N')$?

תשובה: מתקיים אם $L(N) \cap \overline{L(N')} = \emptyset$. חזרה לשאלה 2.

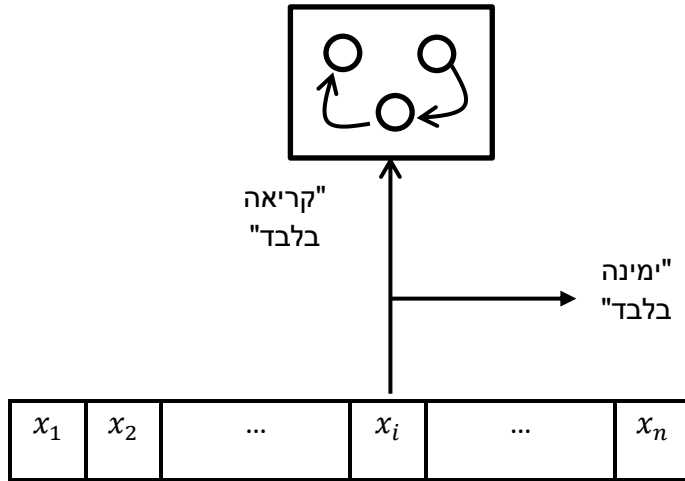
מהו זמן הריצה של שני האלגוריתמים האחרונים (כפונקציה של גודל האס"ד N) ?

הבעיות האלה הן $PSPACE$ -שלמות (נדבר על בעיות כאלה בהמשך). בפרט לא סביר שיש אלג' יעיל.

מכונות טיורינג

אוטומטים היו עבורנו חימום. הם ייצגו מודל יוניפורמי פשוט. כעת נרצה להבין אלגוריתמים כלליים כמו אלו אליהם אנו רגילים. המודל עמו נעבוד הינו מודל תיאורטי פשוט הנקרא "מכונות טיורינג" על שם אלן טיורינג שהגה אותו ב 1936.

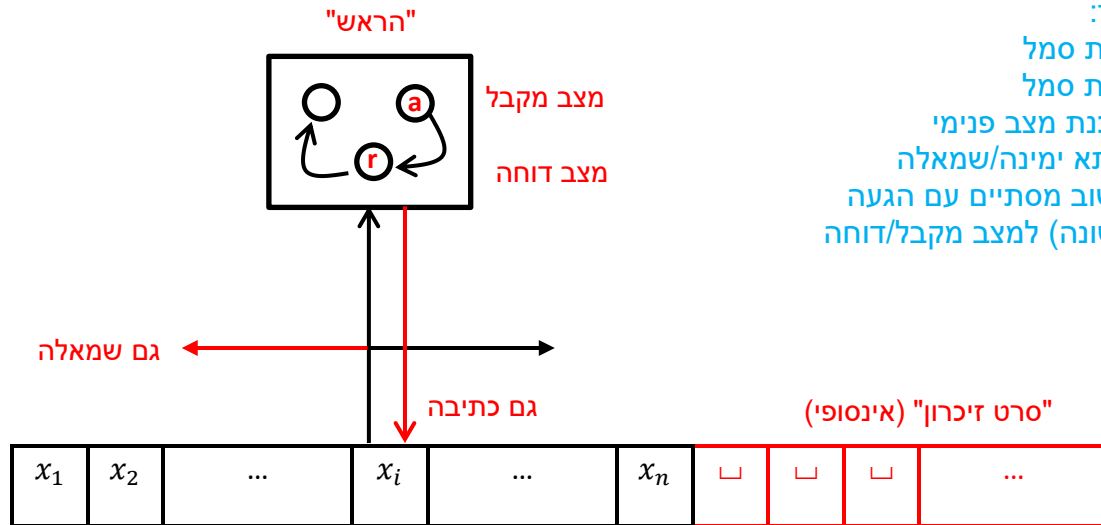
א"ד:



מכונת טיורינג:

מ"ט בכל צעד:

- קוראת סמל
- כותבת סמל
- מעדכנת מצב פנימי
- זזה תא ימינה/שמאלה
- החישוב מסתיים עם הגעה (ראשונה) למצב מקבל/דוחה



דוגמה: $L = \{a^{2^n} : n \geq 0\}$

האם השפה רגולרית? לא... לכל $i \neq j$ מתקיים $[a^{2^i}]_L \neq [a^{2^j}]_L$

למה?

נניח $i < j$ וניקח $z = a^{2^i}$. אזי

$$a^{2^i} z = a^{2^{i+1}} \in L$$

$$a^{2^j} z = a^{2^i+2^j} = a^{2^i(1+2^{j-i})} \notin L, \quad \text{because } 2^i(1+2^{j-i}) \text{ is not a power of 2}$$

תיאור לא פורמלי של מ"ט:

1. אם הסרט ריק, נדחה
2. אם הסרט מכיל a יחיד, נקבל
3. נלך ימינה ונמחק כל a שני
4. אם אמורים למחוק, אך הגענו לסוף הקלט (לפני צעד 3 היה מס' אי-זוגי של a), נדחה
5. נחזור לתחילת הסרט ולצעד 2.

קלט לדוגמה: $a^8 = a^8$

a a a a a a a a
~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~
a ~~a~~ ~~a~~ ~~a~~ a ~~a~~ ~~a~~ ~~a~~
a ~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~ ~~a~~

accept

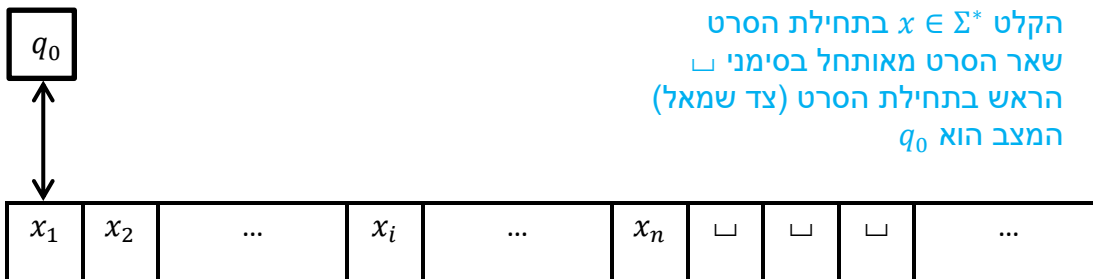
הגדרה: מכונת מטיורינג (מ"ט) היא שביעייה $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ כאשר:

- Q קבוצת מצבים סופית $q_0, q_a, q_r \in Q$
- Σ אלפאבית קלט
- Γ אלפאבית סרט כך ש- $\Sigma \subseteq \Gamma$, $\sqcup \in \Gamma \setminus \Sigma$
- δ פונקציית מעברים כך ש- $\delta: (Q \setminus \{q_a, q_r\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$
- q_0 מצב תחילי
- q_a מצב מקבל
- $q_a \neq q_r$, מצב דוחה,

חישוב של מ"ט:

• בתחילת החישוב:

- הקלט $x \in \Sigma^*$ בתחילת הסרט
- שאר הסרט מאותחל בסימני \sqcup
- הראש בתחילת הסרט (צד שמאל)
- המצב הוא q_0



• צעד חישוב:

- אם המצב הפנימי הוא $q \in Q \setminus \{q_a, q_r\}$ והראש קורא $a \in \Gamma$
- מחשבים $\delta(q, a) = (q', a', D)$

- הראש כותב a' (במקום a)
- עובר למצב q'
- זז צעד ימינה אם $D = R$ ושמאלה אם $D = L$
- (אם $D = L$ והראש בתחילת הסרט אז הוא נותר במקום)

• ברגע שהגענו ל- q_a או ל- q_r החישוב מסתיים.

בהמשך לתמונה הקודמת, אם $\delta(q, x_1) = (q', a', R)$ אז נקבל

